Basic Algebra

Concise Theory and Solved Exercises

Konstantinos Bizanos

Columbia, Missouri
June 3, 2026

Contents

Preface

These concise notes are based on the tutoring classes that I taught during the Fall semester of 2023–2024 for the course Basic Algebra. They were never intended to serve as a complete substitute for a standard textbook; rather, they should be viewed as supplementary material accompanying the course.

In particular, the part devoted to Group Theory contains several fundamental concepts that are essential for any undergraduate student wishing to continue toward more advanced subjects such as Galois Theory, Representation Theory, or more specialized courses in Algebra.

Throughout these notes, the reader will find a considerable number of solved exercises. Nevertheless, this may easily become a trap. I strongly encourage the reader to first attempt every exercise independently before consulting the provided solutions, using them later only as a way to compare approaches, clarity, and mathematical accuracy.

Especially in an era where AI tools are increasingly dominant, a solution by itself is nearly meaningless — perhaps it always was. What truly matters is developing familiarity with the basic techniques and cultivating the intuition, flexibility, and mathematical perception that come only through personal effort and repeated practice.

Before finishing this preface, I should also mention that a document of roughly thirty pages will almost certainly contain typos, inaccuracies, or minor mistakes. Any comments, corrections, or suggestions are therefore more than welcome at the following email address: `kbfg6@missouri.edu`

Konstantinos Bizanos

Chapter 1

Rings

1.1 First Isomorphism Theorem

Example 1.1.1. Show that $\mathbb{R}[x]/\langle x^2+1\rangle \cong \mathbb{C}$.

Solution. Our aim is to apply the First Isomorphism Theorem. Therefore, we look for a homomorphism $\varphi\colon \mathbb{R}[x] \to \mathbb{C}$ such that $\ker\varphi = \langle x^2+1\rangle$. Define $\varphi\colon \mathbb{R}[x] \to \mathbb{C}$ by $\varphi(f(x)) = f(i)$. It is immediate that φ is a ring homomorphism. To show that it is onto, let $a+bi \in \mathbb{C}$. Then we observe that

$$\varphi(bx+a) = a+bi.$$

First, $x^2+1 \in \ker\varphi$ since $i^2 = -1$. Hence, since $\ker\varphi$ is an ideal, we have $f(x)(x^2+1) \in \ker\varphi$, for every $f(x) \in \mathbb{R}[x]$. Thus $\langle x^2+1\rangle \subseteq \ker\varphi$.

Conversely, let $f(x) \in \ker\varphi$. Then $f(i) = 0$, that is, i is a root of $f(x)$. Since $f(x) \in \mathbb{R}[x]$ and i is a root, its conjugate $\bar{i} = -i$ is also a root. Therefore, $x-i, x+i | f(x)$, and since $x-i, x+i$ are relatively prime, it follows that $x^2+1 = (x-i)(x+i)|f(x)$. Hence, $f(x) = q(x)(x^2+1) \in \langle x^2+1\rangle$, and this proves the result. ■

1.2 Chinese Remainder Theorem

Definition 1. Let I, J be ideals of a ring R. We say that I, J are **relatively prime** if

$$I + J = \{a+b \mid a \in I,\ b \in J\} = R$$

If R has identity, equivalently there exist $a \in I$ and $b \in J$ such that $a+b = 1$.

Notation 1. The above definition can be generalized. Namely, the ideals $I_1, \ldots, I_n$ of a ring R are said to be relatively prime if

$$I_1 + \cdots + I_n = \{a_1 + \cdots + a_n \mid a_j \in I_j\} = R.$$

Example 1.2.1 (Important!)**.** Let F be a field, let $f(x), g(x) \in F[x]$ be **relatively prime**, and let $I = \langle f(x) \rangle$ and $J = \langle g(x) \rangle$. Since $f(x)$ and $g(x)$ are relatively prime, there exist $a(x), b(x) \in F[x]$ such that

$$1 = \underbrace{a(x)f(x)}_{\in I} + \underbrace{b(x)g(x)}_{\in J} \in I + J.$$

Consequently, the ideals I, J are relatively prime.

Example 1.2.2 (Important!)**.** Let $m, n \in \mathbb{Z}$ be relatively prime. If $I = m\mathbb{Z}$ and $J = n\mathbb{Z}$, then, just as in the previous case, the ideals I, J are relatively prime.

Theorem 1 (Chinese Remainder Theorem)**.** Let R be a ring and let $I_1, \ldots, I_n$ be ideals of R.

(a) The map

$$\psi \colon R/\bigcap_{j=1}^{n} I_j \to R/I_1 \times \cdots \times R/I_n,\ \psi\left(r + \bigcap_{j=1}^{n} I_j\right) = (r + I_1, \ldots, r + I_n)\,.$$

is a ring monomorphism.

(b) If $I_1, \ldots, I_n$ are relatively prime, then ψ is a ring isomorphism, that is,

$$R/\bigcap_{j=1}^{n} I_j \cong R/I_1 \times \cdots \times R/I_n.$$

Proof. See M. Maliakas' notes. □

Notation 2 (Special Case)**.** If I, J are relatively prime ideals of a ring R, then

$$R/I \cap J \cong R/I \times R/J.$$

Notation 3. Let I, J be ideals of a ring R. We know that $IJ \subseteq I \cap J$. If I, J are relatively prime, then $IJ = I \cap J$. This can be useful in the case where $R = F[x]$, since we know that $\langle f(x) \rangle \cdot \langle g(x) \rangle = \langle f(x)g(x) \rangle$.

Example 1.2.3. Show that $\mathbb{C}[x]/\langle (x-1)(x-2) \rangle \cong \mathbb{C} \times \mathbb{C}$.

Solution. Let $I = \langle x-1 \rangle$ and $J = \langle x-2 \rangle$, which are relatively prime ideals, since $x-1, x-2$ are relatively prime. Also, by the above observation,

$$\langle (x-1)(x-2) \rangle = IJ = I \cap J$$

By the Chinese Remainder Theorem,

$$\mathbb{C}[x]/\langle (x-1)(x-2) \rangle \cong \mathbb{C}[x]/I \cap J \cong \mathbb{C}[x]/I \times \mathbb{C}/J.$$

Using the usual evaluation homomorphism, we know that $\mathbb{C}[x]/\langle x-a \rangle \cong \mathbb{C}$, for every $a \in \mathbb{C}$. Therefore,

$$\mathbb{C}[x]/\langle (x-1)(x-2) \rangle \cong \mathbb{C}[x]/I \times \mathbb{C}/J \cong \mathbb{C} \times \mathbb{C}.$$

■

Example 1.2.4. Show that $\mathbb{R}[x]/\langle f(x) \rangle \cong \mathbb{R} \times \mathbb{C}$, where $f(x) = (x+1)\left(x^2+1\right)$.

Solution. Exercise. ■

1.3 Exercises on Quotient Rings

Exercise 1. How many elements do the following rings have? Which of them are fields?

(a) $R = \mathbb{Z}_2[x]/\langle x^3 + x + 1 \rangle$

(b) $S = \mathbb{Z}_3[x]/\langle x^3 + x + 1 \rangle$

Solution. (a) First, if F is a field with m elements and $f(x)$ is a nonzero polynomial of degree n, then we know that $|F[x]/\langle f(x) \rangle| = m^n$. Hence, $|R| = 2^3 = 8$. Now, we know that R is a field if and only if $f(x)$ is irreducible. Since $f(x)$ has degree 3 and has no root in $\mathbb{Z}_2$, it is irreducible. Therefore, R is a field.

(b) Similarly to (a), $|S| = 3^3 = 27$. The ring S is not a field, since $f(x) = x^3 + x + 1$ is not irreducible ($f(1) = 3 = 0$).

■

Exercise 2. Let $p(x) = x^2 + 1 \in \mathbb{Z}_3[x]$ and $I = \langle p(x) \rangle$.

(a) Show that $\mathbb{Z}_3[x]/I$ is a field with 9 elements.

(b) Determine whether $x^4 + x + 1 + I, x^4 + 2 + I$ are invertible elements in $\mathbb{Z}_3[x]/I$, and if they are, find their inverses.

Solution. (a) See Exercise 4 (a).

(b) Recall that $g(x) + I$ is invertible in $\mathbb{Z}_3[x]/I$ if and only if $\gcd(g(x), p(x)) = 1$.

- The element x^4+2+I is not invertible, since
$$x^4+2=x^4-1=\left(x^2-1\right)\left(x^2+1\right)=\left(x^2-1\right)p(x).$$
- We apply the Euclidean algorithm to $g(x)=x^4+x+1$ and $p(x)$:
$$\begin{aligned} g(x)&=\left(x^2-1\right)p(x)+x+2\\ p(x)&=(x+1)(x+2)+2 \end{aligned}$$
Therefore, we have
$$\begin{aligned} 2&=p(x)-(x+1)(x+2)\\ 2&=p(x)-(x+1)\left[g(x)-\left(x^2-1\right)p(x)\right]\\ 2&=-(x+1)g(x)+q(x)p(x)\\ 1&=(x+1)g(x)+h(x)p(x) \end{aligned}$$
From the last relation, passing to residue classes mod$I$, we get
$$1+I=(x+1+I)\cdot(g(x)+I)+\underbrace{h(x)p(x)+I}_{=0}=(x+1+I)\cdot(g(x)+I).$$
Consequently, $(g(x)+I)^{-1}=x+1+I$.

■

Exercise 3. Consider the ideals $I=\langle x^2+2\rangle$ and $J=\langle x^2+1\rangle$ in $\mathbb{Z}_5[x]$, and let $R=\mathbb{Z}_5[x]/I$ and $S=\mathbb{Z}_5[x]/J$.

(a) Show that R is a field, but S is not an integral domain.

(b) Is it true that $R\cong\mathbb{Z}_5\times\mathbb{Z}_5$? Is it true that $S\cong\mathbb{Z}_5\times\mathbb{Z}_5$?

(c) How many elements does R have? How many invertible elements does S have?

Solution. (a) Show that x^2+2 has no root in $\mathbb{Z}_5$ and conclude that it is irreducible. Therefore, R is a field. Now, $f(x)=x^2+1$ has roots $2,3$ in $\mathbb{Z}_5$, so $x^2+1=(x-2)(x-3)$. We observe that
$$(x-2)+I\cdot(x-3)+I=x^2+1+I=0+I.$$
with $x-2+I\neq 0+I$ and $x-3+I\neq 0+I$, so S is not an integral domain.

(b) The ring R is a field, while $\mathbb{Z}_5\times\mathbb{Z}_5$ is not an integral domain, so the rings cannot be isomorphic. Similarly to Example 1.2.3, we have
$$S=\mathbb{Z}_5[x]/\langle(x-2)(x-3)\rangle\cong\mathbb{Z}_5[x]/\langle(x-2)\rangle\times\mathbb{Z}_5[x]/\langle(x-3)\rangle\cong\mathbb{Z}_5\times\mathbb{Z}_5.$$

(c) As in Exercise 4, we have $|R|=5^2=25$. For the second part, we showed that $S\cong\mathbb{Z}_5\times\mathbb{Z}_5$. Hence, $|U(S)|=|U(\mathbb{Z}_5\times\mathbb{Z}_5)|$. We have shown that
$$U(A\times B)=U(A)\times U(B)$$
where A,B are arbitrary rings. Hence,
$$|U(S)|=|U(\mathbb{Z}_5\times\mathbb{Z}_5)|=|U(\mathbb{Z}_5)\times U(\mathbb{Z}_5)|=|U(\mathbb{Z}_5)|^2=[\varphi(5)]^2=16.$$

■

Chapter 2

Groups

2.1 The Concept of a Group

Definition 2. A set G equipped with an operation $\cdot\colon G \times G \to G$ is called a **group** if

(a) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, for every $a, b, c \in G$ (associativity)

(b) there exists $e \in G$ such that $a \cdot e = e \cdot a = a$, for every $a \in G$ (existence of an identity element)

(c) for every $a \in G$, there exists $b \in G$ such that $ab = ba = e$ (existence of an inverse).

If, in addition, $a \cdot b = b \cdot a$, for every $a, b \in G$, then G is called **abelian**.

Notation 4. Let $(G, \cdot)$ be a group and let $a, b \in G$.

(a) The identity element $e \in G$ is unique. It is often denoted by 1 or 1_G.

(b) The inverse of $a \in G$ is unique and is denoted by a^{-1}.

(c) For $m \in \mathbb{Z}_{>0}$, we define $a^m = \underbrace{a \cdot a \cdots a}_{m \text{ times}}$, while $a^{-m} = \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{m \text{ times}}$. Clearly, $a^0 = 1_G$.

(d) For every $m, n \in \mathbb{Z}$, we have $a^m \cdot a^n = a^{m+n}$.

(e) If $ab = ba$, then $(ab)^n = a^n b^n$, for every $n \in \mathbb{Z}$.

Notation 5. If G is abelian, we often use $+$ instead of $\cdot$ to denote its operation. In that case, the identity element is denoted by 0_G, and instead of a^m we write ma.

Example 2.1.1. The pairs $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ and $(\mathbb{C}, +)$ are abelian groups, where $+$ is the usual addition. Here the identity element is 0, and the inverse of a is $-a$.

Example 2.1.2. Let R be a ring. The pair $(R, +)$, where $+$ is the addition of the ring, is an abelian group (why?). Now, we have shown that if $a, b \in U(R)$, then $ab \in U(R)$ and, moreover, $(ab)^{-1} = b^{-1}a^{-1}$. The set $U(R)$ together with the multiplication of R is a group (why?).

Example 2.1.3. A set with one element is a group, $G = \{1_G\}$, and is called the **trivial group**.

Definition 3. Let $X \neq \emptyset$ be a set. The **set of symmetries** of X is

$$S(X) = \{f \colon X \to X \mid f \text{ is } 1-1 \text{ and onto}\}.$$

Example 2.1.4. Let $X \neq \emptyset$ be a set. The set of symmetries $S(X)$ of X is a group under composition.

Proof. Clearly, composition of functions is associative. Now, the map $\mathrm{id}_X : X \to X$, the usual identity map on X, is the identity element of $S(X)$, since for every $f \in S(X)$, we have $f \circ \mathrm{id}_X(x) = f(x)$, for every $x \in X$. Now, if $f \in S(X)$, then since f is 1-1 and onto, it has an inverse $g \colon X \to X \in S(X)$ such that

$$f \circ g = g \circ f = \mathrm{id}_X.$$

Therefore, every $f \in S(X)$ has an inverse. □

2.2 The Symmetric Group S_n

Definition 4. The **symmetric group of permutations** S_n ($n \in \mathbb{Z}_{>0}$) is the set of symmetries of the set $\{1, \ldots, n\}$, with operation given by composition of functions, that is,

$$S_n = S(\{1, \ldots, n\}) = \{f \colon \{1, \ldots, n\} \to \{1, \ldots, n\} \mid f \text{ is } 1-1 \text{ and onto}\}.$$

The elements $\sigma \in S_n$ will be denoted by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}.$$

Example 2.2.1. In S_3, the permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ is the map for which $\sigma(1) = 3$, $\sigma(2) = 2$ and $\sigma(3) = 1$.

Notation 6. (a) The identity element of S_n is the identity map, that is,

$$1_{S_n} = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}.$$

(b) We have

- $S_1 = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$
- $S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$.

- $S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$

How do we compose two permutations?

Example 2.2.2. In S_3, consider the permutations $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$. We want to compute the composition $\sigma\tau$:

$$\begin{array}{ccc} 1 & 2 & 3 \\ \downarrow{\scriptstyle \tau} & \downarrow{\scriptstyle \tau} & \downarrow{\scriptstyle \tau} \\ 3 & 2 & 1 \\ \downarrow{\scriptstyle \sigma} & \downarrow{\scriptstyle \sigma} & \downarrow{\scriptstyle \sigma} \\ 3 & 1 & 2 \end{array}$$

Hence, it follows that $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$.

Notation 7. By definition, we know that every $\sigma \in S_n$ is 1-1 and onto. Therefore, it has an inverse. How do we compute its inverse?

Let $\sigma \in S_n$. Then we know that $\sigma^{-1}\sigma = 1_{S_n}$. Hence, for $k \in \{1, \ldots, k\}$, we have

$$k \xrightarrow{\sigma} \sigma(k) \xrightarrow{\sigma^{-1}} k$$

Thus, σ^{-1} sends $\sigma(k)$ to k. Therefore, by a slight abuse of notation, we have

$$\sigma^{-1} = \begin{pmatrix} \sigma(1) & \cdots & \sigma(n) \\ 1 & \cdots & n \end{pmatrix}.$$

By arranging the top row in increasing order, we obtain σ^{-1}.

Example 2.2.3. Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$. Then we have

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

Notation 8. Is it true that S_n is abelian for every $n \geq 1$? Of course not! For $n = 1, 2$ it is clearly abelian, but for every $n \geq 3$, the group S_n is not abelian. Consider

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

and

$$\tau = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 3 & 2 & \cdots & n \end{pmatrix}.$$

Then $\sigma\tau(3) = \sigma(2) = 1$, while $\tau\sigma(3) = \tau(3) = 2$, so $\sigma\tau \neq \tau\sigma$.

Proposition 1. For every $n \geq 1$, we have $|S_n| = n!$.

Proof. Let $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$. For $\sigma(1)$, we have n choices. For $\sigma(2)$, we have $n-1$ choices, since σ is 1-1. Continuing in this way, for $\sigma(n)$ we have 1 choice. Therefore, by the multiplication principle, for σ we have $n \cdot (n-1) \cdots 2 \cdot 1 = n!$ choices. □

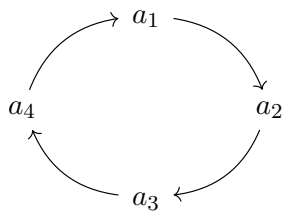
Definition 5. A permutation $\sigma \in S_n$ is called a **cyclic permutation**, or a cycle of length m, if there exist distinct elements $a_1, \ldots, a_m \in \{1, \ldots, n\}$ such that

$$\sigma(a_1) = a_2,\ \sigma(a_2) = a_3,\ \ldots,\ \sigma(a_{m-1}) = a_m,\ \sigma(a_m) = a_1$$

and $\sigma(i) = i$, for every $i \notin \{a_1, \ldots, a_m\}$. In this case, we write

$$\sigma = (a_1\ a_2\ \cdots\ a_m)\,.$$

The number m is called the **length of the cycle**. Every cycle of length 2 is called a **transposition**.



Cycle of length 4.

Example 2.2.4. The permutation $\sigma = (2\ 3\ 1) \in S_5$ is

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

Notation 9. If $\sigma = \begin{pmatrix} a_1 & \cdots & a_m \end{pmatrix}$, then

$$\sigma^{-1} = \begin{pmatrix} a_m & a_{m-1} & \cdots & a_2 & a_1 \end{pmatrix}.$$

$$a_1 \xrightarrow{\sigma} a_2 \xrightarrow{\sigma} a_3 \xrightarrow{\sigma} \cdots \xrightarrow{\sigma} a_m$$

$$a_1 \xleftarrow{\sigma^{-1}} a_2 \xleftarrow{\sigma^{-1}} a_3 \xleftarrow{\sigma^{-1}} \cdots \xleftarrow{\sigma^{-1}} a_m$$

Proposition 2. Let $\sigma, \tau \in S_n$ be disjoint cycles. Then $\sigma\tau = \tau\sigma$.

Corollary 1. Let $\sigma, \tau \in S_n$ be disjoint cycles and let $k \in \mathbb{Z}$. Then $(\sigma\tau)^k = \sigma^k\tau^k$.

Theorem 2 (Decomposition of a Permutation into Disjoint Cycles)**.** Let $\sigma \in S_n$ with $\sigma \neq 1$. Then there exist pairwise disjoint cycles $a_1, \ldots, a_k \in S_n$ such that $\sigma = a_1 \cdots a_k$. This decomposition is unique up to rearrangement of the preceding cycles.

Proof. See M. Maliakas' notes. □

Example 2.2.5. Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 5 & 2 & 9 & 8 & 6 & 7 & 1 \end{pmatrix} \in S_9$. Then

$$\sigma = (1\ 3\ 5\ 9)\,(2\ 4)\,(6\ 8\ 7)\,.$$

2.3 Order of an Element in a Group

Definition 6. Let G be a group and let $g \in G$. If there exists $m \in \mathbb{Z}_{>0}$ such that $g^m = 1$, then the smallest such $m \in \mathbb{Z}_{>0}$ is called the **order** of g and is denoted by $o(g)$ or $|g|$. If there is no $m \in \mathbb{Z}_{>0}$ such that $g^m = 1$, then we say that the order of g is **infinite**.

Example 2.3.1. In every group G, we have $o(g) = 1$ if and only if $g = 1$.

Example 2.3.2. Let $\sigma = (a_1\ a_2\ \cdots\ a_m) \in S_n$ be a cycle of length m. Then $o(\sigma) = m$, since we have shown that $\sigma^m = 1$ and, for every $0 \leq k \leq m-1$, we have $\sigma^k \neq 1$.

Example 2.3.3. Consider the group $(\mathbb{R} \setminus \{0\}, \cdot)$. Then it is immediate that $o(1) = 1$ and $o(-1) = 2$, since $(-1)^2 = 1$.

Example 2.3.4. Consider the group $(\mathbb{Z}_8, +)$ and $[6] \in \mathbb{Z}_8$. We observe that

$$[6]^1 = [6] \neq 0,\ [6]^2 = [36] = [4] \neq [0] \text{ and } [6]^3 = [6][4] = [24] = [0].$$

Consequently, $o([6]) = 3$.

Example 2.3.5. In $(\mathbb{Z}, +)$, every nonzero element has infinite order, since for every $n \neq 0$ and every $m \in \mathbb{Z}_{>0}$, we have $mn \neq 0$.

Notation 10. If G is a finite group, then every element of G has finite order.

Proof. Let $g \in G$. Then, for every $n \in \mathbb{N}$, we have $g^n \in G$. Since G is finite, there exist $m < k$ such that $g^m = g^k$, that is, $g^{k-m} = 1$. From this last relation, we conclude that g has finite order. □

Theorem 3. Let G be a group and let $g \in G$ be an element of order n. The following hold:

(a) For every $m \in \mathbb{Z}_{>0}$ such that $g^m = 1$, we have $n|m$.

(b) For every $k \geq 1$, we have

$$o\left(g^k\right) = \frac{n}{\gcd(k,n)}.$$

Proof. We will prove (a). For (b), see M. Maliakas' notes. Let $m \in \mathbb{Z}_{>0}$ such that $g^m = 1$. Apply Euclidean division to m, n ($n \leq m$). Thus, there exist $q, r \in \mathbb{Z}$ such that $m = nq + r$ with $0 \leq r < n$. If $r \neq 0$, then $0 < r < n$ and

$$g^r = g^{m-nq} = g^m \cdot (g^n)^{-q} = 1.$$

This is a contradiction to the definition of n. □

Proposition 3. Let $\sigma, \tau \in S_n$ be disjoint permutations with orders m, n, respectively. Then

$$o(\sigma\tau) = \text{lcm}(m,n).$$

Proof. Let $k = o(\sigma\tau)$ and $\ell = \text{lcm}(m,n)$. Since k, ℓ are positive integers, it is enough to show that $k|\ell$ and $\ell|k$.

- By Theorem 3, to show that $k|\ell$ it is enough to show that $(\sigma\tau)^\ell = 1$. Since ℓ is a multiple of both m and n, we have $\ell = mx = ny$, for some $x, y \in \mathbb{Z}_{>0}$. Then

  $$(\sigma\tau)^\ell = \sigma^\ell \tau^\ell = (\sigma^m)^x (\tau^n)^y = 1.$$

  The first equality holds because σ, τ are disjoint.

- To show that $\ell|k$, by the definition of the least common multiple, it is enough to show that k is a multiple of both m and n, that is, $m|k$ and $n|k$. By Theorem 3, it is enough to show that $\sigma^k = 1$ and $\tau^k = 1$. We have

  $$(\sigma\tau)^k = \sigma^k \tau^k = 1 \Rightarrow \sigma^k = \tau^{-k}.$$

  Since σ, τ are disjoint, σ^k, τ^{-k} are also disjoint. Therefore, it follows that $\sigma^k = \tau^{-k} = 1$, and this proves the claim.

□

Proposition 4. Let $\sigma \in S_n$ with $\sigma = a_1 a_2 \cdots a_k \neq 1$ a product of disjoint cycles of lengths $n_1, \ldots, n_k$. Then

$$o(\sigma) = \text{lcm}(n_1, \ldots, n_k).$$

Proof. Apply induction, using Example 2.3.2 and Proposition 13. □

2.4 Exercises

Exercise 4. Let G be a group and let $a, b \in G$. Show that:

(a) $o(a)) = o\left(a^{-1}\right)$,

(b) $o\left(b^{-1}ab\right) = o(a)$,

(c) $o(ab) = o(ba)$,

(d) if $b^{-1}a^2b = a^3$ with $a \neq 1$, then $o(a) \geq 5$.

Solution. (a) We have $a^k = 1$ if and only if $a^{-k} = 1$, for every $k \in \mathbb{Z}_{>0}$.

(b) Observe that $\left(b^{-1}ab\right)^k = b^{-1}a^kb$. Therefore, $\left(b^{-1}ab\right)^k = 1$ if and only if $a^k = 1$.

(c) We have $ab = b^{-1}(ba)b$, so by (b) we get the desired result.

(d) The claim is clear if $o(a) = \infty$. Otherwise, by (b), we have $o\left(a^2\right) = o\left(a^3\right)$. Thus,

$$o\left(a^2\right) = \frac{o(a)}{(o(a), 2)} = \frac{o(a)}{(o(a), 3)} = o\left(a^3\right).$$

Hence, $(o(a), 2) = (o(a), 3)$, while $(o(a), 2) = 1$ or 2 and $(o(a), 3) = 1$ or 3. Therefore, $(o(a), 2) = (o(a), 3) = 1$, and since $o(a) \neq 1$, there exists a prime $p \geq 5$ such that $p|o(a)$. This proves the claim. ■

Exercise 5. Let G be a group which has a unique element of order 2, say a. Show that $ab = ba$, for every $b \in G$.

Solution. Let $b \in G$. We want to show that $ab = ba$. Equivalently, it is enough to show that $b^{-1}ab = a$. By Exercise 4 (b), we have $o\left(b^{-1}ab\right) = o(a) = 2$, and by the hypothesis it follows that $b^{-1}ab = a$. ■

Exercise 6. Let G be a group such that for every $g \in G$ with $g \neq 1$, we have $o(g) = 2$. Show that G is abelian.

Solution. Let $a, b \in G$. We want to show that $ab = ba$. By the hypothesis, for every $g \in G$, we have $g^2 = 1$, that is, $g = g^{-1}$. Hence,

$$ab = a^{-1}b^{-1} = (ba)^{-1} = ba.$$

■

Exercise 7. Let $\sigma = (1\ 2\ 3\ 4)(3\ 4\ 5\ 6) \in S_6$.

(a) Find the order of σ^{100}.

(b) Determine whether there exists $\tau \in S_6$ such that $\tau^3 = \sigma$.

Solution. We observe that the given σ is

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 6 & 4 \end{pmatrix} = (1\,2\,3)\,(4\,5\,6).$$

Therefore, by Proposition 4, $o(\sigma) = \text{lcm}(3, 3) = 3$. Hence,

$$o\left(\sigma^{100}\right) = \frac{3}{(3, 100)} = 3.$$

(b) Suppose, toward a contradiction, that there exists $\tau \in S_6$ such that $\tau^3 = \sigma$. Since $o(\sigma) = 3$, we have

$$o\left(\tau^3\right) = \frac{o(\tau)}{(o(\tau), 3)} = 3.$$

We have $(o(\tau), 3) = 1$ or 3. If $(o(\tau), 3) = 3$, then $o(\tau^3) = 1 = o(\sigma)$, which is a contradiction. If $(o(\tau), 3) = 1$, then from the above relation we get $o(\tau) = 3$, and we again arrive at a contradiction. ■

2.5 Subgroups

Definition 7. Let A be a set and let $*\colon A \times A \to A$ be an operation on A. A subset $B \subseteq A$ is called **closed** under the operation $*$ if $x * y \in B$, for every $x, y \in B$. Equivalently, the restriction of the operation $*$ to $B \times B$ gives an operation on B: $*\colon B \times B \to B$.

Definition 8. Let G be a group and let $H \subseteq G$ be closed. The set H is called a **subgroup** of G if it is a group with the operation of G restricted to H. In this case, we write $H \leq G$.

Example 2.5.1. It is clear that $(\mathbb{Z}, +) \leq (\mathbb{Q}, +)$, $(\mathbb{Q}, +) \leq (\mathbb{R}, +)$ and $(\mathbb{R}, +) \leq (\mathbb{C}, +)$. Also, $(\mathbb{R} \setminus \{0\}, \cdot) \leq (\mathbb{C} \setminus \{0\}, \cdot)$.

Example 2.5.2. The set $\mathbb{N}$ is not a closed subset of $(\mathbb{Z}, +)$, since for every nonzero n in $\mathbb{N}$, we have $-n \notin \mathbb{N}$.

Proposition 5. Let $(G, \cdot)$ be a group and let $H \subseteq G$ be nonempty. The following are equivalent.

(a) The set H is a subgroup of G.

(b) For every $a, b \in H$, we have $a \cdot b, a^{-1} \in H$.

(c) For every $a, b \in H$, we have $a \cdot b^{-1} \in H$.

Proof. Prove the above proposition. □

Example 2.5.3. Let $G = S_n$ and $H = \{\sigma \in S_n \mid \sigma(n) = n\}$. We will show that $H \leq G$. Indeed, let $\sigma, \tau \in H$. Then $\sigma \circ \tau(n) = \sigma(n) = n$, so $\sigma\tau \in H$. Also, since $\sigma(n) = n$, we have $\sigma^{-1}(n) = n$, and hence $\sigma^{-1} \in H$.

Example 2.5.4. Let G be an abelian group and let $H = \{g \in G \mid g^2 = 1\}$. We will show that $H \leq G$. Clearly, $H \neq \emptyset$, since $1 \in H$. Now, let $a, b \in H$, that is, $a^2 = b^2 = 1$. Then, since G is abelian, $(ab)^2 = a^2b^2 = 1$, so $ab \in H$. Finally, if $a^2 = 1$, then clearly $a^{-2} = 1$, hence $a^{-1} \in H$.

Proposition 6. Let G be a group and let $\{H_i\}_{i \in I}$ be a family of subgroups of G. Then $\bigcap_{i \in I} H_i$ is a subgroup of G.

Proof. Prove the above proposition. □

2.6 Lagrange's Theorem

Theorem 4 (Lagrange)**.** Let G be a finite group and let $H \leq G$. Then $|H| \Big| |G|$.

Proof. See M. Maliakas' notes. □

Example 2.6.1. Let G be a group of order $n \leq 200$, and let H, K be subgroups of G with orders 10 and 11, respectively.

(a) Find the order of G.

(b) Show that for every $g \in G$, there exist $h \in H$ and $k \in K$ such that $g = hk$.

Solution. (a) By Lagrange's Theorem, since $H, K \leq G$, we have $10, 11 | |G|$. Since $(10, 11) = 1$, it follows that $110 | |G|$. Since $1 \leq |G| \leq 200$, we get $|G| = 110$.

(b) Let $HK = \{hk \mid h \in H,\ k \in K\} \subseteq G$. If we show that $|HK| = 110$, then $G = HK$, and the desired result follows immediately. For each $h \in H$ we have 10 choices, and for each $k \in K$ we have 11 choices.

If we knew that for every $h, h' \in H$ and $k, k' \in K$, the implication $hk = h'k' \Rightarrow h = h'$ and $k = k'$ holds, then by the multiplication principle we would have exactly 110 choices for hk. Let $h, h' \in H$ and $k, k' \in K$ with $hk = h'k'$. Then $(h')^{-1}h = k(k')^{-1} \in H \cap K$.

How many elements does $H \cap K$ have? Since $H \cap K \leq H, K$, by Lagrange's Theorem we have $|H \cap K| | 10$ and $|H \cap K| | 11$. Therefore, $|H \cap K| | (10, 11) = 1$, so $H \cap K = \{1\}$. Hence, since $(h')^{-1}h = k(k')^{-1} \in H \cap K = \{1\}$, we get $(h')^{-1}h = 1$ and $k(k')^{-1} = 1$, that is, $h = h'$ and $k = k'$.

■

2.7 Cyclic Groups

Definition 9. Let G be a group and let $g \in G$. The **cyclic subgroup** generated by g is the set $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$.

Notation 11. Show that the set $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$ is indeed a group.

Notation 12. If the operation of G is additive, then we have $\langle g \rangle = \{ng \mid n \in \mathbb{Z}\}$.

Definition 10. A group G is called **cyclic** if there exists $g \in G$ such that $G = \langle g \rangle$. In this case, g is called a **generator** of G.

Example 2.7.1. In $(\mathbb{Z}, +)$, for every $m \in \mathbb{Z}$, we have $m\mathbb{Z} = \{km \mid k \in \mathbb{Z}\} = \langle m \rangle$, so it is cyclic.

Example 2.7.2. The group $\mathbb{Z}$ is cyclic, and in fact $\mathbb{Z} = \langle 1 \rangle$, since every $n \in \mathbb{Z}$ can be written as $n = n \cdot 1$. Similarly, the group $(\mathbb{Z}_n, +)$ is cyclic of order n, since $\mathbb{Z}_n = \langle [1] \rangle$.

Notation 13. Every cyclic group is abelian.

Proof. Prove the above observation. □

Proposition 7. Every group G of prime order p is cyclic.

Proof. Since $|G| = p \neq 1$, there exists $g \in G$ with $g \neq 1$. Hence, $\langle g \rangle \neq \{1\}$, and by Lagrange's Theorem we have $|\langle g \rangle| \mid |G| = p$. Therefore, $|\langle g \rangle| = 1$ or p, and since $|\langle g \rangle| \neq 1$, we get $|\langle g \rangle| = p = |G|$. Thus $G = \langle g \rangle$. □

Motivation 1. We have seen that $(\mathbb{Z}_n, +)$ is cyclic, with $\mathbb{Z}_n = \langle [1] \rangle = \{[0], \ldots, [n-1]\}$. Could this property carry over to any finite cyclic group?

Proposition 8. Let $G = \langle g \rangle$ be cyclic with $o(g) = n$. Then $G = \left\{1, g, \ldots, g^{n-1}\right\}$.

Proof. We know that $G = \langle g \rangle = \left\{g^k \mid k \in \mathbb{Z}\right\}$. Let $g^k \in G$. By Euclidean division of k by n, there exist $q, r \in \mathbb{Z}$ with $0 \leq r \leq n-1$ such that $k = qn + r$. Then

$$g^k = g^{qn+r} = \underbrace{(g^n)^q}_{1} \cdot g^r = g^r \in \left\{1, g, \ldots, g^{n-1}\right\}.$$

Hence, $G \subseteq \left\{1, g, \ldots, g^{n-1}\right\}$. The reverse inclusion is clear, so we have equality. □

Proposition 9. Let G be a finite group with $|G| = n$. If $g \in G$ with $o(g) = k$, then $k|n$.

Proof. Let $H = \langle g \rangle \leq G$. By Proposition 12, we have $|H| = o(g) = k$. By Lagrange's Theorem, $k = |H| \Big| |G| = n$. □

Example 2.7.3. Let $G = \langle g \rangle$ be a group of order 12. Find the order of the group $\langle g^{26} \rangle \cap \langle g^{99} \rangle$.

Solution. First, by Proposition 12, we have $o(g) = 12$. We observe that $g^{26} = g^{2 \cdot 12+2} = g^2$ and similarly $g^{99} = g^{96+3} = g^{8 \cdot 12+3} = g^3$. Thus, we need to find the order of $\langle g^2 \rangle \cap \langle g^3 \rangle$. We have

$$o\left(g^2\right) = \frac{12}{(2,12)} = 6 \quad \text{and} \quad o\left(g^3\right) = \frac{12}{(3,12)} = 4.$$

First Method

By Proposition 12, we have

$$\langle g^2 \rangle = \left\{1, g^2, g^4, g^6, g^8, g^{10}\right\}$$

and

$$\langle g^3 \rangle = \left\{1, g^3, g^6, g^9\right\}.$$

Hence, $\langle g^2 \rangle \cap \langle g^3 \rangle = \left\{1, g^6\right\}$. Therefore, the order of the corresponding group is 2.

Second Method

If $H = \langle g^2 \rangle \cap \langle g^3 \rangle$, then since $H \leq \langle g^2 \rangle, \langle g^3 \rangle$, by Lagrange's Theorem we have $|H||6$ and $|H||4$, so $|H||(4,6) = 2$. Therefore, $|H| = 1$ or 2. Since $g^6 \in \langle g^2 \rangle \cap \langle g^3 \rangle$ with $g^6 \neq 1$, we get $|H| = 2$. ■

2.8 Even and Odd Permutations

Definition 11. A permutation $\sigma \in S_n$ is called a **transposition** if it is a cycle of length 2, that is, if it has the form $\sigma = (a_1\ a_2)$.

Proposition 10. Every $\sigma \in S_n$ can be written as a product of transpositions.

Proof. We know that every nontrivial permutation can be written as a product of pairwise disjoint cycles. Therefore, it is enough to prove the result assuming that $\sigma = (a_1\ \cdots\ a_m)$ is a cycle of length m. Observe that

$$\sigma = (a_1\ \cdots\ a_m) = (a_1\ a_m)(a_1\ a_{m-1}) \cdots (a_1\ a_2).$$

The above idea for writing a cycle as a product of transpositions may seem unexpected and not obvious at first, but it is fully described by the diagram below. □

Motivation 2. Can we claim that the expression of a permutation as a product of transpositions is unique? Of course not! For example, if $\sigma = (12) \in S_3$, then $\sigma = (12)(13)(13)$. So, is there some feature that remains unchanged in this process? Of course. It is the parity of the number of transpositions. A permutation cannot be written both as a product of an even number and as a product of an odd number of transpositions. For the proof of this claim, see M. Maliakas' notes. Taking this as given, we make the following definitions.

Definition 12. Let $\sigma \in S_n$. We say that σ is **even** if it can be written as a product of an even number of transpositions. Otherwise, σ is called **odd**. Also, we define

$$A_n = \{\sigma \in S_n \mid \sigma \text{ is even}\},$$

which is called the **alternating subgroup** of S_n.

Proposition 11. The set A_n is indeed a subgroup of S_n and, moreover, $|A_n| = |S_n|/2 = n!/2$.

Notation 14. We can define a function sign: $S_n \to \{0, 1\}$ by

$$\text{sign}(\sigma) = \begin{cases} 0, & \sigma \text{ is even} \\ 1, & \sigma \text{ is odd} \end{cases}.$$

Example 2.8.1. In S_{10}, consider the permutation $\sigma = (1\ 3\ \ 5\ 9\ 8)$. Then

$$\sigma = (18)(19)(15)(13),$$

so we conclude that σ is even.

2.9 Exercises

Exercise 8. Let G be a group and let H, K be subgroups of G with orders m, n, respectively, such that $(m, n) = 1$. Show that $H \cap K = \{1\}$.

Solution. We have $H \cap K \leq H$ and $H \cap K \leq K$. Hence, by Lagrange's Theorem, $|H \cap K| \Big| m$ and $|H \cap K| \Big| n$. Therefore, $|H \cap K| | (m, n) = 1$, and so we immediately get $H \cap K = \{1\}$. ■

Exercise 9. Let G be a group of order pq, where p, q are primes. Show that every proper subgroup of G is cyclic.

Solution. Let $H \lneq G$, that is, $|H| < |G| = pq$. By Lagrange's Theorem, we have $|H| \Big| |G| = pq$, and since $|H| < |G| = pq$, it follows that $|H| = 1$ or p or q. Clearly, if $H = \{1\} = \langle 1 \rangle$, while if $|H| = p$ or q, we have already shown that groups of prime order are cyclic. ■

Exercise 10. Let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 5 & 2 & 6 & 3 & 1 \end{pmatrix} \in S_7.$$

(a) Determine whether σ is odd.

(b) Find all $m \in \mathbb{Z}$ such that $\langle \sigma^m \rangle \leq A_7$.

(c) Determine whether there exists $\tau \in S_7$ such that $\sigma = \tau^{2020}$.

Solution. (a) We have $\sigma = (1\ 4\ 2\ 7)(3\ 5\ 6)$, and therefore $\sigma = (17)(12)(14)(36)(35)$. Hence, σ is odd.

(b) We observe that $\langle \sigma^m \rangle \leq A_7$ if and only if every element of $\langle \sigma^m \rangle$ is an even permutation, that is, if and only if σ^{mk} is even, for every $k \in \mathbb{Z}$. The above is equivalent to σ^m being even. From (a), we have

$$\sigma^m = \underbrace{\underbrace{(17)(12)(14)(36)(35)}_{5\ -\ \text{trans.}}\underbrace{(17)(12)(14)(36)(35)}_{5\ -\ \text{trans.}} \cdots \underbrace{(17)(12)(14)(36)(35)}_{5\ -\ \text{trans.}}}_{5m\ -\ \text{transpositions}}.$$

(c) It is easy to observe that for every $\tau \in S_7$, if τ is a product of k transpositions, then τ^{2020} is a product of $2020k$ transpositions, and hence τ^{2020} is even. Since σ is odd, we conclude that there is no $\tau \in S_7$ such that $\sigma = \tau^{2020}$.

■

Exercise 11. Let G be a group of order 105.

(a) If $H \leq G$ with $|H| > 35$, show that $H = G$.

(b) If $g \in G$ with $g^{39} = 1$, show that $g^3 = 1$.

Exercise 12. Let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & a & 1 & b & 6 & 7 & 3 \end{pmatrix} \in S_7.$$

(a) Find a, b such that σ is even.

(b) If σ is even, is it true that $(13)(56)(67) \in \langle \sigma \rangle$?

Exercise 13. Let $\sigma = (2\ 3\ 4\ 5)(4\ 5\ 1\ 6\ 7) \in S_7$.

(a) Find the order of σ and determine whether σ is even.

(b) Find the order of the group $\langle \sigma^{33} \rangle \cap \langle \sigma^{50} \rangle$.

2.10 Group Homomorphisms

Definition 13. Let $(G, \cdot), (H, *)$ be groups. A map $\varphi\colon G \to H$ is called a **group homomorphism** if $\varphi(a \cdot b) = \varphi(a) * \varphi(b)$, for every $a, b \in G$.

- If φ is a homomorphism and 1-1, then it is called a **monomorphism**.
- If φ is a homomorphism and onto, then it is called an **epimorphism**.
- If φ is a homomorphism and both 1-1 and onto, then it is called an **isomorphism**.

We note that two groups G and H are called isomorphic if there exists a group isomorphism $\varphi\colon G \to H$. We write $G \cong H$.

Notation 15. Let $\varphi\colon G \to H$ be a group homomorphism. Then:

(a) $\varphi(1_G) = 1_H$,

(b) $\varphi\left(g^{-1}\right) = [\varphi(g)]^{-1}$, for every $g \in G$,

(c) $\varphi\left(g^n\right) = [\varphi(g)]^n$, for every $g \in G$ and $n \in \mathbb{Z}$.

Example 2.10.1. Let R, S be rings and let $\varphi\colon R \to S$ be a ring homomorphism.

(a) Then $(R, +), (S, +)$ are abelian groups, and $\varphi\colon (R, +) \to (S, +)$ is a group homomorphism.

(b) We have seen that $(U(R), \cdot), (U(S), \cdot)$ are groups, and it is easy to prove that $\varphi|_{U(R)}\colon (U(R), \cdot) \to (U(S), \cdot)$ is a group homomorphism.

Example 2.10.2. Let $\varphi\colon S_n \to \mathbb{Z}_2$ be defined by

$$\varphi(\sigma) = \begin{cases} [0], & \sigma \text{ is even} \\ [1], & \sigma \text{ is odd} \end{cases}.$$

Show that φ is a group epimorphism.

Proposition 12. Let $\varphi\colon G \to H$ and $\psi\colon H \to K$ be group homomorphisms.

(a) The composition $\psi \circ \varphi$ is a group homomorphism.

(b) If φ is a group isomorphism, then φ^{-1} is a group isomorphism.

Proof. Exercise. Compare with the corresponding proposition for rings. □

Proposition 13. Let $\varphi\colon G \to H$ be a group isomorphism. The following hold:

(a) G is finite if and only if H is finite.

(b) G is abelian if and only if H is abelian.

(c) G is cyclic if and only if H is cyclic.

(d) For every $g \in G$, we have $o(g) = o(\varphi(g))$.

Proof. We note that it is enough to prove the forward implications, since by Proposition 12 (b), $\varphi^{-1}\colon H \to G$ is an isomorphism.

(a) Clearly, since φ is 1-1 and onto, we have $|G| = |H|$, and the desired result follows immediately.

(b) Assume that G is abelian. We will show that H is abelian. Let $h_1, h_2 \in H$. Then there exist g_1, g_2 such that $h_1 = \varphi(g_1)$ and $h_2 = \varphi(g_2)$. Then

$$h_1h_2 = \varphi(g_1)\varphi(g_2) = \underbrace{\varphi(g_1g_2) = \varphi(g_2g_1) =}_{G \text{ abelian}} \varphi(g_2)\varphi(g_1) = h_2h_1.$$

Therefore, H is abelian.

(c) Assume that $G = \langle g \rangle$ is cyclic. We will show that H is cyclic, and in fact $H = \langle \varphi(g) \rangle$. Let $h \in H$. Since φ is onto, there exists $x \in G$ such that $h = \varphi(x)$. But $x \in G = \langle g \rangle$, so there exists k such that $x = g^k$. Therefore,

$$h = \varphi(x) = \varphi\left(g^k\right) = [\varphi(g)]^k \in \langle \varphi(g) \rangle.$$

(d) Since φ is an isomorphism, observe that for every $g \in G$, we have $g^k = 1$ if and only if $[\varphi(g)]^k = 1$. □

Notation 16. If we consider groups $(G_1, \cdot), (G_2, *)$, then we can consider their Cartesian product

$$G_1 \times G_2 = \{(g_1, g_2) \mid g_i \in G_i\},$$

which becomes a group in the natural way:

$$(g_1, g_2) \cdot (g_1', g_2') := \left(g_1 \cdot g_1', g_2 * g_2'\right).$$

Notation 17. For every $[k] \in (\mathbb{Z}_n, +)$, we have $o(k) \leq n$, since $n[k] = [kn] = [0]$.

Example 2.10.3. We will examine whether the groups $(\mathbb{Z}_4, +)$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$, as defined in the above observation, are isomorphic. First, we have seen that $\mathbb{Z}_4$ is cyclic. Since $|\mathbb{Z}_2 \times \mathbb{Z}_2| = 4$, in order for it to be cyclic, it would need to contain an element of order 4. However, for every $([a], [b]) \in \mathbb{Z}_2 \times \mathbb{Z}_2$, we have $2([a], [b]) = ([0], [0])$, so $o(([a], [b])) \leq 2$. Therefore, $\mathbb{Z}_2 \times \mathbb{Z}_2$ does not contain an element of order 4, and in particular it is not cyclic. By Proposition 13, it follows that the above groups are not isomorphic.

Definition 14. Let $\varphi\colon G \to H$ be a group homomorphism. We define the **kernel** of φ to be the set

$$\ker \varphi = \{g \in G \mid \varphi(g) = 1_H\}.$$

Notation 18. Show that for a group homomorphism $\varphi\colon G \to H$, we have $\ker \varphi \leq G$ and $\text{Im}\varphi = \{\varphi(g) \mid g \in G\} \leq H$, and that φ is 1-1 if and only if $\ker \varphi = \{1_G\}$.

Proof. Exercise. Compare the above observation with the corresponding result for rings. □

2.11 Classification of Cyclic Groups

Motivation 3. More generally, there are infinitely many distinct cyclic groups, and we may not even know what they are as sets or how they might look. Nevertheless, if we focus only on their structure as groups, as Proposition 13 also suggests, two isomorphic groups are practically two different aspects of the same object. That is, if we examine them with respect to their group-theoretic properties, they are the same. Thus, the following theorem shows that, although we do not know exactly what all cyclic groups are in terms of their underlying sets and operations, up to isomorphism we can identify them with two cases: if G is an infinite cyclic group, then it is isomorphic to $(\mathbb{Z}, +)$, while if G is cyclic of order n, then G is isomorphic to $(\mathbb{Z}_n, +)$. Therefore, up to isomorphism, we have completely classified cyclic groups.

Theorem 5. Let $G = \langle g \rangle$ be a cyclic group.

(a) If $|G| = \infty$, then $G \cong \mathbb{Z}$.

(b) If $|G| = n < \infty$, then $G \cong \mathbb{Z}_n$.

Proof. (a) Assume that $|G| = \infty$, that is, $o(g) = \infty$. Consider $\varphi \colon G \to \mathbb{Z}$ defined by $\varphi\left(g^k\right) = k$. Show that φ is a group isomorphism.

(b) Assume that $|G| = n < \infty$, that is, $o(g) = n < \infty$. Consider $\varphi \colon G \to \mathbb{Z}_n$ defined by $\varphi\left(g^k\right) = [k]$. Show that φ is a group isomorphism.

□

2.12 Structure of Cyclic Groups

Motivation 4. When studying groups, some natural questions arise.

(a) Clearly, every subgroup of a finite group is finite. Also, one can easily prove that every subgroup of an abelian group is abelian. If we are given a cyclic group, can we claim that an analogous statement holds? In other words, is every subgroup of a cyclic group cyclic? The answer is yes!

(b) Also, Lagrange's Theorem tells us that if G is finite and $H \leq G$, then $|H| \Big| |G|$. Does the converse hold for every finite group? That is, if $d||G|$, where G is a finite group and $d > 0$, does there exist $H \leq G$ such that $|H| = d$? In general, no! For example, there is no subgroup of A_4, which has order 12, of order 2. If such a subgroup existed, it would contain an element of order 2, which would be an odd permutation. However, the converse does hold in the special case where G is cyclic. In fact, this subgroup is also unique!

Theorem 6 (Structure of Cyclic Groups)**.** Let $G = \langle g \rangle$ be cyclic.

(a) If $H \leq G$, then H is cyclic.

(b) Assume that $|G| = n < \infty$ and let $d > 0$ such that $d|n$. Then there exists a unique cyclic subgroup of G of order d.

Proof. (a) If $H = \{1\}$, then clearly H is cyclic. If $H \neq \{1\}$, then there exists $k \neq 0$ such that $g^k \in H$. Moreover, since for every $h \in H$ we also have $h^{-1} \in H$, we may assume that $k > 0$. Choose the smallest $k > 0$ such that $g^k \in H$. We will show that $H = \langle g^k \rangle$. Clearly, $\langle g^k \rangle \subseteq H$. Let $g^\lambda \in H$. By Euclidean division of λ by k, there exist unique q, r such that $\lambda = qk + r$ with $0 \leq r < k$. If $r \neq 0$, then

$$g^r = \left(g^k\right)^{-q} \cdot g^\lambda \in H \quad 0 < r < k.$$

By the choice of k, this is a contradiction. Therefore, $r = 0$ and $g^\lambda = \left(g^k\right)^q \in \langle g^k \rangle$.

(b)

- For existence, if $k = n/d$, we will show that $H = \langle g^k \rangle$ is the desired subgroup of order d. We have

$$|H| = o\left(g^k\right) = \frac{n}{(n,k)} = \frac{n}{k} = d.$$

- For uniqueness, let $K = \langle g^\lambda \rangle$ be another subgroup of G of order d. We will show that $H = K$. Since

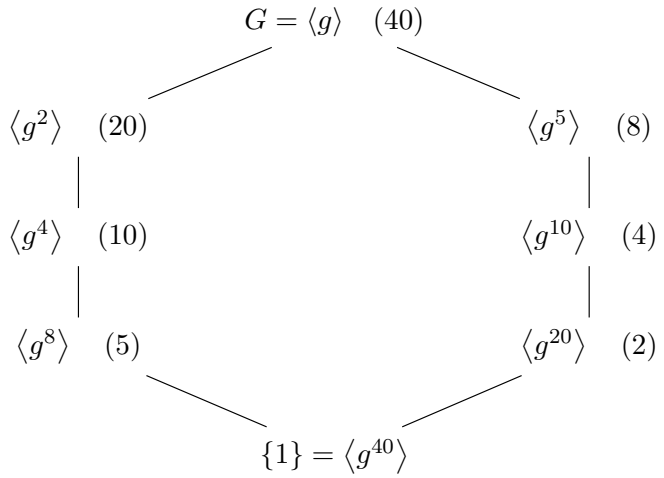
$$d = o\left(g^\lambda\right) = \frac{n}{(\lambda, n)},$$

we have $(\lambda, n) = \frac{n}{d} = k$. Hence, there exist x, y such that $(\lambda, n) = x\lambda + yn = k$. Thus, $g^k = g^{x\lambda} \in K$. Since $H \subseteq K$ and they have the same order, we conclude that $H = K$.

□

Corollary 2. If we are given a finite cyclic group $G = \langle g \rangle$ of order n, then for every $d|n$ with $d > 0$, there exists a unique cyclic subgroup H of G with $H = \left\langle g^{n/d} \right\rangle$. Hence, subgroups of G with the same order coincide.

Example 2.12.1. Let $G = \langle g \rangle$ be cyclic of order 40. The positive divisors of 40 are $1, 2, 4, 5, 8, 10, 20, 40$. Hence, the subgroup diagram of G is the following:



Example 2.12.2. Let $G = \langle g \rangle$ be cyclic of order p^3, where p is prime. The positive divisors of p^3 are $1, p, p^2, p^3$. Hence, the subgroup diagram of G is the following:

$$\begin{array}{ll} G = \langle g \rangle & (p^3) \\ | & \\ \langle g^p \rangle & (p^2) \\ | & \\ \left\langle g^{p^2} \right\rangle & (p) \\ | & \\ \left\langle g^{p^3} \right\rangle = \{1\} & (1) \end{array}$$

2.13 Exercises on Groups

Exercise 14. Let $G = \langle g \rangle$ be cyclic of order 120 and let $H = \left\langle g^{636} \right\rangle$.

(a) Find the smallest positive integer m such that $g^m \in H$.

(b) Find the generators of H.

Solution. (a) First, we easily observe that $H = \left\langle g^{636} \right\rangle = \left\langle g^{36} \right\rangle$ and $o\left(g^{36}\right) = 120/(36, 120) = 10$. Hence, $|H| = 10$, and by the structure theorem for cyclic groups,

$$H = \left\langle g^{120/10} \right\rangle = \left\langle g^{12} \right\rangle = \left\{1, g^{12}, g^{24}, \ldots, g^{12 \cdot 9}\right\}.$$

Thus, the required m is 12.

(b) The elements of H are of the form h^k, where $h = g^{12}$ and $H = \langle h \rangle$. An element h^k is a generator of H if and only if $H = \left\langle h^k \right\rangle$, if and only if $o\left(h^k\right) = o(h)/(o(h), k) = 10$, if and only if $(10, k) = 1$, with $0 \leq k \leq 9$. Hence, $k = 1, 3, 7, 9$, and the desired generators are h, h^3, h^7, h^9.

■

Exercise 15. Let G be a cyclic group of order $n^5 - n$, for $n > 1$. Show that there exists a subgroup of G of order 30.

Solution. By the structure theorem for cyclic groups, it is enough to show that $2 \cdot 3 \cdot 5 = 30 | n^5 - n$, for every $n > 1$. Since $2, 3, 5$ are pairwise relatively prime, it is enough to show that $2 | n^5 - n$, $3 | n^5 - n$ and $5 | n^5 - n$. This follows by applying Fermat's Theorem three times, for $p = 2, 3, 5$, and is left as an exercise. ■

Exercise 16. Let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 4 & 10 & 11 & 9 & 3 & 12 & 1 & 2 & 7 & 6 & 5 & 8 \end{pmatrix} \in S_{12}.$$

We denote by $\langle x \rangle$ the cyclic subgroup of S_{12} generated by $x \in S_{12}$.

(a) Show that $\langle \sigma^{2019} \rangle = \langle \sigma^{1821} \rangle$.

(b) How many generators does $\langle \sigma \rangle$ have? How many of them are even permutations?

(c) Find the subgroups of order 2 and 3 of $\langle \sigma \rangle$, and write their elements as products of disjoint cycles.

Solution. (a) We have $\sigma = (1\ 4\ 9\ 7)(2\ 10\ 6\ 12\ 8)(3\ 11\ 5)$. Hence,

$$o(\sigma) = \text{lcm}(3, 4, 5) = 60,$$

with

$$o\left(\sigma^{1821}\right) = \frac{60}{(60, 1821)} = 20$$

and similarly

$$o\left(\sigma^{2019}\right) = \frac{60}{(60, 2019)} = 20.$$

By the structure theorem for cyclic groups, since $\langle \sigma^{2019} \rangle$ and $\langle \sigma^{1821} \rangle$ are cyclic subgroups of $\langle \sigma \rangle$ of the same order, they are equal.

(b) We have $\langle \sigma \rangle = \left\{1, \sigma, \ldots, \sigma^{59}\right\}$. Also, σ^k, with $0 \leq k \leq 59$, is a generator of $\langle \sigma \rangle$ if and only if $\langle \sigma \rangle = \left\langle \sigma^k \right\rangle$, if and only if $o\left(\sigma^k\right) = 60$, if and only if $(k, 60) = 1$. Hence, the required number is $\varphi(60) = 8$. Now, σ is odd, since it can be written as a product of 9 transpositions. Therefore, σ^k is even if and only if k is even. However, σ^k is a generator if and only if $(k, 60) = 1$, in particular when k is odd. Hence, none of the generators is an even permutation.

(c) Let H and K be the subgroups of orders 2 and 3, respectively. By the structure theorem for cyclic groups,

$$H = \left\langle \sigma^{60/2} \right\rangle = \langle \sigma^{30} \rangle = \left\{1, \sigma^{30}\right\}$$

and similarly

$$K = \left\langle \sigma^{60/3} \right\rangle = \langle \sigma^{20} \rangle = \left\{1, \sigma^{20}, \sigma^{40}\right\}.$$

For example, we compute σ^{20} as a product of disjoint cycles:

$$\begin{aligned} & \sigma^{20} = (1\ 4\ 9\ 7)^{20}(2\ 10\ 6\ 12\ 8)^{20}(3\ 11\ 5)^{20} \\ = \quad & \left[(1\ 4\ 9\ 7)^4\right]^5 \left[(2\ 10\ 6\ 12\ 8)^5\right]^4 (3\ 11\ 5)^{18}(3\ 11\ 5)^2 \\ = \quad & (3\ 11\ 5)^2 = (3\ 5\ 11). \end{aligned}$$

■

Exercise 17. Let $\sigma = (1\ 2\ 5\ 7)(1\ 2\ 4\ 6\ 8) \in S_8$.

(a) Find a representation of σ^{10} as a product of pairwise disjoint cycles.

(b) Find the smallest positive integer n such that $\langle \sigma^{7n} \rangle = \langle \sigma^{100} \rangle$.

(c) Is it true that there exists $\tau \in S_8$ such that $\tau^{-1}\sigma\tau = \sigma^2$?

Solution. (a) We have

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 4 & 3 & 6 & 7 & 8 & 1 & 2 \end{pmatrix} = (1\ 5\ 7)\,(2\ 4\ 6\ 8).$$

Therefore,

$$\sigma^{10} = (1\ 5\ 7)^{10}\,(2\ 4\ 6\ 8)^{10} = (1\ 5\ 7)\,(2\ 4\ 6\ 8)^2.$$

Hence, $\sigma^{10} = (1\ 5\ 7)\,(2\ 6)(4\ 8)$ as a product of disjoint cycles.

(b) First, $o(\sigma) = \text{lcm}(3, 4) = 12$, so $o\left(\sigma^{100}\right) = 3$. By the structure theorem for cyclic groups,

$$\langle \sigma^{7n} \rangle = \langle \sigma^{100} \rangle$$

if and only if

$$o\left(\sigma^{7n}\right) = \left|\langle \sigma^{7n} \rangle\right| = 3.$$

Equivalently, we need n such that $(7n, 12) = 4$. The smallest such n is $n = 4$.

(c) It is easy to show that if τ is a product of k transpositions, then τ^{-1} is also a product of k transpositions. Since σ can be written as a product of 5 transpositions, for every $\tau \in S_8$, the element $\tau^{-1}\sigma\tau$ is odd, while σ^2 is even. Hence, there does not exist $\tau \in S_8$ such that $\tau^{-1}\sigma\tau = \sigma^2$.

■

Exercise 18. Consider the symmetric group S_n, where n is an odd integer with $n \geq 5$, the element

$$\sigma = (1\ 2\ 3)\,(2\ 3\ \cdots\ n)$$

and the cyclic subgroup $H = \langle \sigma \rangle$ of S_n.

(a) Find the order of σ as a function of n, and determine whether H has a subgroup of order 4.

(b) Show that $(1\ 2) \in H$. Is it true that $(1\ 3) \in H$?

(c) Show that there does not exist $\tau \in S_n$ such that $\sigma = \tau^{2022}$.

Solution. (a) We observe that

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots & n \\ 2 & 1 & 4 & 5 & 6 & \cdots & 3 \end{pmatrix} = (1\ 2)(3\ 4\ 5\ \cdots\ n).$$

The length of the cycle $(3\ 4\ 5\ \cdots\ n)$ is $n - 2$, which is odd since n is odd. Hence,

$$o(\sigma) = \text{lcm}(2, n-2) = 2(n-2).$$

If H had a subgroup of order 4, then by Lagrange's Theorem we would need $4|2(n-2)$, that is, $2|n-2$, which cannot happen since $n - 2$ is odd.

(b) Since $n-2$ is odd, it is of the form $n-2 = 2k+1 \geq 3$ because $n \geq 5$. Therefore, $\sigma^{n-2} \in H$ and, in fact,

$$\sigma^{n-2} = (1\ 2)^{n-2}(3\ 4\ 5\ \cdots\ n)^{n-2} = (1\ 2) \in H.$$

Now, if $\sigma^m \in H$, then $\sigma^m(1) \in \{1, 2\}$. Therefore, $(1\ 3) \notin H$.

(c) Observe that

$$\sigma = (1\ 2)(3\ n)(3\ n-1)\cdots(3\ 4).$$

Thus, σ is a product of $n-2$ transpositions, so it is odd. Now, if $\tau \in S_n$ is a product of k transpositions, then τ^{2022} is a product of $2022k$ transpositions, hence τ^{2022} is even. Therefore, there does not exist $\tau \in S_n$ such that $\sigma = \tau^{2022}$.

■

Exercise 19. Consider the permutation $\sigma = (12)(345678) \in S_8$ and the cyclic group $G = \langle\sigma\rangle$ generated by σ.

(a) Does G contain an element of order 3?

(b) Does the permutation (178) belong to the subgroup G?

Solution. (a) We have $o(\sigma) = \text{lcm}(2, 6) = 6$, so G is cyclic of order 6. Since $3|6$, by the structure theorem for cyclic groups, there exists a unique cyclic subgroup H of G of order 3, namely

$$H = \left\langle \sigma^{6/3} \right\rangle = \left\langle \sigma^2 \right\rangle.$$

Hence, $o\left(\sigma^2\right) = |H| = 3$.

(b) We have $\tau = (178) \in G$ if and only if there exists k such that

$$\tau = \sigma^k = (12)^k(345678)^k.$$

However, for every k we have $\sigma^k(1) \in \{1, 2\}$, while $\tau(1) = 7$. Hence, $(178) \notin G$.

■

Exercise 20. Consider the permutations $\sigma, \tau \in S_9$ with

$$\sigma = (1\ 4\ 9\ 3\ 8\ 6)\,(2\ 7\ 5) \quad \text{and} \quad \tau = (1\ 7\ 4\ 9)\,(2\ 6)(3\ 8\ 5).$$

Also consider the groups $G = \langle\sigma\rangle$ and $H = \langle\tau\rangle$.

(a) Determine whether the groups G and H are isomorphic.

(b) For which prime numbers p is the permutation σ^p a generator of the group G?

Solution. (a) Observe that $|G| = o(\sigma) = \text{lcm}(3, 6) = 6$ and $|H| = o(\tau) = \text{lcm}(2, 3, 4) = 12$. Since G, H are finite cyclic groups of different orders, by the classification theorem for cyclic groups, they are not isomorphic.

(b) We have that σ^p is a generator of G if and only if

$$G = \langle \sigma^p \rangle ,$$

if and only if

$$|G| = o\left(\sigma^p\right),$$

if and only if

$$o\left(\sigma^p\right) = \frac{6}{(p,6)} = 6.$$

For every prime p with $p \neq 2, 3$, the element σ^p is a generator of G.

■

Exercise 21. Let $\sigma = (1\ 6\ 2\ 3) \in S_6$.

(a) If $\varphi\colon S_6 \to \mathbb{Z}_9$ is a group homomorphism, show that $\sigma \in \ker \varphi$.

(b) Find the order of the group $\left\langle \sigma^{2010} \right\rangle \cap \left\langle \sigma^{2011} \right\rangle$.

(c) Determine whether there exists $\tau \in S_6$ such that $\sigma = \tau^4$.

Solution. (a) We want to show that $\sigma \in \ker \varphi$, equivalently $\varphi(\sigma) = [0]$, that is, $o(\varphi(\sigma)) = 1$. Since $o(\sigma) = 4$, we have $\sigma^4 = 1$, and therefore $(\varphi(\sigma))^4 = 1$. Hence, $o(\varphi(\sigma))|4$. Moreover, $o(\varphi(\sigma))|9 = |\mathbb{Z}_9|$, so $o(\varphi(\sigma))|(4, 9) = 1$.

(b) Since $o\left(\sigma^{2010}\right) = 2$, by the structure theorem for cyclic groups we have $\left\langle \sigma^{2010} \right\rangle = \left\langle \sigma^2 \right\rangle$. Similarly, $\left\langle \sigma^{2011} \right\rangle = \langle \sigma \rangle$. Hence, the given intersection is

$$\left\langle \sigma^2 \right\rangle \cap \langle \sigma \rangle = \left\langle \sigma^2 \right\rangle ,$$

which has order 2.

(c) We have that σ is odd (why?), while for every $\tau \in S_6$, the element τ^4 is even. Therefore, there cannot exist such a τ with $\sigma = \tau^4$.

■