Cooper Johnston

Introduction to Abstract Algebra

Adopted from lectures, notes, and exercises by

Hugues Verdure and Philippe Moustrou

for the course MAT-2300, Algebra 1 at

UiT – The Arctic University of Norway
Department of Mathematics and Statistics

Contents

Chapter 0

Foundations

0.1 Prerequisites, conventions, and notation

We will assume the reader is familiar with the concept of a set, set-builder notation, and basic set operations. By convention, the set of natural numbers $\mathbb{N}$ will be taken to start from 1.

0.2 Sets and relations

Definition 0.2.1. For two sets A and B, any subset of $A \times B$ is called a relation, and for all (a, b) in this relation, we say a is related to b, denoted, for example, by $a \sim b$.

Definition 0.2.2. A relation $a \sim b$ is called an equivalence relation if it is

1. reflexive: for every a, we have $a \sim a$;
2. symmetric: for every a, b such that $a \sim b$, we have $b \sim a$; and
3. transitive: for every a, b, c such that $a \sim b$ and $b \sim c$, we have $a \sim c$.

Definition 0.2.3. The set $[a] = \{b \mid a \sim b\}$ is called the equivalence class of a.

Theorem 0.2.4. Let $\sim$ be an equivalence relation on a set X. Then, the equivalence classes are disjoint and form a partition of X.

Proof. Let $x_1, x_2 \in X$ and consider the equivalence classes $[x_1]$ and $[x_2]$. Suppose they are not disjoint. Then, there exists a y such that $y \in [x_1] \cap [x_2]$, so $x_1 \sim y$ and $x_2 \sim y$. By the symmetric property, $x_1 \sim y$ and $y \sim x_2$, so by the transitive property, $x_1 \sim x_2$.

Now let $x \in [x_1]$. Then, $x_1 \sim x$, and since $x_1 \sim x_2$, we have $x_2 \sim x$, so $x \in [x_2]$. Thus, $[x_1] \subseteq [x_2]$, and similarly, $[x_2] \subseteq [x_1]$, so $[x_1] = [x_2]$. ■

0.3 Examples of proofs

Claim 0.3.1 (For a direct proof)**.** The product of two odd numbers is odd.

Proof. Let a and b be odd. Then, $a = 2n + 1$ and $b = 2k + 1$ for some $n, k \in \mathbb{Z}$, so we have

$$ab = (2n + 1)(2k + 1) = 4nk + 2n + 2k + 1 = 2(2nk + n + k) + 1$$

which is odd since $2nk + n + k \in \mathbb{Z}$. ■

Claim 0.3.2 (For a proof by contraposition)**.** Let $n \in \mathbb{Z}$. If n^2 is odd, then n is odd.

Proof. Suppose n is even. Then, $n = 2k$ for some $k \in \mathbb{Z}$, so

$$n^2 = (2k)^2 = 4k^2 = 2(2k^2)$$

which is even since $2k^2 \in \mathbb{Z}$. Hence, if n^2 is odd, then n is odd. ■

Claim 0.3.3 (For a proof by contradiction)**.** Let $p \in \mathbb{Z}$. If p is prime, then $\sqrt{p} \notin \mathbb{Q}$.

Proof. Suppose $\sqrt{p} \in \mathbb{Q}$. Then, there exist some $a, b \in \mathbb{Z}$, $b \neq 0$ such that $\sqrt{p} = a/b$. Without loss of generality, assume $\gcd(a, b) = 1$. We see

$$p = \left(\frac{a}{b}\right)^2 = \frac{a^2}{b^2} \iff pb^2 = a^2 \implies p \mid a^2,$$

and since p is prime, we see $p \mid a$. There must then exist some $n \in \mathbb{Z}$ such that $a = np$, so

$$pb^2 = a^2 = (np)^2 = n^2p^2 \iff b^2 = n^2p \implies p \mid b^2 \iff p \mid b.$$

Thus, p divides both a and b, but this is a contradiction since $\gcd(a, b) = 1$. Hence, $\sqrt{p} \notin \mathbb{Q}$. ■

Claim 0.3.4 (For a proof by induction)**.** Let $n \in \mathbb{N}$. If $n \geq 5$, then $n! \geq 2^n$.

Proof. For our base step, we see $5! = 120$ and $2^5 = 32$, so $5! \geq 2^5$.

As our inductive hypothesis, assume $k! \geq 2^k$ for some $k \geq 5$. Then,

$$(k + 1)k! \geq (k + 1)2^k \geq 6 \cdot 2^k \geq 2 \cdot 2^k = 2^{k+1} \implies (k + 1)! \geq 2^{k+1}.$$

Hence, $n! \geq 2^n$ for all $n \geq 5$. ■

Note that this does not address the fact that $4! \geq 2^4$.

Solved exercises

Set operations

For each of the following, find $A \cap B$, $A \cup B$, $A \setminus B$, $B \setminus A$, $A \times B$, and $B \times A$.

Exercise 0.1. Let $A = \{-1, 1\}$ and $B = \{1, 2, 3\}$.

Solution. We have

$$\begin{aligned}
A \cap B &= \{1\}, \\
A \cup B &= \{-1, 1, 2, 3\}, \\
A \setminus B &= \{-1\}, \\
B \setminus A &= \{2, 3\}, \\
A \times B &= \{(-1, 1), (-1, 2), (-1, 3), (1, 1), (1, 2), (1, 3)\}, \\
B \times A &= \{(1, -1), (1, 1), (2, -1), (2, 1), (3, -1), (3, 1)\}.
\end{aligned}$$ □

Exercise 0.2. Let $A = [-1, 1]$ and $B = (0, 3]$.

Solution. We have

$$\begin{aligned}
A \cap B &= (0, 1], \\
A \cup B &= [-1, 3], \\
A \setminus B &= [-1, 0], \\
B \setminus A &= (1, 3], \\
A \times B &= \{(a, b) \mid a \in [-1, 1], b \in (0, 3]\}, \\
B \times A &= \{(b, a) \mid b \in (0, 3], a \in [-1, 1]\}.
\end{aligned}$$ □

Exercise 0.3. Let $A = (1, 3)$ and $B = [0, \infty)$.

Solution. We have

$$\begin{aligned}
A \cap B &= (1, 3), \\
A \cup B &= [0, \infty), \\
A \setminus B &= \varnothing, \\
B \setminus A &= [0, 1] \cup [3, \infty), \\
A \times B &= \{(a, b) \mid a \in (1, 3), b \in [0, \infty)\}, \\
B \times A &= \{(b, a) \mid b \in [0, \infty), a \in (1, 3)\}.
\end{aligned}$$ □

Proofs

Let $a, b, c \in \mathbb{N}$ where a and b are coprime. Prove the following.

Exercise 0.4. If $a \mid bc$, then $a \mid c$.

Solution. Suppose $a \mid bc$. Then, there exists some $n \in \mathbb{Z}$ such that $na = bc$, so $b \mid na$. Now suppose n is not a multiple of b. Then, a and b must share a common factor greater than 1, but a and b are coprime, so this is impossible. Therefore, n must be a multiple of b; that is, there exists some $k \in \mathbb{Z}$ such that $n = kb$, so

$$na = bc \iff \frac{n}{b}a = c \iff \frac{bk}{b}a = c \iff ka = c \implies a \mid c.$$ □

Exercise 0.5. If $a \mid c$ and $b \mid c$, then $ab \mid c$.

Solution. Suppose $a \mid c$ and $b \mid c$. Then, c is a multiple of a, and c is a multiple of b. Let $p_1 p_2 \cdots p_n$ be the prime factorization of a, and let $q_1 q_2 \cdots q_k$ be the prime factorization of b. Since a and b are coprime, we see $\{p_1, p_2, \dots, p_n\} \cap \{q_1, q_2, \dots, q_k\} = \varnothing$, so the prime factorization of c must include all of the p_is and all of the q_is. Therefore, c is a multiple of $p_1 p_2 \cdots p_n q_1 q_2 \cdots q_k = ab$, so $ab \mid c$. □

Chapter 1

Groups and Subgroups

1.1 Groups

Definition 1.1.1. Let S be a set. A mapping

$$\begin{array}{rccc} \odot: & S \times S & \to & S \\ & (x,y) & \mapsto & x \odot y \end{array}$$

is called a law of composition on S.

Note that S is necessarily closed under the operation defined by such a law. Examples include addition of natural numbers and multiplication of $n \times n$ matrices. Subtraction of natural numbers, however, is not closed and therefore not a law of composition.

Definition 1.1.2. A law of composition $\odot$ on S is called associative if for every $x, y, z \in S$, we have $(x \odot y) \odot z = x \odot (y \odot z)$. The law $\odot$ is called commutative if for every $x, y \in S$, we have $x \odot y = y \odot x$.

Definition 1.1.3. Let G be a set and $\odot$ be a law of composition on G. A pair $(G, \odot)$ is called a group if

1. $\odot$ is associative;
2. there exists a neutral element $e \in G$ such that for every $g \in G$, we have $g \odot e = e \odot g = g$; and
3. for every $g \in G$, there exists an inverse element $g^{-1} \in G$ such that $g \odot g^{-1} = g^{-1} \odot g = e$.

A group whose law is commutative is called abelian.

We will typically refer to a group by its set and denote compositions of its elements using multiplicative notation ab if commutativity is not assumed, or additive notation $a + b$ if commutativity is assumed; in the latter case, the inverse of a is denoted $-a$.

Proposition 1.1.4. The neutral element of a group is unique.

Proof. Let G be a group, and let $e_1, e_2 \in G$ such that for every $g \in G$, we have

$$e_1 g = g e_1 = g \quad \text{and} \quad e_2 g = g e_2 = g.$$

Then, in particular, $e_1 e_2 = e_1$ and $e_1 e_2 = e_2$, so $e_1 = e_2$. ∎

Proposition 1.1.5. Let G be a group. For every $g \in G$, its inverse element g^{-1} is unique.

Proof. Let $g \in G$. Suppose h_1 and h_2 are both inverses of g. Then,

$$gh_1 = h_1 g = e \quad \text{and} \quad gh_2 = h_2 g = e,$$

so

$$h_1 = h_1 e = h_1(gh_2) = (h_1 g)h_2 = eh_2 = h_2.$$ ∎

Proposition 1.1.6. Let G be a group, and let $g, h, i \in G$. Then,

1. $(g^{-1})^{-1} = g$;
2. $(gh)^{-1} = h^{-1}g^{-1}$;
3. the equations $gx = h$ and $xg = h$ have unique solutions $x \in G$; and
4. if $gi = hi$ or $ig = ih$, then $g = h$.

These can be proven with straightforward computations.

1.2 Subgroups

Definition 1.2.1. Let $(G, \odot)$ be a group, and let $H \subseteq G$. If $(H, \odot|_{H\times H})$ is a group, it is called a subgroup of G.

Theorem 1.2.2. Let G be a group, and let $H \subseteq G$, $H \neq \varnothing$. Then, H is a subgroup of G if and only if for every $x, y \in H$, we have $xy^{-1} \in H$.

Proof. First note that by uniqueness of the neutral element, the neutral element of a subgroup must be the same as that of its parent group, and further, the inverse of an element of a subgroup must be the same as the inverse of that element in the parent group.

($\Rightarrow$) Suppose H is a subgroup of G. Let $x, y \in H$. Since H is a group, $y^{-1} \in H$, so $xy^{-1} \in H$.

($\Leftarrow$) Suppose that for every $x, y \in H$, we have $xy^{-1} \in H$. In particular, since $H \neq \varnothing$, we can take some $h \in H$ to see $hh^{-1} = e_G \in H$, so $h^{-1} = e_G h^{-1} \in H$. This means $(y^{-1})^{-1} = y \in H$. Thus, $xy \in H$, so H is closed under the law of composition on G. Further, since this law is associative on G, it is also associative on H. Hence, we have demonstrated the criteria for H to be a group. ∎

To denote the set of integer multiples of some $n \in \mathbb{Z}$, we will use the notation $n\mathbb{Z} = \{k \in \mathbb{Z} \mid k \equiv 0 \pmod{n}\}$.

Proposition 1.2.3. Let $n \in \mathbb{Z}$. Then, $(n\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$.

Proof. We see $0 \in n\mathbb{Z}$ for all $n \in \mathbb{Z}$, so $n\mathbb{Z} \neq \emptyset$. Let $a, b \in n\mathbb{Z}$. Then, $a = kn$ and $b = ln$ for some $k, l \in \mathbb{Z}$, so we have

$$a + (-b) = a - b = kn - ln = (k - l)n \in n\mathbb{Z}.$$

Hence, by Theorem 1.2.2, $(n\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$. ■

Proposition 1.2.4. Every subgroup of $(\mathbb{Z}, +)$ is of the form $(n\mathbb{Z}, +)$ for some $n \in \mathbb{Z}$.

Proof. Let H be a subgroup of $(\mathbb{Z}, +)$. If $H = \{0\}$, then $H = 0\mathbb{Z}$. Otherwise, let $k \in H \setminus \{0\}$. Without loss of generality, take k to be positive. Now let $S = H \cap \mathbb{Z}^+$. Since $k \in S$, we see $S \neq \emptyset$, so S has a minimal element, say n.

Since $n \in H$, we see $n\mathbb{Z} \subseteq H$. Additionally, rewriting k in terms of its Euclidean division by n as $k = nq + r$ where $q, r \in \mathbb{Z}$, $0 \leq r < n$, we see $r = k - nq$. Since n is minimal, we must have $r = 0$. Thus, $k = nq \in n\mathbb{Z}$, so $H \subseteq n\mathbb{Z}$. Hence, $H = n\mathbb{Z}$. ■

Proposition 1.2.5. Let G be a group, and let $S \subseteq G$. Then, there exists a unique subgroup H of G such that

1. $S \subseteq H$ and
2. if H' is a subgroup of G and $S \subseteq H'$, then H is a subgroup of H'.

Proof A. Let X be the set of all subgroups of G that contain S. Since $G \in X$, we see $X \neq \emptyset$. Now let $H = \cap_{J \in X} J$. We see $S \subseteq H$. Finally, let $x, y \in H$. Then, $x, y \in J$ for all $J \in X$, and since each J is a subgroup of G, we have $xy^{-1} \in J$ for all $J \in X$. Thus,

$$xy^{-1} \in \bigcap_{J \in X} J = H,$$

so, by Theorem 1.2.2, H is a subgroup of G.

Now suppose there exist two subgroups H_1, H_2 satisfying 1 and 2. Then, $S \subseteq H_1$ and $S \subseteq H_2$. Since H_2 is a subgroup of G containing S, by 2 we have $H_1 \subseteq H_2$; likewise, $H_2 \subseteq H_1$, so $H_1 = H_2$. Hence, H is unique. ■

Alternatively, we can use a constructive proof:

Proof B. Let $H = \{g_1^{\pm 1} g_2^{\pm 1} \cdots g_k^{\pm 1} \mid g_1, g_2, \dots, g_k \in S\}$. Then, $S \subseteq H$. Further, let $x, y \in H$. Then, $x = g_1^{\pm 1} g_2^{\pm 1} \cdots g_n^{\pm 1}$ and $y = h_1^{\pm 1} h_2^{\pm 1} \cdots h_m^{\pm 1}$ for some $g_1, g_2, \dots, g_n$,

$h_1, h_2, \dots, h_m \in S$, so

$$\begin{aligned} xy^{-1} &= g_1^{\pm 1} g_2^{\pm 1} \cdots g_n^{\pm 1} (h_1^{\pm 1} h_2^{\pm 1} \cdots h_m^{\pm 1})^{-1} \\ &= g_1^{\pm 1} g_2^{\pm 1} \cdots g_n^{\pm 1} (h_m^{\pm 1})^{-1} \cdots (h_2^{\pm 1})^{-1} (h_1^{\pm 1})^{-1} \\ &= g_1^{\pm 1} g_2^{\pm 1} \cdots g_n^{\pm 1} h_m^{\mp 1} \cdots h_2^{\mp 1} h_1^{\mp 1} \in H. \end{aligned}$$

Thus, H is a subgroup of G. Uniqueness can be shown in the same way as in Proof A. ■

Definition 1.2.6. The subgroup H from Proposition 1.2.5 is called the subgroup generated by S, denoted $\langle S \rangle$. This is, in other words, the smallest subgroup of G that contains S. When $\langle S \rangle = G$ for some group G, we say S generates G. When this S is finite, we say G is finitely generated.

Definition 1.2.7. A group generated by one element, say x, is called a cyclic group, denoted $\langle x \rangle$.

We will use the notation x^n to denote an element x of a group composed with itself n times.

Proposition 1.2.8. Let G be a group, and let $g \in G$. Then,

1. $\langle g \rangle = \langle \{g\} \rangle = \{g^m \mid m \in \mathbb{Z}\}$;
2. $\langle g \rangle$ is infinite if and only if there does not exist an $m \in \mathbb{N}$ such that $g^m = e$; and
3. if $\langle g \rangle$ is finite, then $|\langle g \rangle| = \min\{m \in \mathbb{N} \mid g^m = e\}$.

Proof.

1. Since $\langle g \rangle$ is a group, it must contain all compositions of g with itself, i.e. g^m for all $m \in \mathbb{N}$, as well as its inverse g^{-1} and the inverses of those compositions, so at the minimum, $\langle g \rangle$ contains $\{g^m \mid m \in \mathbb{Z}\}$, which is a subgroup of G. Hence, $\langle g \rangle = \{g^m \mid m \in \mathbb{Z}\}$.
2. Suppose $\langle g \rangle$ is finite. Equivalently, there exist some $n, k \in \mathbb{Z}$, $n \neq k$ such that $g^n = g^k$; without loss of generality, take $n > k$. We see

   $$g^n = g^k \iff g^n g^{-k} = g^k g^{-k} \iff g^{n-k} = e,$$

   i.e. there exists an $m = n - k \in \mathbb{N}$ such that $g^m = e$. Hence, $\langle g \rangle$ is infinite if and only if such an m does not exist.
3. From the proof for 2, it follows that if $\langle g \rangle$ is finite, then the set $\{m \in \mathbb{N} \mid g^m = e\}$ is nonempty and therefore has a least element, say n. We see $\{e, g, g^2, \dots, g^{n-1}\} \subseteq \langle g \rangle$. Let $g^k \in \langle g \rangle$ for some $k \in \mathbb{Z}$. We can rewrite k in terms of its Euclidean division by n as $k = nq + r$ for some $q, r \in \mathbb{Z}$, $0 \leq r < n$, giving us

   $$g^k = g^{nq+r} = (g^n)^q g^r = e^q g^r = g^r \in \{e, g, g^2, \dots, g^{n-1}\},$$

   so $\langle g \rangle \subseteq \{e, g, g^2, \dots, g^{n-1}\}$. Hence, $\langle g \rangle = \{e, g, g^2, \dots, g^{n-1}\}$, so $|\langle g \rangle| = n$. ■

Definition 1.2.9. Let x be some element in a group. Then, the cardinality of $\langle x\rangle$ is called the order of x, denoted $\mathrm{ord}(x)$.

1.3 Cosets

Definition 1.3.1. Let G be a group and H be a subgroup of G, and let $g \in G$. Then, the set

$$gH = \{gh \mid h \in H\}$$

is called the left coset of H associated with g, and the set

$$Hg = \{hg \mid h \in H\}$$

is called the right coset of H associated with g.

Theorem 1.3.2. Let G be a group and H be a subgroup of G, and let $x, y \in G$. Then, the relations $\sim_l$ and $\sim_r$ on G such that

$$x \sim_l y \iff x^{-1}y \in H \quad \text{and} \quad x \sim_r y \iff xy^{-1} \in H$$

are equivalence relations.

Proof. By Definition 0.2.2, we have three criteria for $\sim_l$ to be an equivalence relation:

1. We see $x^{-1}x = e \in H$, so $x \sim_l x$ (reflexive).
2. Suppose $x \sim_l y$. Then, $x^{-1}y \in H$, so $(x^{-1}y)^{-1} = y^{-1}x \in H$; therefore, $y \sim_l x$ (symmetric).
3. Let $z \in G$. Suppose $x \sim_l y$ and $y \sim_l z$. Then, $x^{-1}y, y^{-1}z \in H$, so $(x^{-1}y)(y^{-1}z) \in H$ and
$$(x^{-1}y)(y^{-1}z) = x^{-1}(yy^{-1})z = x^{-1}z;$$
thus, $x \sim_l z$ (transitive).

Hence, $\sim_l$ is an equivalence relation. The same for $\sim_r$ can be proven similarly. ■

Corollary 1.3.3 (Alternative definition of the left and right cosets)**.** Let G be a group and H be a subgroup of G, and take $\sim_l$ and $\sim_r$ as defined in Theorem 1.3.2. Then, the left cosets of H in G are the equivalence classes of $\sim_l$, and the right cosets are the equivalence classes of $\sim_r$.

Corollary 1.3.4. Let G be a group and H be a subgroup of G. The left cosets of H in G form a partition of G. The same applies for the right cosets.

We will use the notation G/H to denote to denote the set of left cosets of H in G and $H\backslash G$ to denote the set of right cosets.

Proposition 1.3.5. Let G be a group and H be a subgroup of G. Then, there exists a bijection between G/H and $H\backslash G$. It follows that the number of left cosets is equal to the number of right cosets when finite.

Proof. Consider the mapping

$$f: \begin{array}{ccc} G/H & \to & H\backslash G \\ xH & \mapsto & Hx^{-1} \end{array}.$$

Let $x, y \in G$. By Corollary 1.3.3, we see

$$\begin{aligned} xH = yH &\iff y^{-1}x \in H \iff (y^{-1}x)^{-1} \in H \iff x^{-1}y \in H \\ &\iff Hx^{-1} = Hy^{-1}, \end{aligned}$$

so f is well-defined and injective. We also see that for every $Hy \in H\backslash G$, we have $f(y^{-1}H) = Hy$, so f is surjective. Hence, f is a bijection. ■

Definition 1.3.6. Let G be a group and H be a subgroup of G. The cardinality of G/H is called the index of H in G, denoted $[G : H]$.

Proposition 1.3.7. Let G be a group and H be a subgroup of G. Then, there exists a bijection between any two cosets of H in G. It follows that if H is finite, then all the cosets are finite and have the same cardinality.

Proof. Let $g \in G$. Consider the mapping

$$f_g: \begin{array}{ccc} H & \to & gH \\ h & \mapsto & gh \end{array}.$$

By the definition of gH, we see f_g is well-defined and surjective. Let $h, h' \in H$ such that $gh = gh'$. Then, by Proposition 1.1.6, we see $h = h'$, so f_g is injective. Hence, f_g is a bijection. ■

Theorem 1.3.8 (Lagrange's theorem)**.** Let G be a finite group and H be a subgroup of G. Then, the order of every subgroup of H divides the order of G.

Proof. By Corollary 1.3.4, we see G is the union of the left cosets, which are necessarily disjoint, so $|G|$ is the sum of the cardinalities of the cosets. By Proposition 1.3.7, the cardinalities of the cosets are the same and equal to $|H|$, so

$$|G| = [G : H]|H|.$$ ■

Corollary 1.3.9. Let G be a group and H, K be subgroups of G where $K \subseteq H$. Then,

$$[G : K] = [G : H][H : K].$$

Corollary 1.3.10. Let G be a group, and let $g \in G$. If G is finite, then $\mathrm{ord}(g)$ divides $|G|$. It follows that $g^{|G|} = e$.

Corollary 1.3.11. Let G be a finite group. If $|G|$ is prime, then, G is cyclic; in other words, $G = \langle g \rangle$ for all $g \in G \setminus \{e\}$.

1.4 Normal subgroups

Definition 1.4.1. Let G be a finite group and H be a subgroup of G. If for every $g \in G$, we have $gH = Hg$, i.e. the left and right cosets are the same, then H is called a normal subgroup of G.

Theorem 1.4.2. Let G be a finite group and H be a subgroup of G. Then, H is a normal subgroup of G if and only if for every $g \in G$ and $h \in H$, we have $ghg^{-1} \in H$.

Proof.

($\Rightarrow$) Suppose H is a normal subgroup of G. Then, for all $g \in G$, we have $gH = Hg$, so for all $h \in H$, we have $gh \in Hg$. This means there exists some $k \in H$ such that $gh = kg$, so

$$ghg^{-1} = kgg^{-1} = k.$$

Hence, $ghg^{-1} \in H$.

($\Leftarrow$) Suppose for every $g \in G$ and $h \in H$, we have $ghg^{-1} \in H$. Let $x \in jH$ for some $j \in G$. Then, there exists some $k \in H$ such that

$$x = jk = jk(j^{-1}j) = (jkj^{-1})j \in Hj,$$

so $jH \subseteq Hj$. Similarly, it can be shown that $Hj \subseteq jH$; hence, $jH = Hj$. ∎

Theorem 1.4.3. Let G be a group and H be a normal subgroup of G. Then, G/H can be given a group structure with the composition law

$$\begin{array}{rccc} \oslash : & G/H \times G/H & \to & G/H \\ & (xH, yH) & \mapsto & (xy)H \end{array}.$$

Proof. We have three criteria for $(G/H, \oslash)$ to be a group:

1. Let $x_1, x_2, y_1, y_2 \in G$ such that $x_1H = x_2H$ and $y_1H = y_2H$. Since H is a normal subgroup, for all $h \in H$, there exists some $h' \in H$ such that $y_1h = h'y_2$, so $x_1y_1h = x_1h'y_2$. Similarly, there exists some $h'' \in H$ such that $x_1h' = h''x_2$, so
$$x_1y_1h = x_1h'y_2 = h''x_2y_2.$$
This means that $(x_1y_1)H = H(x_2y_2)$, so since H is a normal subgroup, $(x_1y_1)H = (x_2y_2)H$. Thus, $\oslash$ is well-defined. Associativity follows from the law of composition on G.

2. Since $H = e_GH$, we have, for all $gH \in G/H$,
$$H \oslash gH = e_GH \oslash gH = (e_Gg)H = gH,$$
and, similarly, $gH \oslash H = gH$, so we have the neutral element H.

3. Let $gH \in G/H$. Naturally, the inverse of gH is $g^{-1}H$:
$$(gg^{-1})H = e_GH = H.$$
∎

Solved exercises

Groups

Determine whether the following are groups, and show why or why not.

Exercise 1.1. Consider $(\{1, 0, -1\}, +)$ where $+$ is standard addition.

Solution. Notice $1 + 1 = 2 \notin \{1, 0, -1\}$, so $(\{1, 0, -1\}, +)$ is not a group. □

Exercise 1.2. Consider $(\mathbb{R}, \odot)$ where $\odot$ is defined such that for $x, y \in \mathbb{R}$, we have $x \odot y = xy + (x^2 - 1)(y^2 - 1)$.

Solution. Notice

$$\begin{aligned} 2 \odot (3 \odot 4) &= 2 \odot \big((3)(4) + (3^2 - 1)(4^2 - 1)\big) = 2 \odot 132 \\ &= (2)(132) + (2^2 - 1)(132^2 - 1) = 52\,533, \end{aligned}$$

while

$$\begin{aligned} (2 \odot 3) \odot 4 &= \big((2)(3) + (2^2 - 1)(3^2 - 1)\big) \odot 4 = 30 \odot 4 \\ &= (30)(4) + (30^2 - 1)(4^2 - 1) = 13\,605, \end{aligned}$$

so $\odot$ is not associative. Hence, $(\mathbb{R}, \odot)$ is not a group. □

Exercise 1.3. Consider $(\mathbb{R}^+, \odot)$ where $\odot$ is defined such that for $x, y \in \mathbb{R}^+$, we have $x \odot y = \sqrt{x^2 + y^2}$.

Solution. Notice that for all $x \in \mathbb{R}^+$,

$$x \odot 0 = \sqrt{x^2 + 0^2} = \sqrt{x^2} = x,$$

so 0 is the neutral element under $\odot$; however, $0 \notin \mathbb{R}^+$, so $(\mathbb{R}^+, \odot)$ is not a group. □

Exercise 1.4. Consider $(\mathbb{R} \setminus \{-1\}, \odot)$ where $\odot$ is defined such that for $x, y \in \mathbb{R} \setminus \{-1\}$, we have $x \odot y = x + y + xy$.

Solution. Suppose there exists a pair (x, y) such that $x \odot y = -1$. Then,

$$\begin{aligned} x + y + xy &= -1 \\ y(1 + x) &= -1 - x \\ y &= -\frac{1 + x}{1 + x} \\ y &= -1, \end{aligned}$$

so such a pair cannot be in $(\mathbb{R} \setminus \{-1\}) \times (\mathbb{R} \setminus \{-1\})$; thus, $\odot$ is a law of composition on $\mathbb{R} \setminus \{-1\}$. We also see

$$\begin{aligned}(x \odot y) \odot z = (x + y + xy) \odot z &= (x + y + xy) + z + (x + y + xy)z \\ &= x + y + xy + z + xz + yz + xyz \\ &= x + (y + z + yz) + x(y + z + yz) = x \odot (y + z + yz) \\ &= x \odot (y \odot z),\end{aligned}$$

so $\odot$ is associative. Finally, notice that for all $x \in \mathbb{R} \setminus \{-1\}$, we have

$$x \odot 0 = x + 0 + x(0) = x$$

(neutral element), and

$$\begin{aligned}x \odot -\frac{x}{1+x} &= x - \frac{x}{1+x} + x\left(-\frac{x}{1+x}\right) = x - \frac{x}{1+x} - \frac{x^2}{1+x} \\ &= \frac{x(1+x) - x}{1+x} - \frac{x^2}{1+x} = \frac{x^2}{1+x} - \frac{x^2}{1+x} = 0\end{aligned}$$

(inverse). Hence, $(\mathbb{R} \setminus \{-1\}, \odot)$ is a group. □

Exercise 1.5. Consider $(\mathcal{C}, \cdot)$ where $\mathcal{C} = \{z \in \mathbb{C} \mid |c| = 1\}$ and $\cdot$ is standard multiplication.

Solution. Since $\mathcal{C}$ is the unit circle, we can uniquely represent each $z \in \mathcal{C}$ in polar form as $z = e^{i\theta}$ for some $\theta \in (-\pi, \pi]$, and we know $e^{i\theta} \in \mathcal{C}$ for all $\theta \in \mathbb{R}$. Let $e^{i\theta_1}, e^{i\theta_2} \in \mathcal{C}$. Then,

$$e^{i\theta_1} \cdot e^{i\theta_2} = e^{i\theta_1 + i\theta_2} = e^{i(\theta_1 + \theta_2)} \in \mathcal{C},$$

so standard multiplication is a law of composition on $\mathcal{C}$, and we know standard multiplication is associative. The neutral element under standard multiplication is $1 = e^{i(0)} \in \mathcal{C}$. Finally, notice that for all $e^{i\theta} \in \mathcal{C}$,

$$e^{i\theta} \cdot e^{i(-\theta)} = e^{i\theta - i\theta} = e^0 = 1$$

(inverse). Hence, $(\mathcal{C}, \cdot)$ is a group. □

Exercise 1.6. Consider $(\mathrm{SL}_n(\mathbb{R}), \cdot)$ where $\mathrm{SL}_n(\mathbb{R})$ is the set of all $n \times n$ matrices over $\mathbb{R}$ with determinant 1 and $\cdot$ is standard matrix multiplication.

Solution. Let $A, B \in \mathrm{SL}_n(\mathbb{R})$. Then,

$$\det(AB) = \det(A)\ \det(B) = (1)(1) = 1,$$

so $AB \in \mathrm{SL}_n(\mathbb{R})$. Thus, standard matrix multiplication is a law of composition on $\mathrm{SL}_n(\mathbb{R})$, and we know standard matrix multiplication is associative. The neutral element under standard matrix multiplication is I_n and $\det(I_n) = 1$, so $I_n \in \mathrm{SL}_n(\mathbb{R})$. Finally, taking A^{-1} as the standard matrix inverse, we see

$$\det(A^{-1}) = \frac{1}{\det(A)} = \frac{1}{1} = 1,$$

so $A^{-1} \in \mathrm{SL}_n(\mathbb{R})$. Hence, $(\mathrm{SL}_n(\mathbb{R}), \cdot)$ is a group. $\square$

Exercise 1.7. Consider $(Q, \cdot)$ where $Q = \{\pm I_2, \pm I, \pm J, \pm K\}$,

$$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad I = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \qquad J = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \qquad K = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix},$$

and $\cdot$ is standard matrix multiplication.

Solution. For I_2, I, J, and K, we have the composition table

$\cdot$	I_2	I	J	K
I_2	I_2	I	J	K
I	I	$-I_2$	K	$-J$
J	J	$-K$	$-I_2$	I
K	K	J	$-I$	$-I_2$

and we know for any matrices A and B,

$$(-A)B = A(-B) = -AB \quad \text{and} \quad (-A)(-B) = AB,$$

so standard matrix multiplication is a law of composition on Q. We also know standard matrix multiplication is associative. The neutral element under standard matrix multiplication of 2×2 matrices is $I_2 \in Q$. Finally, from the composition table, we have the inverses

$$I_2^{-1} = I_2 \qquad I^{-1} = -I \qquad J^{-1} = -J \qquad K^{-1} = -K$$

and from these we see

$$(-I_2)^{-1} = -I_2 \qquad (-I)^{-1} = I \qquad (-J)^{-1} = J \qquad (-K)^{-1} = K.$$

Hence, $(Q, \cdot)$ is a group. $\square$

Exercise 1.8. Consider $(H, \cdot)$ where H is the set of upper triangular 3×3 matrices over $\mathbb{R}$ whose diagonal entries are all 1 and $\cdot$ is standard matrix multiplication.

Solution. Let $a, b, c, x, y, z \in \mathbb{R}$. Then,

$$\begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a + x & b + xc + y \\ 0 & 1 & c + z \\ 0 & 0 & 1 \end{bmatrix} \in H,$$

so standard matrix multiplication is a law of composition on H, and we know standard matrix multiplication is associative. The neutral element under standard matrix multiplication of 3×3 matrices is $I_3 \in H$. Finally, computing the standard matrix inverse, we see

$$\begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -x & xz - y \\ 0 & 1 & -z \\ 0 & 0 & 1 \end{bmatrix} \in H.$$

Hence, $(H, \cdot)$ is a group. □

Subgroups

For each of the following, determine whether H is a subgroup of G, and show why or why not.

Exercise 1.9. Let $G = (\mathbb{R}, +)$ and $H = \{-1, 0, 1\}$.

Solution. Notice $1 + 1 = 2 \notin H$. Hence, H is not a subgroup of G. □

Exercise 1.10. Let $G = (\mathbb{R}, +)$ and $H = \mathbb{R} \setminus \{0\}$.

Solution. The neutral element of G is $0 \notin H$. Hence, H is not a subgroup of G. □

Exercise 1.11. Let $G = (\mathbb{C} \setminus \{0\}, \cdot)$ and $H = \mathbb{R} \setminus \{0\}$.

Solution. Let $h_1, h_2 \in H = \mathbb{R} \setminus \{0\}$. Then, since $h_1, h_2 \neq 0$, we have

$$h_1 h_2^{-1} = h_1 \cdot \frac{1}{h_2} = \frac{h_1}{h_2} \in \mathbb{R} \setminus \{0\} = H.$$

Hence, H is a subgroup of G. □

Exercise 1.12. Let $G = (\mathbb{R} \setminus \{0\}, \cdot)$ and $H = \{-1, 1\}$.

Solution. We see

$$(-1)^{-1} = \frac{1}{-1} = -1 \quad \text{and} \quad 1^{-1} = \frac{1}{1} = 1,$$

so

$$\begin{aligned} -1 \cdot (-1)^{-1} &= -1 \cdot -1 = 1 \in H, & -1 \cdot 1^{-1} &= -1 \cdot 1 = -1 \in H, \\ 1 \cdot (-1)^{-1} &= 1 \cdot -1 = -1 \in H, & 1 \cdot 1^{-1} &= 1 \cdot 1 = 1 \in H. \end{aligned}$$

Hence, H is a subgroup of G. □

Exercise 1.13. Let $G = (\mathbb{C} \setminus \{0\}, \cdot)$ and $H = \{e^{i(2\pi k)/n} \mid k \in \{0, 1, \ldots, n-1\}\}$ for some $n \in \mathbb{N}$.

Solution. Let $h_1, h_2 \in H$. Then, $h_1 = e^{i(2\pi k)/n}$ and $h_2 = e^{i(2\pi l)/n}$ for some $k, l \in \{0, 1, \dots, n-1\}$, so

$$h_2^{-1} = \left(e^{i(2\pi l)/n}\right)^{-1} = e^{-i(2\pi l)/n},$$

and we see

$$h_1 h_2^{-1} = e^{i(2\pi k)/n} \cdot e^{-i(2\pi l)/n} = e^{i(2\pi(k-l))/n}.$$

Let $m = (k - l) \bmod n$. Then,

$$h_1 h_2^{-1} = e^{i(2\pi(k-l))/n} = e^{i(2\pi m)/n} \in H.$$

Hence, H is a subgroup of G. □

Exercise 1.14. Let $G = (\mathrm{GL}_n(\mathbb{R}), \cdot)$ where $\mathrm{GL}_n(\mathbb{R})$ is the set of all invertible $n \times n$ matrices over $\mathbb{R}$, and let $H = (\mathrm{SL}_n(\mathbb{R}), \cdot)$.

Solution. Let $A, B \in H = \mathrm{SL}_n(\mathbb{R})$. Then,

$$\det(A) = \det(B) = 1 \neq 0,$$

so A^{-1} and B^{-1} exist and

$$\det(B^{-1}) = \frac{1}{\det(B)} = \frac{1}{1} = 1.$$

Therefore,

$$\det(AB^{-1}) = \det(A)\det(B^{-1}) = 1 \cdot 1 = 1$$

so $AB^{-1} \in H$. Hence, H is a subgroup of G. □

Cyclic groups

Exercise 1.15. Let G be a group, and let $x \in G$ where x is of order k. Prove that if m is an integer such that $x^m = e_G$, then $k \mid m$.

Solution. Since x is of order k, we have by definition that k is the smallest positive integer such that $x^k = e_G$. Suppose $x^m = e_G$ for some $m \in \mathbb{Z}$. We can rewrite m in terms of its Euclidean division by k as $m = kq + r$ for some $q, r \in \mathbb{Z}$ where $0 \leq r < k$, giving us

$$x^m = x^{kq+r} = x^{kq}x^r = (x^k)^q x^r = e_G^q x^r = x^r.$$

so $x^r = e_G$. Since $r < k$ and k is minimal, we must have $r = 0$, so $m = kq$. Hence, $k \mid m$. □

Chapter 2

Relations Between Groups

2.1 Group homomorphisms

Definition 2.1.1. Let $(G, \odot)$ and $(G', \oslash)$ be groups. A mapping $\phi : G \to G'$ is called a group homomorphism if for every $x, y \in G$, we have

$$\phi(x \odot y) = \phi(x) \oslash \phi(y).$$

Definition 2.1.2. A group homomorphism is called an isomorphism if it is a bijection. A group G is called isomorphic to a group G' if there exists an isomorphism $\phi : G \to G'$. We denote this by $G \simeq G'$.

Proposition 2.1.3. Let $\phi : (G, \odot) \to (G', \oslash)$ be a homomorphism. Then,

1. $\phi(e_G) = e_{G'}$; and
2. for all $g \in G$, we have $\phi(g^{-1}) = (\phi(g))^{-1}$.

Proof.

1. By definition, for all $x \in G'$, we have $x \oslash (x)^{-1} = (x)^{-1} \oslash x = e_{G'}$. In particular,
$$e_{G'} = \phi(e_G) \oslash (\phi(e_G))^{-1} = (\phi(e_G))^{-1} \oslash \phi(e_G).$$
Since ϕ is a homomorphism, we also have
$$\begin{aligned} \phi(e_G) &= \phi(e_G \odot e_G) \\ \phi(e_G) &= \phi(e_G) \oslash \phi(e_G) \\ \phi(e_G) \oslash (\phi(e_G))^{-1} &= \phi(e_G) \oslash \phi(e_G) \oslash (\phi(e_G))^{-1} \\ e_{G'} &= \phi(e_G) \oslash e_{G'} \\ e_{G'} &= \phi(e_G). \end{aligned}$$

2. By definition, $(\phi(g))^{-1}$ is the inverse of $\phi(g)$ in G'. We see
$$\phi(g^{-1}) \oslash \phi(g) = \phi(g^{-1} \odot g) = \phi(e_G) = e'_G,$$

so $\phi(g^{-1})$ is also the inverse of $\phi(g)$ in G'. Hence, by uniqueness of the inverse,

$$\phi(g^{-1}) = (\phi(g))^{-1}. \qquad \blacksquare$$

Definition 2.1.4. Let $\phi : G \to G'$ be a homomorphism. The set

$$\mathrm{im}(\phi) = \{\phi(g) \mid g \in G\}$$

is called the image of ϕ.

Proposition 2.1.5. Let $\phi : G \to G'$ be a homomorphism. Then, $\mathrm{im}(\phi)$ is a subgroup of G'.

Proof. Let $x, y \in \mathrm{im}(\phi)$. Then, there exist some $u, v \in G$ such that $\phi(u) = x$ and $\phi(v) = y$, so

$$xy^{-1} = \phi(u)(\phi(v))^{-1} = \phi(u)\,\phi(v^{-1}) = \phi(uv^{-1}).$$

Since $uv^{-1} \in G$, we see $xy^{-1} \in \mathrm{im}(\phi)$. Hence, $\mathrm{im}(\phi)$ is a subgroup of G'. $\blacksquare$

Definition 2.1.6. Let $\phi : G \to G'$ be a homomorphism. The set

$$\ker(\phi) = \{g \in G \mid \phi(g) = e_{G'}\}$$

is called the kernel of ϕ.

Theorem 2.1.7. Let $\phi : G \to G'$ be a homomorphism. Then, ϕ is injective if and only if $\ker(\phi) = \{e_G\}$.

Proof.

($\Rightarrow$) Suppose ϕ is injective. Since $\phi(e_G) = e_{G'}$, we know $\{e_G\} \subseteq \ker(\phi)$. Let $x \in \ker(\phi)$. Then, $\phi(x) = e_{G'} = \phi(e_G)$, so since ϕ is injective, $x = e_G$, which implies $\ker(\phi) \subseteq \{e_G\}$. Hence, $\{e_G\} = \ker(\phi)$.

($\Leftarrow$) Suppose $\ker(\phi) = \{e_G\}$. Let $x, y \in G$ such that $\phi(x) = \phi(y)$. Then,

$$e_{G'} = \phi(x)(\phi(x))^{-1} = \phi(y)(\phi(x))^{-1} = \phi(y)\,\phi(x^{-1}) = \phi(yx^{-1}).$$

Thus, $yx^{-1} \in \ker(\phi)$, so $yx^{-1} = e_G$, which implies $y = x$. Hence, ϕ is injective. $\blacksquare$

Theorem 2.1.8. Let $\phi : G \to G'$ be a homomorphism. Then, $\ker(\phi)$ is a normal subgroup of G.

Proof. Let $g \in G$ and $x \in \ker(\phi)$. Then, $\phi(x) = e_{G'}$, so

$$\phi(gxg^{-1}) = \phi(g)\phi(x)\phi(g^{-1}) = \phi(g)e_{G'}(\phi(g))^{-1} = \phi(g)(\phi(g))^{-1} = e_{G'}. \qquad \blacksquare$$

Theorem 2.1.9. Let G be a group and H be a subgroup of G. Then, H is a normal subgroup of G if and only if there exists a surjective homomorphism $\phi : G \to G'$ for some group G' such that $H = \ker(\phi)$.

Proof. Suppose H is a normal subgroup of G. Consider the mapping

$$\begin{array}{rccc} \phi: & G & \to & G/H \\ & g & \mapsto & gH \end{array}$$

where G/H has group structure as given in Theorem 1.4.3. Let $x, y \in G$. We see

$$\phi(xy) = (xy)H = xHyH = \phi(x)\phi(y),$$

so ϕ is a homomorphism, surjective by construction. Now let $k \in \ker(\phi)$. Since H is the neutral element of G/H, this means $\phi(k) = kH = H$, which is true if and only if $k \in H$. Hence, $\ker(\phi) = H$. The converse is a direct consequence of Theorem 2.1.8. ∎

Theorem 2.1.10. Let $\phi : G \to G'$ be an isomorphism. Then, ϕ^{-1} is an isomorphism.

Proof. Let $\odot$ denote the law of composition for group G and $\oslash$ denote the law for G', let $f = \phi^{-1}$, and let $x, y \in G'$. f is clearly well-defined, and we see

$$\phi(f(x) \odot f(y)) = \phi(f(x)) \oslash \phi(f(y)) = x \oslash y = \phi(f(x \oslash y)).$$

Since ϕ is injective, this implies $f(x) \odot f(y) = f(x \oslash y)$, so f is a homomorphism. Injectivity and surjectivity can be easily verified. Hence, f is an isomorphism. ∎

Theorem 2.1.11 (Fundamental theorem on homomorphisms)**.** Let $\phi : G \to G'$ be a homomorphism. Then, the mapping

$$\begin{array}{rccc} \psi: & G/\ker(\phi) & \to & \mathrm{im}(\phi) \\ & g\ker(\phi) & \mapsto & \phi(g) \end{array}$$

is an isomorphism.

Proof. We have four criteria for ψ to be an isomorphism:

1. Let g, h be such that $g\ker(\phi) = h\ker(\phi)$. Then, $h^{-1}g \in \ker(\phi)$, so

$$\begin{aligned} \phi(h^{-1}g) &= e_{G'} \\ (\phi(h))^{-1}\phi(g) &= e_{G'} \\ \phi(g) &= \phi(h). \end{aligned}$$

   Thus, ψ is well-defined.

2. Let $g\ker(\phi), h\ker(\phi) \in G/\ker(\phi)$. Then,

$$\begin{aligned} \psi(g\ker(\phi)\, h\ker(\phi)) &= \psi((gh)\ker(\phi)) = \phi(gh) = \phi(g)\,\phi(h) \\ &= \psi(g\ker(\phi))\,\psi(h\ker(\phi)), \end{aligned}$$

   so ψ is a homomorphism.

3. Let $g \ker(\phi) \in \ker(\psi)$. Then, $\psi(g \ker(\phi)) = e_{G'}$, so $g \in \ker(\phi)$, which implies $g \ker(\phi) = \ker(\phi)$. Thus, by Theorem 2.1.7, ψ is injective.
4. ψ is surjective by construction since it maps to $\operatorname{im}(\phi)$. ∎

This theorem is also known as the first isomorphism theorem.

2.2 Permutation groups

Proposition 2.2.1. Let X be a set, and let $\mathcal{S}(X)$ be the set of all bijections from X to X. Then, $(\mathcal{S}(X), \circ)$, where $\circ$ is composition of mappings, is a group.

Proof. We have three criteria for $(\mathcal{S}(X), \circ)$ to be a group:

1. Let $\sigma, \tau \in \mathcal{S}(X)$. Then, $\sigma \circ \tau$ is a mapping from X to X. Let $x, y \in X$ such that $(\sigma \circ \tau)(x) = (\sigma \circ \tau)(y)$. Then, since σ and τ are injective, we have

$$\begin{aligned} \sigma(\tau(x)) &= \sigma(\tau(y)) \\ \tau(x) &= \tau(y) \\ x &= y, \end{aligned}$$

so $\sigma \circ \tau$ is injective, and any injective mapping from a set to itself is also surjective. Thus, $\sigma \circ \tau \in \mathcal{S}(X)$, and we know composition of mappings is associative.

2. The neutral element is naturally the identity mapping id:

$$(\sigma \circ \mathrm{id})(x) = \sigma(\mathrm{id}(x)) = \sigma(x) = \mathrm{id}(\sigma(x)) = (\mathrm{id} \circ \sigma)(x).$$

3. Since every $\sigma \in \mathcal{S}(X)$ is injective, every σ has an inverse mapping. ∎

Definition 2.2.2. Take $\mathcal{S}(X)$ as defined in Proposition 2.2.1 for some set X. A subgroup of $\mathcal{S}(X)$ is called a permutation group. Any mapping in such a group is called a permutation.

Theorem 2.2.3 (Cayley's theorem)**.** Every group is isomorphic to a permutation group.

Proof. Let G be a group. For each $a \in G$, we define a mapping

$$\sigma_a : \begin{array}{ccc} G & \to & G \\ g & \mapsto & ag \end{array}.$$

For some $b \in G$, let $x, y \in G$ such that $\sigma_b(x) = \sigma_b(y)$. Then, $bx = by$, so left cancellation implies $x = y$. Thus, σ_b is injective, and any injective mapping from a set to itself is also surjective, so $\sigma_b \in \mathcal{S}(G)$.

Now, we define a mapping

$$\begin{array}{rccc} \phi: & G & \to & \mathcal{S}(G) \\ & g & \mapsto & \sigma_g \end{array}.$$

Let $a, b \in G$. Then, for all $x \in G$, we have

$$\phi(ab)(x) = \sigma_{ab}(x) = abx = a\sigma_b(x) = \sigma_a(\sigma_b(x)) = \phi(a)\circ\phi(b),$$

so ϕ is a homomorphism. If $a \in \ker(\phi)$, then $\phi(a) = \sigma_a = \mathrm{id}$, which is true if and only if for all $x \in G$, we have

$$\phi(a)(x) = \sigma_a(x) = ax = x \iff a = e_G.$$

Thus, $\ker(\phi) = \{e_G\}$, so ϕ is injective. By Proposition 2.1.5, $\mathrm{im}(\phi)$ is a subgroup of $\mathcal{S}(X)$; hence, we can construct an isomorphism $\psi : G \to \mathrm{im}(\phi)$. ■

Definition 2.2.4. Let $A = \{1, 2, \dots, n\}$ for some $n \in \mathbb{N}$. Then, $\mathcal{S}_n = \mathcal{S}(A)$ is called the symmetric group on n elements.

More generally, $\mathcal{S}_n$ can be used to describe the group of permutations of any finite set. Since any finite set is isomorphic to a subset of $\mathbb{N}$, we can apply this definition by assigning a label in A to each element. The results we will show for $\mathcal{S}_n$ therefore apply with this generalization as well.

Note that for any $n \in \mathbb{N}$, we have $|\mathcal{S}_n| = n!$. This may be familiar if you recall the notion of a permutation of a set as a rearrangement of its elements. The notation may also be familiar—consider the following permutation $\sigma \in \mathcal{S}_5$:

$$\begin{aligned} 1 &\mapsto 3 \\ 2 &\mapsto 2 \\ 3 &\mapsto 5 \\ 4 &\mapsto 4 \\ 5 &\mapsto 1. \end{aligned}$$

This can be written as

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}.$$

Definition 2.2.5. Let $\sigma = \mathcal{S}_n$. The set

$$\mathrm{supp}(\sigma) = \{i \in \{1, 2, \dots, n\} \mid \sigma(i) \neq i\}$$

is called the support of σ.

Proposition 2.2.6. Let $\sigma, \tau \in \mathcal{S}_n$. If $\mathrm{supp}(\sigma) \cap \mathrm{supp}(\tau) = \varnothing$, then $\sigma\circ\tau = \tau\circ\sigma$.

Proof. Let $i \in \{1, 2, \dots, n\}$. We have three cases:

1. Suppose $i \notin \operatorname{supp}(\sigma) \cup \operatorname{supp}(\tau)$. Then, $\sigma(i) = \tau(i) = i$, so

$$(\sigma \circ \tau)(i) = \sigma(\tau(i)) = \sigma(i) = i = \tau(i) = \tau(\sigma(i)) = (\tau \circ \sigma)(i).$$

2. Suppose $i \in \operatorname{supp}(\sigma)$. Then, $i \notin \operatorname{supp}(\tau)$, so

$$(\sigma \circ \tau)(i) = \sigma(\tau(i)) = \sigma(i),$$

and since $i \in \operatorname{supp}(\sigma)$, we have $\sigma(i) \in \operatorname{supp}(\sigma)$, so $\sigma(i) \notin \operatorname{supp}(\tau)$. Thus,

$$(\tau \circ \sigma)(i) = \tau(\sigma(i)) = \sigma(i) = (\sigma \circ \tau)(i).$$

3. If $i \in \operatorname{supp}(\tau)$, the proof can be done in the same way as in the above case.

Hence, $\sigma \circ \tau = \tau \circ \sigma$. ■

Cycles

Definition 2.2.7. An element $\sigma \in \mathcal{S}_n$ is called a cycle if there exists some $x \in \{1, 2, \dots, n\}$ such that $\operatorname{supp}(\sigma) = \{\sigma^i(x) \mid i \in \mathbb{N}\}$. Let $l = |\operatorname{supp}(\sigma)|$. We denote the cycle

$$\left(x, \sigma(x), \dots, \sigma^{l-1}(x)\right)$$

where l is called its length. A cycle of length 2 is called a transposition.

Proposition 2.2.8. Let σ be a cycle of length l. Then, $\operatorname{ord}(\sigma) = l$.

This follows by construction.

Proposition 2.2.9. Let $\sigma \in \mathcal{S}_n$, and let $A = \{1, 2, \dots, n\}$. Then, the relation $\sim$ on A defined such that for all $a, b \in A$,

$$a \sim b \iff \text{there exists some } k \in \mathbb{Z} \text{ such that } b = \sigma^k(a)$$

is an equivalence relation.

Proof. We have three criteria for $\sim$ to be an equivalence relation:

1. Since $a = \sigma^0(a)$, we have $a \sim a$ (reflexive).
2. Suppose $a \sim b$. Then, $b = \sigma^k(a)$ for some $k \in \mathbb{Z}$, so $a = \sigma^{-k}(b)$. Thus, $b \sim a$ (symmetric).
3. Let $c \in A$. Suppose $a \sim b$ and $b \sim c$. Then, $b = \sigma^k(a)$ and $c = \sigma^m(b)$ for some $k, m \in \mathbb{Z}$, so $c = \sigma^m(\sigma^k(a)) = \sigma^{m+k}(a)$. Thus, $a \sim c$ (transitive). ■

Corollary 2.2.10 (Alternative definition of a cycle)**.** Take $\sim$ as defined in Proposition 2.2.9 for some $\sigma \in \mathcal{S}_n$. Then, σ is a cycle if and only if $\sim$ has at most one equivalence class containing more than one element.

Theorem 2.2.11. Let $\sigma \in \mathcal{S}_n$. Then, there exist some unique cycles $\tau_1, \tau_2, \dots, \tau_k$ with disjoint supports such that $\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_k$. In other words, every permutation of a finite set can be decomposed as the product of unique cycles with disjoint supports.

Proof. Let $A_1, A_2, \dots, A_k$ be the equivalence classes of $\sim$, and let $\tau_1, \tau_2, \dots, \tau_k$ be the cycles defined such that

$$\tau_i(x) = \begin{cases} \sigma(x), & x \in A_i \\ x, & \text{otherwise.} \end{cases}$$

We see $\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_k$, and since $A_1, A_2, \dots, A_k$ are necessarily disjoint, $\tau_1, \tau_2, \dots, \tau_k$ have disjoint supports. ■

Definition 2.2.12. Let $\sigma \in \mathcal{S}_n$ with decomposition $\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_k$ as given by Theorem 2.2.11. Let $l_1, l_2, \dots, l_k$ denote the lengths of $\tau_1, \tau_2, \dots, \tau_k$, respectively, where $l_1 \geq l_2 \geq \cdots \geq l_k$. The sequence $(l_1, l_2, \dots, l_k)$ is called the type of σ.

Proposition 2.2.13. Let $\sigma \in \mathcal{S}_n$ with type $(l_1, l_2, \dots, l_k)$. Then,

$$\operatorname{ord}(\sigma) = \operatorname{lcm}\{l_1, l_2, \dots, l_k\}.$$

Proof. We can decompose σ into cycles as $\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_k$ where $\tau_1, \tau_2, \dots, \tau_k$ have length $l_1, l_2, \dots, l_k$, respectively. Since the τ_is have disjoint supports, they commute, so for every $m \in \mathbb{N}$, we have

$$\sigma^m = \tau_1^m \circ \tau_2^m \circ \cdots \circ \tau_k^m.$$

Since $\operatorname{ord}(\tau_i) = l_i$ for $1 \leq i \leq k$, we see that if $\sigma^m = \mathrm{id}$, then m is a multiple of each of the l_is. Hence, by definition, $\operatorname{ord}(\sigma)$ is the lowest such m. ■

Transpositions and alternating groups

Corollary 2.2.14 (to Theorem 2.2.11)**.** Every permutation in $\mathcal{S}_n$ can be decomposed as the product of transpositions.

Proposition 2.2.15. Let $\sigma \in \mathcal{S}_n$. Either all transposition decompositions of σ are the product of an even number of transpositions, or all of them are the product of an odd number of transpositions.

Proof. Consider the group of permutations of the rows of the $n \times n$ identity matrix I_n. Let us call this group P. As remarked following Definition 2.2.4, $P \simeq \mathcal{S}_n$. We know $\det(I_n) = 1$, and transposing any two rows of a square matrix changes the sign of its determinant.

Let $\rho \in P$, and let $A = \rho(I_n)$. Suppose ρ can be decomposed as an even number of transpositions. Then, $\det(A) = 1$. Now suppose ρ can also be decomposed as an odd number of transpositions. Then, $\det(A) = -1$, a contradiction. Hence, no

$\rho \in P$ can be decomposed into the product of both an even number and an odd number of transpositions. ∎

Definition 2.2.16. Let $\sigma \in \mathcal{S}_n$, and let k be the number of transpositions in some transposition decomposition of σ. The number $\epsilon(\sigma) = (-1)^k$ is called the signature of σ. The permutation σ is called even if k is even or odd if k is odd.

Proposition 2.2.17. Let $\mathcal{A}_n = \{\sigma \in \mathcal{S}_n \mid \epsilon(\sigma) = 1\}$. Then, $\mathcal{A}_n$ is a normal subgroup of $\mathcal{S}_n$.

Proof. Let $\alpha \in \mathcal{A}_n$ and $\sigma \in \mathcal{S}_n$. For some $k, m \in \mathbb{N}$, α can be decomposed as the product of some number $2k$ of transpositions and σ can be decomposed as the product of some number m of transpositions, so there exists a decomposition of $\sigma \circ \alpha \circ \sigma^{-1}$ into some number $m + 2k + m = 2(m+k)$ of transpositions. Since $2(m+k)$ is even, $\sigma \circ \alpha \circ \sigma^{-1} \in \mathcal{A}_n$. Hence, by Theorem 1.4.2, $\mathcal{A}_n$ is a normal subgroup of $\mathcal{S}_n$. ∎

We can alternatively show that the mapping

$$\begin{array}{rccc} \epsilon : & (\mathcal{S}_n, \circ) & \to & (\{-1, 1\}, \cdot) \\ & \sigma & \mapsto & \epsilon(\sigma) \end{array}$$

is a group homomorphism and that $\mathcal{A}_n = \ker(\epsilon)$. By Theorem 2.1.8, this implies $\mathcal{A}_n$ is a normal subgroup of $\mathcal{S}_n$.

Definition 2.2.18. $\mathcal{A}_n$ as defined in Proposition 2.2.17 is called the alternating group on n elements.

2.3 Finitely generated abelian groups

Recall the Cartesian product of two sets A and B:

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

We can give group structure to the Cartesian product of an arbitrary number of groups.

Proposition 2.3.1. Let G_1 and G_2 be two groups. The set $G_1 \times G_2$ together with the law of composition

$$\begin{array}{rccc} \odot : & (G_1 \times G_2) \times (G_1 \times G_2) & \to & G_1 \times G_2 \\ & ((a_1, a_2), (b_1, b_2)) & \mapsto & (a_1 b_1, a_2 b_2) \end{array}$$

is a group.

Proof. We have three criteria for $(G_1 \times G_2, \odot)$ to be a group:

1. Let $(a_1, a_2), (b_1, b_2), (c_1, c_2) \in G_1 \times G_2$. Then,

$$\begin{aligned}((a_1, a_2) \odot (b_1, b_2)) \odot (c_1, c_2) &= (a_1 b_1, a_2 b_2) \odot (c_1, c_2)\\ &= ((a_1 b_1) c_1, (a_2 b_2) c_2)\\ &= (a_1 (b_1 c_1), a_2 (b_2 c_2))\\ &= (a_1, a_2) \odot (b_1 c_1, b_2 c_2)\\ &= (a_1, a_2) \odot ((b_1, b_2) \odot (c_1, c_2)),\end{aligned}$$

so $\odot$ is associative.

2. Let e_1 be the neutral element of G_1 and e_2 be the neutral element of G_2. Naturally, the neutral element of $G_1 \times G_2$ is then (e_1, e_2):

$$(a_1, a_2) \odot (e_1, e_2) = (a_1 e_1, a_2 e_2) = (a_1, a_2).$$

3. Naturally, the inverse of (a_1, a_2) is (a_1^{-1}, a_2^{-1}):

$$(a_1, a_2) \odot (a_1^{-1}, a_2^{-1}) = (a_1 a_2^{-1}, a_2 a_2^{-1}) = (e_1, e_2). \qquad \blacksquare$$

Corollary 2.3.2. Let $\{G_i\}_{i \in I}$ be a family of groups for some non-empty (perhaps infinite) index set I. The set

$$\prod_{i \in I} G_i = \{(g_i)_{i \in I} \mid g_i \in G_i \text{ for all } i \in I\},$$

where $(g_i)_{i \in I}$ denotes the sequence of g_is as a touple, together with the law of composition $\odot$ defined such that for all $(g_i)_{i \in I}, (h_i)_{i \in I} \in \{G_i\}_{i \in I}$, we have

$$(g_i)_{i \in I} \odot (h_i)_{i \in I} = (g_i h_i)_{i \in I}$$

is a group.

Corollary 2.3.3. Let $\{G_i\}_{i \in I}$ be a family of abelian groups for some non-empty index set I. The set

$$\bigoplus_{i \in I} G_i = \{(g_i)_{i \in I} \mid g_i \in G_i \text{ for all } i \in I, g_i \neq e_i \text{ for only finitely many } i \in I\},$$

where e_i denotes the neutral element of group G_i, together with the law of composition $\odot$ given in Corollary 2.3.2, is a group. Furthermore, $\bigoplus_{i \in I} G_i = \prod_{i \in I} G_i$ when I is finite; otherwise, $\bigoplus_{i \in I} G_i$ is a proper subgroup of $\prod_{i \in I} G_i$.

Definition 2.3.4. Let $\{G_i\}_{i \in I}$ be a family of groups for some non-empty index set I. The group $\prod_{i \in I} G_i$ from Corollary 2.3.2 is called the direct product of the G_is.

If the G_is are abelian, the group $\bigoplus_{i \in I} G_i$ from Corollary 2.3.3 is called the direct sum of the G_is.

For a finite family of groups $\{G_1, G_2, \ldots, G_n\}$, we can denote their direct sum as

$$G_1 \oplus G_2 \oplus \cdots \oplus G_n.$$

2.4 Group action on a set

2.5 Sylow's theorem (?)

Solved exercises

Group homomorphisms

We define the mapping

$$\begin{array}{rrcl} f: & (\mathbb{R},+) & \to & (\mathbb{C}\setminus\{0\},\cdot) \\ & x & \mapsto & e^{i(2\pi x)} \end{array}$$

where $(\mathbb{R},+)$ and $(\mathbb{C}\setminus\{0\},\cdot)$ are presumed to be groups (this can be shown).

Exercise 2.1. Show that f is a group homomorphism.

Solution. Let $x, y \in \mathbb{R}$. Then,

$$f(x+y) = e^{i(2\pi(x+y))} = e^{i(2\pi x)+i(2\pi y)} = e^{i(2\pi x)} \cdot e^{i(2\pi y)} = f(x)\cdot f(y)$$

so f is a group homomorphism. $\square$

Exercise 2.2. Find $\ker(f)$.

Solution. We know $e_{\mathbb{C}} = 1$, so

$$\ker(f) = \{x \in \mathbb{R} \mid e^{i(2\pi x)} = 1\} = \mathbb{Z}.$$ $\square$

Exercise 2.3. Find $\operatorname{im}(f)$.

Solution. By definition, we have

$$\operatorname{im}(f) = \{e^{i(2\pi x)} \in \mathbb{C}\setminus\{0\} \mid x \in \mathbb{R}\} = \{z \in \mathbb{C} \mid |z| = 1\},$$

which is the complex unit circle group, often denoted $\mathbb{T}$. $\square$

Exercise 2.4. Construct an isomorphism from f using the fundamental theorem on homomorphisms.

Solution. We define

$$\begin{array}{rrcl} \psi: & (\mathbb{R},+)/\ker(f) & \to & \operatorname{im}(f) \\ & x\ker(f) & \mapsto & f(x) \end{array} \equiv \begin{array}{rcl} (\mathbb{R},+)/\mathbb{Z} & \to & \mathbb{T} \\ x\mathbb{Z} & \mapsto & e^{i(2\pi x)} \end{array}.$$ $\square$

Isomorphisms

Let G be a group. For each $a \in G$, we define the mapping

$$f_a : \begin{array}{ccc} G & \to & G \\ x & \mapsto & axa^{-1} \end{array}.$$

Exercise 2.5. Show that f_a is an isomorphism.

Solution. Let $x, y \in G$. Then,

$$f_a(xy) = a(xy)a^{-1} = ax(a^{-1}a)ya^{-1} = (axa^{-1})(aya^{-1}) = f_a(x)f_a(y),$$

so f_a is a group homomorphism. Additionally, for every z in the codomain G, we have $z = f_a(a^{-1}za)$, so f_a is surjective, and any surjective mapping between two sets of the same cardinality is also injective. Hence, f_a is an isomorphism. □

Exercise 2.6. Show that for all $x \in G$, we have $\mathrm{ord}(f_a(x)) = \mathrm{ord}(x)$.

Solution. Let $n = \mathrm{ord}(x)$. Then, n is the minimal positive integer such that

$$\begin{aligned} x^n &= e_G \\ ax^na^{-1} &= ae_Ga^{-1} \\ ax^na^{-1} &= aa^{-1} \\ f_a(x^n) &= e_G. \end{aligned}$$

Since f_a is a homomorphism, $f_a(x^n) = (f_a(x))^n$. Hence, $\mathrm{ord}(f_a(x)) = n$. □

The dihedral group

Let p be a prime number greater than or equal to 3, and let G be a group of cardinality $2p$.

Exercise 2.7. What can we say if G has an element of order $2p$?

Solution. Let $g \in G$ such that $\mathrm{ord}(g) = 2p$. Then, since $\langle g \rangle \subseteq G$ and

$$|\langle g \rangle| = \mathrm{ord}(g) = 2p = |G|,$$

we see $G = \langle g \rangle$. Hence, G is a cyclic group. □

Now assume G has no element of order $2p$.

Exercise 2.8. Show that G has an element of order p.

Solution. Let H be a subgroup of G. By Lagrange's theorem, $|H|$ divides $|G|$, so $|H| \in \{1, 2, p, 2p\}$. Let $g \in G \setminus \{e\}$. Since $\langle g \rangle$ is a subgroup of G and since, by assumption, $\operatorname{ord}(g) \neq 2p$, we see $\operatorname{ord}(g) \in \{2, p\}$.

Suppose G does not have an element of order p. Then, for all $x, y \in G \setminus \{e\}$, we have $\operatorname{ord}(x) = \operatorname{ord}(y) = 2$, so $x^2 = y^2 = e$. Thus,

$$\begin{aligned}(xy)(xy) &= e\\ xyxyy &= ey\\ xyx &= y\\ xxyx &= xy\\ yx &= xy,\end{aligned}$$

so G is abelian. We therefore have that $\{e, x, y, xy\}$ is a subgroup of G of order 4, a contradiction. Hence, G has an element of order p. □

Exercise 2.9. Let $a \in G$ such that $\operatorname{ord}(a) = p$, let H be the subgroup of G generated by a, and let $b \in G \setminus H$. Show that

$$G = \{e, a, a^2, \dots, a^{p-1}, b, ba, ba^2, \dots, ba^{p-1}\}.$$

Solution. Since $b \notin H$, we see

$$H = \langle a \rangle = \{e, a, a^2, \dots, a^{p-1}\} \quad \text{and} \quad bH = \{b, ba, ba^2, \dots, ba^{p-1}\}$$

are cosets of H in G, each of cardinality p. Since the cosets are disjoint, we have $|H \cup bH| = 2p = |G|$, so

$$G = H \cup bH = \{e, a, a^2, \dots, a^{p-1}, b, ba, ba^2, \dots, ba^{p-1}\}.$$ □

Exercise 2.10. Show that $b^2 = e$.

Solution. We have shown that for every $g \in G$, we have $g \in H$ or $g \in bH$. Since $b \notin H$, there does not exist any $n \in \mathbb{Z}$ such that $a^n = b$. Suppose $b^2 \in bH$. Then, there exists some $n \in \mathbb{Z}$ such that

$$\begin{aligned}b^2 &= ba^n\\ bb &= ba^n\\ b^{-1}bb &= b^{-1}ba^n\\ b &= a^n,\end{aligned}$$

a contradiction. Thus, $b^2 \in H$, so there exists some $m \in \mathbb{Z}$ such that $b^2 = a^m$.

We have also shown that for every $g \in G \setminus \{e\}$, we have $\operatorname{ord}(g) = 2$ or $\operatorname{ord}(g) = p$. Suppose $\operatorname{ord}(b) = p$. Then, $b^p = e$. By Bézout's theorem, since $\gcd(2, p) = 1$, there exist some $k, l \in \mathbb{Z}$ such that $2k + pl = 1$. Thus,

$$b = b^1 = b^{2k+pl} = b^{2k}\, b^{pl} = (b^2)^k (b^p)^l = (b^2)^k = (a^m)^l = a^{mk},$$

a contradiction. Hence, $\operatorname{ord}(b) = 2$. □

Exercise 2.11. Show that $ab = ba^{p-1}$.

Solution. We have shown that for every $g \in G \setminus H$, we have $g^2 = e$. Thus,

$$\begin{aligned} (ba^{p-1})^2 &= e \\ ba^{p-1}ba^{p-1} &= e \\ ba^{p-1}ba^{p} &= a \\ ba^{p-1}be &= a \\ ba^{p-1}bb &= ab \\ ba^{p-1} &= ab. \end{aligned}$$ □

Exercise 2.12. We define the dihedral group $\mathcal{D}_n$ as the group of symmetries of the regular n-gon, consisting of n rotations of angle $2\pi k/n$ for $k \in \{0, 1, \dots, n-1\}$ and n reflections about the lines intersecting its center and each vertex. It can be shown that for any rotation $r \in \mathcal{D}_n$ and any reflection $s \in \mathcal{D}_n$, r and s generate $\mathcal{D}_n$; that is,

$$\mathcal{D}_n = \{\mathrm{id}, r, r^2, \dots, r^{n-1}, sr, sr^2, \dots, sr^{n-1}\}.$$

Show that $G \simeq \mathcal{D}_p$.

Solution. Let r be a rotation in $\mathcal{D}_p$, and let s be a reflection in $\mathcal{D}_p$. Consider the mapping $\phi : G \to \mathcal{D}_p$ such that for all $n \in \mathbb{Z}$,

$$\phi(a^n) = r^n, \qquad \phi(ba^n) = sr^n.$$

Let $n, m \in \mathbb{Z}$. Any composition of elements in G is of one of the following forms:

$$\begin{aligned} a^n a^m &= a^{n+m}, \\ a^n ba^m &= (a^{n-1}a)ba^m = a^{n-1}(ba^{p-1})a^m = a^{n-1}ba^{p-1+m} = \cdots = ba^{n(p-1)+m}, \\ ba^n a^m &= ba^{n+m}, \\ ba^n ba^m &= b(ba^{n(p-1)+m}) = a^{n(p-1)+m}. \end{aligned}$$

Thus, ϕ is well-defined, and it can be shown through straightforward computations that for all $x, y \in G$, we have $\phi(xy) = \phi(x)\phi(y)$, so ϕ is a homomorphism.

Since every element of G maps to a unique element in $\mathcal{D}_p$, we see ϕ is injective. Additionally, since

$$\mathcal{D}_p = \{\mathrm{id}, r, r^2, \dots, r^{p-1}, sr, sr^2, \dots, sr^{p-1}\},$$

we see each element of $\mathcal{D}_p$ is reached by some element of G, so ϕ is surjective. Hence, ϕ is an isomorphism. □

Chapter 3

Rings and Fields

3.1 Rings

Definition 3.1.1. Let R be a set, and let $+$ and $\cdot$ be two laws of composition on R. The triple $(R, +, \cdot)$ is called a ring if

1. $(R, +)$ is an abelian group;
2. $\cdot$ is associative; and
3. $\cdot$ is distributive over $+$, i.e. for all $x, y, z \in R$, we have

$$(x + y) \cdot z = x \cdot z + y \cdot z \quad \text{and} \quad z \cdot (x + y) = z \cdot x + z \cdot y.$$

Let $(R, +, \cdot)$ be a ring, and let $a, b \in R$. For the neutral element of R under $+$, we will use the notation 0 or 0_R; for the inverse of a under $+$, we will use the notation $-a$; and for the composition $a \cdot b$, we will use the notation ab. We will also assume the conventional order of operations, i.e. that $\cdot$ comes before $+$.

Proposition 3.1.2. Let $(R, +, \cdot)$ be a ring. Then,

1. for all $a \in R$, we have $a(0) = 0a = 0$; and
2. for all $a, b \in R$, we have

$$a(-b) = (-a)b = -(ab) \quad \text{and} \quad (-a)(-b) = ab.$$

Proof.

1. We can rewrite 0 as $0 + 0$ and use the distributive property:

$$\begin{aligned} a(0) &= a(0 + 0) & 0a &= (0 + 0)a \\ a(0) &= a(0) + a(0) & 0a &= 0a + 0a \\ a(0) - (a(0)) &= a(0) + a(0) - (a(0)) & 0a - (0a) &= 0a + 0a - (0a) \\ 0 &= a(0) & 0 &= 0a. \end{aligned}$$

2. Note that for any $x, y \in R$, we have $x = y$ if and only if $x - y = 0$. Thus, since

$$a(-b) + (ab) = a(-b + b) = a(0) = 0,$$

we have $a(-b) = -(ab)$. Similarly, we can show $(-a)b = (-ab)$. By substitution, we then see

$$(-a)(-b) - (ab) = (-a)(-b) + a(-b) = (-a + a)(-b) = 0(-b) = 0,$$

so $(-a)(-b) = ab$. ■

Definition 3.1.3. A ring $(R, +, \cdot)$ is called

1. commutative if $\cdot$ is commutative;
2. a ring with identity if there exists some $u \in R$ such that for every $a \in R$, we have $au = ua = a$; or
3. an integral domain if it is a commutative ring with identity and for all $a, b \in R$, if $ab = 0$, then $a = 0$ or $b = 0$.

As with groups, we will also typically denote a ring $(R, +, \cdot)$ simply by its set R. We will also denote the element $u \in R$ from Definition 3.1.3 by 1 or 1_R.

Proposition 3.1.4. Let R be a ring with identity. Then,

1. the element $1 \in R$ is unique; and
2. if there exist $b, c \in R$ such that $ab = ca = 1$ for some $a \in R$, then $b = c$.

Proof.

1. Suppose there exist $u, v \in R$ such that for every $a \in R$, we have $au = ua = a$ and $av = va = a$. Then, in particular, $u = uv = v$.
2. By the associative property, we see

$$b = 1b = (ca)b = c(ab) = c(1) = c.$$ ■

Definition 3.1.5. Let R be a commutative ring with identity. An element $a \in R\setminus\{0\}$ is called a zero divisor if there exists some $b \in R \setminus \{0\}$ such that $ab = 0$.

Proposition 3.1.6. Let R be a commutative ring with identity. Then, the following are equivalent:

1. R has no zero divisors;
2. R is an integral domain;
3. for every $a, b, c \in R$ where $a \neq 0$, if $ab = ac$, then $b = c$.

Proof. Clearly, R is an integral domain if and only if R has no zero divisors. Now, let $a \in R \setminus \{0\}$ and suppose for all $b, c \in R$, we have

$$\begin{aligned} ab &= ac \\ ab - ac &= 0 \\ a(b-c) &= 0. \end{aligned}$$

Since $a \neq 0$, we see by definition R is an integral domain if and only if this implies $b - c = 0$ or, equivalently, $b = c$. ∎

Definition 3.1.7. Let R be a ring with identity. An element $a \in R$ is called a unit if there exists some $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$. The set of units of R is denoted R^*.

Proposition 3.1.8. Let R be a ring with identity. Then, $(R^*, \cdot)$ is a group.

Proof. We have three criteria for $(R^*, \cdot)$ to be a group:

1. Let $a, b \in R^*$. Then, there exist some $a^{-1}, b^{-1} \in R$ such that

   $$aa^{-1} = a^{-1}a = 1 \quad \text{and} \quad bb^{-1} = b^{-1}b = 1.$$

   Since associativity follows from the ring, we have

   $$\begin{aligned} (ab)(b^{-1}a^{-1}) &= a(bb^{-1})a^{-1} = a(1)a^{-1} = aa^{-1} = 1, \\ (b^{-1}a^{-1})(ab) &= b^{-1}(a^{-1}a)b = b^{-1}(1)b = b^{-1}b = 1. \end{aligned}$$

   Thus, $\cdot$ is an associative law of composition on R^*.
2. For every $a \in R^*$, we have $1a = a(1) = a$, so 1 is the neutral element.
3. By construction, a^{-1} is then the inverse of a. ∎

Definition 3.1.9. A ring R is called a field if it is a commutative ring with identity and all its nonzero elements are units, i.e. $R \setminus \{0\} = R^*$.

Proposition 3.1.10. Let R be a ring with identity. Every unit of R is not a zero divisor.

Proof. Let $a \in R^*$. Then, there exists some $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$. Suppose a is a zero divisor. Then, there exists some $b \in R \setminus \{0\}$ such that $ab = ba = 0$, so

$$(aa^{-1})b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}(0) = 0 \quad \text{and} \quad (aa^{-1})b = 1b = b,$$

which implies $b = 0$, a contradiction. Hence, a cannot be a zero divisor. ∎

Corollary 3.1.11. Any field is an integral domain.

Theorem 3.1.12. Any finite integral domain is a field.

Proof. Let R be a finite integral domain, and let $a \in R \setminus \{0\}$. Consider the mapping

$$\begin{array}{rccc} f: & R & \to & R \\ & x & \mapsto & ax \end{array}.$$

Let $x, x' \in R$ such that $ax = ax'$. Since R is an integral domain, left cancellation implies $x = x'$, so f is injective. Further, since f is an injective map between finite sets of the same cardinality, f is also surjective, so there exists some $b \in R$ such that $f(b) = ab = 1 \in R$, and since an integral domain is necessarily commutative, we also have $ba = 1$. Hence, a is a unit, so $R \setminus \{0\} = R^*$. ∎

Definition 3.1.13. Let $(R, +, \cdot)$ be a ring, and let $S \subseteq R$. If $(S, +, \cdot)$ is a ring, it is called a subring of R.

Theorem 3.1.14. Let R be a ring, and let $S \subseteq R$, $S \neq \emptyset$. Then, S is a subring of R if and only if for every $a, b \in S$, we have $a - b \in S$ and $ab \in S$.

Proof. For S to be a ring, $(S, +)$ must be an abelian group. Since $S \subseteq R$, this is the case if and only if $(S, +)$ is a subgroup of $(R, +)$ which, by Theorem 1.2.2, is true if and only if for all $a, b \in S$, we have $a - b \in S$.

Associativity and distributivity of $\cdot$ follow from the parent ring R. Hence, all that remains is that S is closed under $\cdot$, i.e. for all $a, b \in S$, we have $ab \in S$. ∎

Definition 3.1.15. Let R be a ring with identity, and let

$$K = \{n \in \mathbb{N} \mid \underbrace{1_R + \cdots + 1_R}_{n \text{ times}} = 0\}.$$

The number

$$\mathrm{char}(R) = \begin{cases} 0, & K = \emptyset \\ \min(K), & \text{otherwise} \end{cases}$$

is called the characteristic of R.

Proposition 3.1.16. The characteristic of an integral domain is either 0 or prime.

Proof. Let R be an integral domain, and let $n = \mathrm{char}(R)$. If $n = 0$, we are finished; for the other case, since n cannot be 1, take $n > 1$. Suppose n is not prime. Then, there exist $p, q \in \mathbb{Z}^+$, $p, q < n$ such that $n = pq$, so

$$\begin{aligned}
0_R &= \underbrace{1_R + \cdots + 1_R}_{n \text{ times}} = \underbrace{1_R + \cdots + 1_R}_{pq \text{ times}} \\
&= \underbrace{\underbrace{(1_R + \cdots + 1_R)}_{p \text{ times}} + \cdots + \underbrace{(1_R + \cdots + 1_R)}_{p \text{ times}}}_{q \text{ times}} \\
&= \underbrace{\underbrace{(1_R + \cdots + 1_R)}_{p \text{ times}}1_R + \cdots + \underbrace{(1_R + \cdots + 1_R)}_{p \text{ times}}1_R}_{q \text{ times}} \\
&= \underbrace{(1_R + \cdots + 1_R)}_{p \text{ times}}\underbrace{(1_R + \cdots + 1_R)}_{q \text{ times}}.
\end{aligned}$$

Since R is an integral domain, this implies

$$\underbrace{1_R + \cdots + 1_R}_{p \text{ times}} = 0_R \quad \text{or} \quad \underbrace{1_R + \cdots + 1_R}_{q \text{ times}} = 0_R,$$

which is a contradiction. ■

Homomorphisms of rings

Definition 3.1.17. Let $(R, +, \cdot)$ and $(S, \oplus, \odot)$ be two rings. A mapping $\phi : R \to S$ is called a homomorphism of rings if for all $x, y \in R$, we have

$$\phi(x + y) = \phi(x) \oplus \phi(y) \quad \text{and} \quad \phi(x \cdot y) = \phi(x) \odot \phi(y).$$

A homomorphism of rings that is a bijection is called an isomorphism.

Proposition 3.1.18. Let $(R, +, \cdot)$ and $(S, \oplus, \odot)$ be two rings. If there exists a homomorphism of rings $\phi : R \to S$, then there exists a group homomorphism $\psi : (R, +) \to (S, \oplus)$.

Proof. ■ Do this proof!

Proposition 3.1.19. Let $\phi : R \to S$ be a homomorphism of rings. Then, ϕ is an isomorphism if and only if there exists a unique isomorphism $\rho : S \to R$ such that $\rho \circ \phi = \mathrm{id}_R$ and $\phi \circ \rho = \mathrm{id}_S$.

Proof. ■ Do this proof!

Definition 3.1.20. Let ϕ be a homomorphism of rings. The image and kernel of the underlying group homomorphism ψ from Proposition 3.1.18 are called the image and kernel of ϕ.

Proposition 3.1.21. Let $\phi : R \to S$ be a homomorphism of rings. Then,

1. $\operatorname{im}(\phi)$ is a subring of S;
2. $\ker(\phi)$ is a subring of R;
3. ϕ is injective if and only if $\ker(\phi) = \{0_R\}$;
4. ϕ is surjective if and only if $\operatorname{im}(\phi) = S$; and
5. for every $x \in R$ and $y \in \ker(\phi)$, we have $xy \in \ker(\phi)$.

Proof. ■

3.2 Ideals

Definition 3.2.1. Let R be a ring. A non-empty $I \subseteq R$ is called an ideal of R if

1. $(I, +)$ is a subgroup of $(R, +)$ and
2. for all $x \in R$ and $i \in I$, we have $xi \in I$ and $ix \in I$.

Definition 3.2.2. Let R be a commutative ring with identity. An ideal I of R is called

1. prime if for every $x, y \in R$, if $xy \in I$, then $x \in I$ or $y \in I$; or
2. maximal if $I \neq R$ and if there exists an ideal J such that $I \subseteq J$, then $I = J$ or $J = R$.

3.3 Arithmetic in integral domains

3.4 Polynomials

Solved exercises