MATH 323, Algebra I, Fall 2020

Course notes, Chapter 3, Abelian groups

Laurence Barker, Bilkent University. Version: 14 November 2020.

These notes, updated as the course progresses, are a record of the prepared text of the lectures, with a little more detail added, but they cannot cover much of the oral component of the lectures.

Summary of contents

Many of the concepts and theorems of group theory become much easier in the special case of abelian groups. In this file, we shall be studying that comparatively easy special case.

In most of abstract group theory, a multiplicative notation is conventionally used. Yet, in many applications, abelian groups are expressed using additive notation. By first learning the material in the case of abelian groups, we shall have an opportunity to become familiar with notation that is often employed when abelian groups appear in other areas of mathematics.

We shall be discussing:

- the notion of an abelian group,
- Cayley tables for finite abelian groups,
- isomorphisms of abelian groups,
- subgroups of abelian groups,
- Lagrange's Theorem in the case of finite abelian groups,
- cyclic groups
- direct products of abelian groups,
- quotients for abelian groups,
- homomorphisms of abelian groups,
- the three isomorphism theorems in the case of abelian groups,
- The Chinese Remainder Theorem.
- Sylow's Theorem in the case of finite abelian groups.

Homework 1 is at the end of this file.

The notion of an abelian group: We define an **abelian group** to be a pair $(A, *)$, where A is a set and $*$ is a binary operation on A such that the following three conditions hold:

Associativity Axiom: For all $a, b, c \in A$, we have $(a * b) * c = a * (b * c)$. So we can write $a * b * c$ unambiguously.

Identity Axiom: There is an element $e \in A$ such that, for all $a \in A$, we have $e * a = a$. We call e an **identity element** of A.

Inversion Axiom: For all $a \in A$, there exists $b \in A$ such that $a * b = e$.

Commutativity Axiom: For all $a, b \in A$, we have $a * b = b * a$.

For an abelian group $(A, *)$, the set A is called the **underlying set** of $(A, *)$. The function $*$ is called the **operation** of $(A, *)$.

A comment: Later, when we define the general notion of a *group*, we shall drop the Commutativity Axiom. Thus, the definition of a group is simpler than the definition of an abelian group. However, abelian groups tend to be much easier to work with.

Another comment: In older texts, another axiomatic condition seems to appear, called **closure**. The presentation tends to go something like: "For each $a, b \in A$, there is a thing $a * b$." [Wait! What kind of thing is it? Might it be a rabbit?] "Closure Axiom: For all $a, b \in A$, the thing $a * b$ is an element of $A * A$." [Oh, so it is not a rabbit, after all.] From a modern point of view, the "closure axiom" is obsolete. Its content has been absorbed into the definition of a function. However, that little item of history is illuminating, because some closure properties do persist in one of the standard modern definitions of a subgroup, as below.

Example: *Let A be a singleton set, that is to say, a set with size 1. Write $A = \{a\}$. Then we can make A become an abelian group with operation $*$ such that $a + a = a$. An abelian group with only a single element is called a* **trivial group**.

Example: *These are, arguably, the most important examples of all: The pair $(\mathbb{Z}, +)$ is an abelian group. For any positive integer n, the pair $(\mathbb{Z}/n, +)$ is an abelian group.*

Example: *These, too, are of very widespread importance:* For any positive integer n, the pair $((\mathbb{Z}/n)^\times, .)$ is an abelian group, where the dot indicates multiplication as defined in Part 1.

Remark 3.1: *Let $(A, *)$ be an abelian group. The A has a unique identity element.*

Proof: Let $e, f \in A$ such that $e * a = a$ and $f * a = a$ for all $a \in A$. Then $f = e + f = f + e = e$. $\square$

Thanks to the above remark, it makes sense to speak of *the* identity element of A.

Remark 3.2: *Let $(A, *)$ be an abelian group and $a \in A$. Then there exists a unique element b such that $a * b = e$.*

Proof: This existence is clear. Suppose $a * b = a * c = e$ with $b, c \in A$. Then $b * a = e$, hence

$$b = b * e = b * a * c = e * c = c\,. \quad \square$$

Often, in the jargon, instead of speaking of an abelian group $(A, *)$, we speak of the abelian group A, equipped with the operation $*$.

For instance, we may speak of the abelian group $\mathbb{Z}/n$, equipped with addition. We may speak of the abelian group $(\mathbb{Z}/n)^\times$, equipped with multiplication.

The jargon is very useful because, normally, when considering many different groups, we do not employ many different symbols for their binary operations.

In fact, we normally employ one of the following two notations.

Additive notation: Consider an abelian group A. Let us write the operation as addition. Thus, instead of writing $a * b$ we write $a + b$. In that case:

- An element e, as above is called an **zero element** of A, and is written as 0_A or just 0.
- Given $a \in A$ then, by Remark 3.2, there exists a unique element $b \in A$ such that $a + b = 0$. We write $-a = b$, and we call $-a$ the **negative** of a. Note that a is the negative of $-a$. That is, $-(-a) = a$.

Multiplicative notation: Again, consider an abelian group A. Let us write the operation as addition. Thus, instead of writing $a * b$ we write $a.b$ or just ab. In that case:

- The identity element e, as above is also called an **unity element** of A, and it is written as 1_A or just 1.
- Given $a \in A$ then, by Remark 3.2, there exists a unique $b \in A$ such that $ab = 1$. We write $b = a^{-1}$, and we call b the **inverse** of a. Note, a is the inverse of b. Thus, $(a^{-1})^{-1}$.

A few examples of abelian groups: Consider an abelian group $(A, *)$. When the underlying set A is finite, we say that $(A, *)$ is **finite**. In that case, we define the **order** of $(A, *)$ to be the size $|A|$ of the underlying set A. In other words, the order of the group $(A, *)$ is the number of elements of the set A. When the underlying set A is infinite, we say that the abelian group $(A, *)$ is **infinite**.

The term *order* is a misnomer. When $(A, *)$ is infinite, it would make sense to speak of the cardinality of $(A, *)$, meaning the infinite cardinal number $|A|$. There are such things as infinite ordinal numbers, but they only apply to sets equipped with a relation called a well-ordering. Usually, when infinite abelian groups arise in mathematics, they do not come equipped with a well-ordering. So, notions of the order of an infinite abelian group rarely arise.

Sometimes, avoiding that misnomer, the order $|A|$ of a finite abelian group $(A, *)$ is called the **size** of A.

Let us first give some examples of infinite abelian groups

- The abelian group $(\mathbb{Z}, +)$.

Let $\mathbb{Q}$ denote the field of rational numbers. Let $\mathbb{R}$ and $\mathbb{C}$ denote the field of real numbers and the field of complex numbers, respectively.

- The abelian groups $(\mathbb{Q}, +)$ and $(\mathbb{R}, +)$ and $(\mathbb{C}, +)$ are infinite.

Let $\mathbb{Q}^\times$, $\mathbb{R}^\times$, $\mathbb{C}^\times$ denote the sets of nonzero rational, real, complex numbers, respectively. Thus, $\mathbb{Q}^\times = \mathbb{Q} - \{0\}$, and similarly for $\mathbb{R}^\times$ and $\mathbb{C}^\times$.

• Writing a dot to indicate multiplication, the abelian groups $(\mathbb{Q}^\times, .)$ and $(\mathbb{R}^\times, .)$ and $(\mathbb{C}^\times, .)$ are infinite.

The pair $(\mathbb{Z} - \{0\}, .)$ is not a group. For instance, the element 2 has no inverse in $\mathbb{Z} - \{0\}$. However, consistently with general notation in ring theory, let us define

$$\mathbb{Z}^\times = \{-1, 1\}$$

as a subset of $\mathbb{Z}$. Then $(\mathbb{Z}^\times, .)$ is a finite abelian group with order 2. In Chapter 2, we already saw some other examples of finite abelian groups. Let us review them.

• For a positive integer n, the finite abelian group $(\mathbb{Z}/n, +)$ has order $|\mathbb{Z}/n| = n$.

For any integer n such that $n \geq 2$, the pair $(\mathbb{Z}/n, .)$ is not an abelian group, since the element $[0]$ does not have an inverse.

• The finite abelian group $((\mathbb{Z}/n)^\times, .)$ has order $\phi(n)$, where ϕ denotes the Euler totient function. For a brief commentary on ϕ, see Homework 1 at the end of this section.

Cayley tables for finite abelian groups: Consider a finite abelian group A, with operation $*$. One very explicit way of specifying A is to write down a table, where the rows and columns are indexed by the elements of A and, for $a, b \in A$, the entry in row a and column b is the element $a * b = b * a$.

Note that, although we often casually speak of the Cayley table, one cannot write down a Cayley table on paper or screen without choosing a total ordering of the elements.

The additive group $\mathbb{Z}/4$, we mean, the group $(\mathbb{Z}/4, +)$, has the following Cayley table. The operation being addition, the Cayley table could also be called the addition table.

$(\mathbb{Z}/4, +)$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

The multiplicative group $(\mathbb{Z}/5)^\times$ has the following Cayley table. We could also call it the multiplication table.

$((\mathbb{Z}/5)^\times, .)$	$[1]$	$[2]$	$[3]$	$[4]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$
$[2]$	$[2]$	$[4]$	$[1]$	$[3]$
$[3]$	$[3]$	$[1]$	$[4]$	$[2]$
$[4]$	$[4]$	$[3]$	$[2]$	$[1]$

The two tables may appear to have little in common. However, changing the ordering of the rows and columns of the second table, then putting the two tables side-by-side, we see that they do have the same pattern. Indeed, the elements $[0]$, $[1]$, $[2]$, $[3]$ of $\mathbb{Z}/4$, appearing in the left-hand table, behave exactly like the elements, in respective order, $[1]$, $[2]$, $[4]$, $[3]$ of $(\mathbb{Z}/5)^\times$, appearing in the right-hand table.

$\mathbb{Z}/4$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

$(\mathbb{Z}/5)^\times$	[1]	[2]	[4]	[3]
[1]	[1]	[2]	[4]	[3]
[2]	[2]	[4]	[3]	[1]
[4]	[4]	[3]	[1]	[2]
[3]	[3]	[1]	[2]	[4]

On the other hand, the abelian group $(\mathbb{Z}/8)^\times$, though also of order 4, has a quite different Cayley table, as follows. There is no way of changing the ordering of the elements of $(\mathbb{Z}/8)^\times$ to make its Cayley table look like those of the additive group $\mathbb{Z}/4$ and the additive group $(\mathbb{Z}/5)^\times$.

$((\mathbb{Z}/8)^\times, .)$	[1]	[3]	[5]	[7]
[1]	[1]	[3]	[5]	[7]
[3]	[3]	[1]	[7]	[5]
[5]	[5]	[7]	[1]	[3]
[7]	[7]	[5]	[3]	[1]

Thus, in some abstract sense, the additive abelian group $\mathbb{Z}/4$ and the multiplicative abelian group $(\mathbb{Z}/5)^\times$ are essentially the same as each other, whereas the multiplicative group $(\mathbb{Z}/8)^\times$ is essentially different from them.

The notion introduced in the next section captures that sense of essential sameness.

Isomorphisms of abelian groups: In this and the subsequent sections of this file, we shall mainly be discussing theory of abelian groups, in abstract. Let us employ the additive notation.

Let A and B be abelian groups, we mean to say, let $(A, +)$ and $(B, +)$ be abelian groups. We define an **isomorphism** $\theta : A \leftarrow B$ to be a bijection $A \leftarrow B$ such that, for all $b, b' \in B$, we have

$$\theta(b + b') = \theta(b) + \theta(b') \ .$$

When there exists an isomorphism $A \leftarrow B$, we say that A is **isomorphic** to B and we write $A \cong B$.

Remark 3.3: *Given abelian groups A and B and C, then:*
(1) *we have $A \cong A$,*
(2) *if $A \cong B$, then $B \cong A$,*
(3) *if $A \cong B$ and $B \cong C$ then $A \cong C$.*

Proof: Part (1) holds because the identity function id_A is an isomorphism $A \leftarrow A$. Part (2) holds because, given an isomorphism $\theta : A \leftarrow B$, then the inverse $\theta^{-1} : B \leftarrow A$ is an isomorphism. Part (3) holds because, given isomorphisms θ as before and $\phi : B \leftarrow C$, then the composite $\theta \circ \phi : A \leftarrow C$ is an isomorphism. □

Thus, isomorphism of abelian groups satisfies the reflexivity, symmetry and transitivity conditions characteristic of equivalence relations. We hesitate to call it an equivalence relation, though, because the class of abelian groups is a proper class, not a set. Recall, equivalence relations are defined on sets. In the jargon, we say that the relation $\cong$ on abelian groups is a **formal equivalence relation**.

Subgroups of abelian groups: Recall, given sets $A' \subseteq A$ and $B' \subseteq B$ and functions $f : A \leftarrow B$ and $f' : A' \leftarrow B'$ such that $f(b') = f'(b')$ for all $b' \in B'$, then we say that f **restricts** to f' and we call f' a **restriction** of f.

The next remark is obvious.

Remark 3.4: *Let B be an abelian group and $C \subseteq B$. Then the following three conditions are equivalent:*
(a) *The group operation $+ : B \leftarrow B \times B$ restricts to a group operation $C \leftarrow C \times C$.*
(b) *For all $c, c' \in C$, we have $c + c' \in C$ and $-c \in C$.*
(c) *For all $c, c' \in C$, we have $c - c' \in C$.*

When those three equivalent conditions hold, we write $C \leq B$, we call C a **subgroup** of B, and we regard C as an abelian group whose operation $+$ restricted from the operation $+$ on B.

As examples, the abelian group $\mathbb{Z}/4$ has exactly 3 subgroups, namely, $\{[0]\}$ and $\{[0], [2]\}$ and $\mathbb{Z}/4$. The abelian group $(\mathbb{Z}/8)^\times$ has exactly 5 subgroups, namely:

$$\{[1]\}\ , \quad \{[1], [3]\}\ , \quad \{[1], [5]\}\ , \quad \{[1], [7]\}\ , \quad (\mathbb{Z}/8)^\times\ .$$

For any abelian group A, two of the subgroups are $\{0\}$ and A. The subgroup $\{0\}$ is called the **trivial subgroup** of A.

Lagrange's Theorem for finite abelian groups: Lagrange did have an input into the following theorem, in his work on symmetries of polynomial functions. But that work long preceeded the formulation of the notion of a group.

Given an abelian group B, a subgroup $C \leq B$ and an element $b \in B$, then the set

$$b + C = \{b + c : c \in C\} = \{c + b : c \in C\}$$

is called a **coset** of C in B..

Theorem 3.5: (Lagrange's Theorem, in the case of finite abelian groups.) *Let C be a subgroup of an abelian group B. Then $|C|$ divides $|B|$.*

Proof: Let $\equiv$ be the relation on B such that, given $f, g \in B$, then $f \equiv g$ if and only if $f - g \in C$. We shall show that $\equiv$ is an equivalence relation. Let $f, g, h \in C$. Since $f - f = 0 \in C$, we have $f \equiv f$. If $f - g \in C$, then $g - f = -(f - g) \in C$, so $g \equiv f$. If $f - g \in C$ and $g - h \in C$ then $f - h = (f - g) + (g - h) \in C$, so $f \equiv h$. We have confirmed that $\equiv$ is an equivalence relation.

The equivalence class of f under $\equiv$ is the coset $f + C$. So the cosets of C are mutually disjoint. The function $f + C \leftarrow C$ given by $f + c \leftarrow\!\shortmid c$ is bijective, indeed, the inverse is given by $g \mapsto g - f$. So all the cosets of C have size $|C|$. We have shown that $|B|/|C|$ is the number of cosets of C. $\square$

As an example, we saw above that the multiplicative group $(\mathbb{Z}/8)^\times$ has exactly 1 subgroup with order 1, it has exactly 3 subgroups with order 2, it has no subgroups with order 3, it has 1 subgroup with order 4. Evidently, the order of every subgroup of $(\mathbb{Z}/8)^\times$ divides the order $|(\mathbb{Z}/8)^\times| = 4$.

Cyclic groups and cyclic subgroups: Let A be an abelian group. Given $a \in A$, we write $2a = a + a$ and $3a = a + a + a$ and so on. Generally, for any integer m, we define ma to be the element of A such that $(m+1)a = ma + a$ and $0.a = 0$, we mean, $0_{\mathbb{Z}}.a = 0_A$, where $0_{\mathbb{Z}}$ is the integer zero and 0_A is the zero element of A. Thus, for instance, $2m = m + m$ and $3m = m + m + m$. We have $(-2)a = (-a) + (-a) = -(a + a) = -(2a)$, so we can write $-2a$ unambiguously. Similarly, we can write $-ma$ unambiguously.

We define a **cyclic group** to be an abelian group C such that, for some element $g \in C$, we have

$$C = \{mg : m \in \mathbb{Z}\} .$$

We call g a **generator** of C and we write $C = \langle g \rangle$.

For any abelian group A and $a \in A$, the set

$$\langle a \rangle = \{ma : m \in \mathbb{Z}\}$$

is a subgroup of A. We mean to say, the set $\langle a \rangle$ becomes a subgroup when we equip it with the restriction of the operation on A. Furthermore, $\langle a \rangle$ is plainly a cyclic group. We call $\langle a \rangle$ the **cyclic subgroup of A generated by** a. When $\langle a \rangle$ is finite, we say that a has **finite order** and we call $|\langle a \rangle|$ the **order** of a. Thus, when a has finite order, the order $|\langle a \rangle|$ is the smallest positive integer m such that $ma = 0$. When $\langle a \rangle$ is infinite, we say that a has **infinite order**.

Lagrange's Theorem for finite abelian groups has the following immediate corollary.

Corollary 3.6: *Let a be an element of a finite abelian group A. Then a has finite order. Furthermore, $|\langle a \rangle|$ divides $|A|$.*

To illustrate the corollary, we note that the elements [0], [1], [2], [3], [4], [5] of the abelian group $\mathbb{Z}/6$ have orders 1, 6, 3, 2, 3, 1, respectively.

The infinite abelian group $\mathbb{Z}$ is cyclic. In fact, $\mathbb{Z}$ has precisely 2 generators, namely 1 and -1. For each positive integer n, the finite group $\mathbb{Z}/n$ is cyclic and has generator [1], we mean, $[1]_n$. The next result says that, up to isomorphism, there are no other cyclic groups.

Proposition 3.7: *Let A be a cyclic group. If A is infinite, then $A \cong \mathbb{Z}$. If A is finite with order n, then $A \cong \mathbb{Z}/n$.*

Proof: Let g be a generator for A. If, as s runs over the integers, the elements sg are mutually distinct, then A is infinite and there is an isomorphism $A \leftrightarrow \mathbb{Z}$ given by $sg = s$.

Now suppose that the elements sg are not mutually distinct. Given integers s and t such that $sg = tg$, then $(s - t)g = 0 = (t - s)g$. So there exists a positive integer n such that $ng = 0$, moreover, taking n to be the smallest such positive integer, then $A = \{0, g, ..., (n-1)g\}$ and the elements 0, g, $2g$, ..., $(n-1)g$ are mutually distinct. It is now clear that A is finite, in fact, $|A| = n$ and there is an isomorphism $A \leftrightarrow \mathbb{Z}/n$ given by $mg \leftrightarrow [mg]_n$. $\square$

Thus, any two infinite cyclic groups are isomorphic to each other. Also, any two finite cyclic groups with the same order are isomorphic to each other.

The subgroups of a cyclic group: We shall describe the subgroups of any given cyclic group.

Proposition 3.8: *Let A be a cyclic group. Then every subgroup of A is cyclic.*

Proof: Let $B \leq A$. If $B = \{0\}$ then $B = \langle 0 \rangle$. Now suppose $B \neq \{0\}$. Then $mg \in B$ for some integer m. Since $-mg \in B$, we may assume m to be positive. Let n be any integer such that $ng = 0$. Then $n = km + r$ for some integers k and r with $0 \leq r < m$. But $rg = (n - km)g \in B$. By the minimality of m, we have $r = 0$. So m divides n. Therefore, $B = \langle mg \rangle$. $\square$

For any finite cyclic group, we have the following classification of the subgroups.

Proposition 3.9: *Let A be a finite cyclic group. Then there is a bijective correspondence between the divisors d of $|A|$ and the subgroups B of $\mathbb{Z}/n$ such that $d \leftrightarrow B$ provided $B \cong \mathbb{Z}/d$.*

Proof: Let $n = |A|$. By Proposition 3.7, $A \cong \mathbb{Z}/n$. So we may assume that $A = \mathbb{Z}/n$. Plainly, for each divisor d of n, the subgroup $B_d = \langle [n/d] \rangle$ is isomorphic to $\mathbb{Z}/d$. It remains only to show that A has no other subgroups. Let $B \leq A$. Let m be the smallest positive integer such that $[m] \in B$. Define $k = \gcd(m, n)$. By the Greatest Common Divisor Theorem, there exist integers x and y such that $k = xm + yn$. Then $[k] = x[m]$, so $[k] \in B$. But $k \leq m$, so the minimality of m implies that $k = m$. Therefore, m divides n, moreover, $[m]$ is a generator of B. We conclude that $B = B_{n/m}$. $\square$

For example, the subgroups of the cyclic $\mathbb{Z}/6 = \{[0], [1], [2], [3], [4], [5]\}$ are

$$\langle [0] \rangle = \{[0]\}\ , \quad \langle [3] \rangle = \{[0], [3]\}\ , \quad \langle [2] \rangle = \langle 4 \rangle = \{[0], [2], [4]\}\ , \quad \langle [1] \rangle = \langle 5 \rangle = \mathbb{Z}/6$$

The respective orders of those subgroups are 1, 2, 3, 6, which are precisely the divisors of 6.

Classification of the subgroups of an infinite cyclic group is easier, and can be found in Exercise 2.A.

Direct products of abelian groups: Recall, given sets X and Y, we define the direct product $X \times Y$ to be the set of pairs (x, y) with $x \in X$ and $y \in Y$.

Now consider abelian groups A and B. We make the direct product

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

become an abelian group with operation $+$ given by

$$(a, b) + (a', b') = (a + a', b + b')$$

for $a, a' \in A$ and $b, b' \in B$. It is easy to check that $(A \times B, +)$ is indeed an abelian group, the zero element being $(0, 0)$, the negative of (a, b) being $-(a, b) = (-a, -b)$.

Observe that there is an isomorphism $(\mathbb{Z}/8)^\times \leftarrow \mathbb{Z}/2 \times \mathbb{Z}/2$ given by

$$[1] \leftarrow\!\shortmid ([0], [0])\ , \qquad [3] \leftarrow\!\shortmid ([0], [1])\ , \qquad [5] \leftarrow\!\shortmid ([1], [0])\ , \qquad [7] \leftarrow\!\shortmid ([1], [1])\ .$$

Thus, up to isomorphism, $(\mathbb{Z}/8)^\times$ can be described in terms of cyclic groups,

$$(\mathbb{Z}/8)^\times \cong \mathbb{Z}/2 \times \mathbb{Z}/2 \, .$$

Further examples of cyclic subgroups: Consider an abelian group $(A, +)$, we mean to say, an abelian group A with operation written as addition. Recall, the order $|\langle a \rangle|$ of an element $a \in A$ is the smallest positive integer m such that $ma = 0$, unless $ma \neq 0$ for all positive integers m, in which case we write $|\langle a \rangle| = \infty$.

We have already given some examples of that, but let us now give one more. The orders of the 6 elements [0], [1], [2], [3], [4], [5] of $\mathbb{Z}/6$ are 1, 6, 3, 2, 3, 5 respectively.

When we write the operation as multiplication instead of addition, nothing changes, except for the notation. Consider, now, an abelian group $(A, .)$, we mean, an abelian group A with operation written as addition. Thus, we are now writing, for instance, a^{-2} and a^{-1} and 1 and a^3 in place of ..., $-2a$ and $-a$ and 1 and $3a$, respectively. For $a \in A$, the order $|\langle a \rangle|$ is the smallest positive integer m such that $a^m = 1$, except when $a^m \neq 1$ for all positive integers m.

The next table shows the powers of the 6 elements of $(\mathbb{Z}/7)^\times$.

		m					
	a^m	[1]	[2]	[3]	[4]	[5]	[6]
a	[1]	[1]	[1]	[1]	[1]	[1]	[1]
	[2]	[2]	[4]	[1]	[2]	[4]	[1]
	[3]	[3]	[2]	[6]	[4]	[5]	[1]
	[4]	[4]	[2]	[1]	[4]	[2]	[1]
	[5]	[5]	[4]	[6]	[2]	[3]	[1]
	[6]	[6]	[1]	[6]	[1]	[6]	[1]

Thus, for instance, $[2]^1 = [2] \neq [1]$ and $[2]^2 = [4] \neq [1]$ but $[2]^3 = [1]$. So the smallest positive integer m satisfying $[2]^m = [1]$ is 3. In other words, the element [2] of $(\mathbb{Z}/7)^\times$ has order 3. From the table, we see that the elements [1], [2], [3], [4], [5], [6] have orders 1, 3, 6, 3, 6, 2, respectively.

Evidently, the abelian groups $(\mathbb{Z}/6, +)$ and $((\mathbb{Z}/7)^\times, .)$ have something in common. They both have exactly 1 element with order 1, exactly 1 element with order 2, exactly 2 elements with order 3, exactly 2 with order 6.

Since $|(\mathbb{Z}/7)^\times| = 6 = |\langle [3] \rangle|$, we have

$$(\mathbb{Z}/7)^\times = \langle [3] \rangle \, .$$

In particular, $(\mathbb{Z}/7)^\times$ is cyclic. So, by Proposition 3.7,

$$(\mathbb{Z}/7)^\times \cong \mathbb{Z}/6 \, .$$

From the row labelled [3] in the latest table, we see that there is an isomorphism $(\mathbb{Z}/7)^\times \leftarrow \mathbb{Z}/6$ given by $[3]_7 \leftarrow\!\shortmid [1]_6$. Then $[3]^2 \leftarrow\!\shortmid [2]$ and $[3]^3 \leftarrow\!\shortmid [3]$ and so on. Thus,

$$[3] \leftarrow\!\shortmid [1] \, , \quad [2] \leftarrow\!\shortmid [2] \, , \quad [6] \leftarrow\!\shortmid [3] \, , \quad [4] \leftarrow\!\shortmid [4] \, , \quad [5] \leftarrow\!\shortmid [5] \, . \quad [1] \leftarrow\!\shortmid [0] \, .$$

To see that isomorphism in a very tangible way, let us compare the Cayley tables, but with the elements of $(\mathbb{Z}/7)^\times$ arranged in a suitable order. First, the Cayley table for $\mathbb{Z}/6$ is very easy to write down.

$\mathbb{Z}/6$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

Now let us write out the Cayley table for $(\mathbb{Z}/7)^\times$, but with the rows and columns ordered as dictated by the above isomorphism.

$(\mathbb{Z}/7)^\times$	[1]	[3]	[2]	[6]	[4]	[5]
[1]	[1]	[3]	[2]	[6]	[4]	[5]
[3]	[3]	[2]	[6]	[4]	[5]	[1]
[2]	[2]	[6]	[4]	[5]	[1]	[3]
[6]	[6]	[4]	[5]	[1]	[3]	[2]
[4]	[4]	[5]	[1]	[3]	[2]	[6]
[5]	[5]	[1]	[3]	[2]	[6]	[4]

As a smaller example, consider the abelian groups $(\mathbb{Z}/8)^\times$ and $\mathbb{Z}/2 \times \mathbb{Z}/2$. In the previous section, we noted that those two abelian groups are isomorphic to each other. Thus, from an abstract point of view, those two abelian groups are essentially the same. The abelian group $(\mathbb{Z}/8)^\times \cong \mathbb{Z}/2 \times \mathbb{Z}/2$ is not cyclic, and all 3 of its non-identity elements have order 2.

Quotients for abelian groups: Let B be an abelian group and let $C \leq B$. We write the set of cosets of C in B as

$$B/C = \{b + C : b \in b\} .$$

We make B/C become an abelian group by defining the operation $+$ to be such that

$$(b_1 + C) + (b_2 + C) = b_1 + b_2 + C$$

for $b, b' \in B$. We must check, first of all, that the function $+ : B/C \leftarrow B/C \times B/C$ is well-defined. Then we must check that the pair $(B/C, +)$ is an abelian group.

For well-definedness, let $b_1', b_2' \in B$ such that $b_1' + C = b_1 + C$ and $b_2' + C = b_2 + C$. We are required to show that

$$b_1' + b_2' + C = b_1 + b_2 + C .$$

Since $b_1' \in b_1 + C$, there exists $c_1 \in C$ such that $b_1' = b_1 + C$. Similarly, there exists $c_2 \in C$ such that $b_2' = b_2 + c_2$. Hence,

$$b_1' + b_2' + C = b_1 + c_1 + b_2 + c_2 + C .$$

But $c_1 + c_2 \in C$, so $c_1 + c_2 + C = C$. The required equality follows, and the well-definedness is confirmed.

Now let us check the axioms, one by one. The associativity for B/C follows from the associativity for B, since

$$((b_1 + C) + (b_2 + C)) + b_3 + C = b_1 + b_2 + b_3 + C = (b_1 + C) + ((b_2 + C) + (b_3 + C))$$

for $b_1, b_2, b_3 \in B$. The Identity Axiom holds for B/C because the element $0 + C = C$ is plainly the zero element of B/C. The Inversion Axiom holds because

$$(-b + C) + (b + C) = -b + b + C = C = b - b + C = (b + C) + (-b + C)$$

for all $b \in B$. The commutativity for B/C is inherited from the commutativity for B, indeed,

$$(b_1 + C) + (b_2 + C) = b_1 + b_2 + C = b_2 + b_1 + C = (b_2 + C) + (b_1 + C)$$

for all $b_1, b_2 \in B$. We have confirmed that the definition of B/C makes sense.

The group B/C is called the **quotient** of B by C.

Our first example is an infinite one. For any positive integer n, let $n\mathbb{Z}$ denote the subset of $\mathbb{Z}$ consisting of those integers that are divisible by n. Thus, $n\mathbb{Z} = \{nx : x \in Z\}$. It is not hard to see that $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. We have already been discussing the quotient of $\mathbb{Z}$ by $n\mathbb{Z}$, though we have been employing a customized notation for it,

$$\mathbb{Z}/n = \mathbb{Z}/n\mathbb{Z} \ .$$

The rationale for the customized notation is that the expression $\mathbb{Z}/n$ can be viewed as an abbreviation of $\mathbb{Z}/n\mathbb{Z}$. For each $x \in \mathbb{Z}$, the coset of $n\mathbb{Z}$ owning x is

$$[x]_n = x + \mathbb{Z}/n \ .$$

Homomorphisms of abelian groups Let A and B be abelian groups. The following definition is similar to the definition we gave for the notion of an isomorphism. We define a **homomorphism** $A \leftarrow B$ to be a function $\theta : A \leftarrow B$ such that

$$\theta(b_1 + b_2) = \theta(b_1) + \theta(b_2)$$

for all $b_1, b_2 \in B$. Thus, the isomorphisms of abelian groups are precisely the bijective homomorphisms.

Remark 3.10: *Let A and B be abelian groups. Let $\theta : A \leftarrow B$ be a homomorphism. Then $\theta(0_B) = 0_A$. Also, for any $b \in B$, we have $\theta(-b) = -\theta(b)$ and, more generally, $\theta(mb) = m\theta(b)$ for all $m \in \mathbb{Z}$.*

Proof: Since $0_B + 0_B = 0_B$, we have $\theta(0_B) + \theta(0_B) = \theta(0_B)$. Adding $-\theta(0_B)$ to both sides, we deduce that $\theta(0_B) = 0_A$.

We have $b + (-b) = 0_B$. So $\theta(b) + \theta(-b) = 0_A = \theta(b) + (-\theta(b))$. Adding $-\theta(b)$ to both sides, we deduce that $\theta(-b) = -\theta(b)$. An easy inductive argument now yields the more general equality. $\square$

Proposition 3.11: *Let A and B be abelian groups. Let $\theta : A \leftarrow B$ be a homomorphism. Writing the image as*

$$\mathrm{im}(\theta) = \{\theta(b) : b \in B\}$$

then $\mathrm{im}(\theta) \leq A$. *Defining*

$$\ker(\theta) = \{b \in B : \theta(b) = 0\}$$

then $\ker(\theta) \leq B$.

Proof: Given $a, a' \in \mathrm{im}(\theta)$, then $a = \theta(b)$ and $a' = \theta(b')$ for some $b, b' \in B$. We have $a - a' = \theta(b) - \theta(b') = \theta(b - b') \in \mathrm{im}(\theta)$. Applying condition (c) of Remark 3.4, we deduce that $\mathrm{im}(\theta) \leq A$.

Given $c, c' \in \ker(\theta)$, then $\theta(c - c') = \theta(c) - \theta(c') = 0 - 0 = 0$, hence $c - c' \in \ker(\theta)$. Arguing as before, we deduce that $\ker(\theta) \leq B$. $\square$

The subgroup $\ker(\theta)$ of B is called the **kernel** of θ. For any abelian group B, every subgroup $C \leq B$ is the kernel of a homomorphism. Indeed, the homomorphism $B/C \leftarrow B$ given by $bC \leftarrow\!\shortmid b$ has kernel C.

Theorem 3.12: (First Isomorphism Theorem for Abelian Groups:) *Let A and B be abelian groups and $\theta : A \leftarrow B$ a homomorphism. Then*

$$\mathrm{im}(\theta) \cong B/\ker(\theta) \ .$$

In fact, there is a group isomorphism $\Theta : \mathrm{im}(\theta) \leftarrow B/\ker(\theta)$ such that, for all $b \in B$, we have $\Theta(b + \ker(\theta)) = \theta(b)$.

Proof: Let $K = \ker(\theta)$. We first show that Θ is well-defined. Given $b, b' \in B$ such that $b + K = b' + K$, then $b = b' + k$ for some $k \in K$. Hence, $\theta(b) = \theta(b') + \theta(k) = \theta(b')$. So Θ is well-defined.

Given $b_1, b_2 \in B$, then

$$\Theta(b_1 + K) + \Theta(b_2 + K) = \theta(b_1) + \theta(b_2) = \theta(b_1 + b_2)$$

$$= \Theta(b_1 + b_2 + K) = \Theta((b_1 + K) + (b_2 + K)) \ .$$

So Θ is a homomorphism.

Plainly, Θ is surjective. Let $b, b' \in B$ such that $\Theta(b + K) = \Theta(b' + K)$. Thus, $\theta(b) = \theta(b')$. So $\theta(b - b') = \theta(b) - \theta(b') = 0$. Therefore, $b - b' \in K$, in other words, $b + K = b' + K$. We have shown that Θ is injective. The bijectivity of Θ is now demonstrated, and we conclude that Θ is an isomorphism. $\square$

Theorem 3.13: (Second Isomorphism Theorem for Abelian Groups:) *Let $H \leq G \geq K$ be abelian groups. Then $K \leq H + K \leq G$ and $H \cap K \leq H$, furthermore,*

$$(H + K)/K \cong H/(K \cap H) \ .$$

In fact, there is an isomorphism $(H+K)/K \leftarrow H/(H\cap K)$ *given by* $h+K \leftarrow\!\shortmid h+H\cap K$ *for* $h \in H$.

Proof: Plainly, $K \leq H + K \leq G$ and $H \cap K \leq H$. Let $\phi : (H + K)/K \leftarrow H$ be the function such that $\phi(h) = h + K$. Plainly, ϕ is a surjective homomorphism and $\ker(\phi) = H \cap K$. The required conclusion now follows from the First Isomorphism Theorem. □

To illustrate the theorem, let k and h be positive integers. Then, as subgroups of $\mathbb{Z}$, we have $k\mathbb{Z} + h\mathbb{Z} = a\mathbb{Z}$ and $k\mathbb{Z} \cap h\mathbb{Z} = b\mathbb{Z}$ where $a = \gcd(k, h)$ and $b = \mathrm{lcm}(k, h)$.

Theorem 3.14: (Third Isomorphism Theorem for Abelian Groups:) *Let* $E \leq F \leq G$ *be abelian groups. Then* $F/E \leq G/E$ *and*

$$G/F \cong (G/E)/(F/E) \ .$$

In fact, there is a group isomorphism $(G/F) \leftarrow (G/E)/(F/E)$ *given by* $g + F \leftarrow\!\shortmid (g + E) + (F/E)$ *for* $g \in G$.

Proof: Let $\psi : G/F \leftarrow (G/E)/(F/E)$ be the function such that $\psi(g + E) = g + F$. Plainly ψ is a well-defined surjective homomorphism and $\ker(\Phi) = F/E$. □

As an illustration, let e, f, g be positive integers such that e is divisible by f, also f is divisible by g. Then $e\mathbb{Z} \leq f\mathbb{Z} \leq g\mathbb{Z}$. We have

$$g\mathbb{Z}/f\mathbb{Z} \cong (f/g)\mathbb{Z} = (g\mathbb{Z}/e\mathbb{Z})/(f\mathbb{Z}/e\mathbb{Z}) \ .$$

Incidental Exercise: Interpret the Three Isomorphism Theorems for finite-dimensional vector spaces. Note, given a field F and a subspace U of an F-vector space V, the **quotient space** U/V is defined to be the quotent U/V, as above, with the evident vector space structure.

The Chinese Remainder Theorem: We shall present two results, which we shall call the Additive Chinese Remainder Theorem and the Multiplicative Chinese Remainder Theorem. They can both be viewed as parts of a result called the Chinese Remainder Theorem, which is best expressed in the context of ring theory.

Theorem 3.14: (Additive Chinese Remainder Theorem.) *Let* m *and* n *be coprime positive integers. Then there is an isomorphism*

$$\mathbb{Z}/m \times \mathbb{Z}/n \leftarrow \mathbb{Z}/mn$$

given by $([z]_m, [z]_n) \leftarrow\!\shortmid [z]_{mn}$ *for* $z \in \mathbb{Z}$.

Proof: Let $\theta : \mathbb{Z}/n \times \mathbb{Z}/m \leftarrow \mathbb{Z}/nm$ be the specified function. Plainly, θ is well-defined. For $x, y \in \mathbb{Z}$, we have

$$\theta([x]_{mn} + [y]_{mn}) = \theta([x + y]_{mn}) = ([x + y]_m, [x + y]_n)$$

$$= ([x]_m, [x]_n) + ([y]_m, [y]_n) = \theta([x]_{mn}, [y]_{mn}) = \theta([x]_{mn}) + \theta([y]_{mn}) \ .$$

So θ is a homomorphism.

It remains only to show that θ is bijective. Since $|\mathbb{Z}/m \times \mathbb{Z}/n| = mn = |\mathbb{Z}/mn|$, it suffices to show that θ is injective. Given $[x]_{mn} \in \ker(\theta)$, then $x \in m\mathbb{Z} \cap n\mathbb{Z} = mn\mathbb{Z}$ because m and n are coprime. Hence $[x]_{mn} = 1$. We have shown that $\ker(\theta)$ is the trivial subgroup of $\mathbb{Z}/mn$. It now follows from the First Isomorphism Theorem that θ is injective, as required. □

Theorem 3.15: (Multiplicative Chinese Remainder Theorem.) *Let m and n be coprime positive integers. Then there is an isomorphism*

$$(\mathbb{Z}/m)^\times \times (\mathbb{Z}/n)^\times \leftarrow (\mathbb{Z}/mn)^\times$$

given by $([z]_m, [z]_n) \leftarrow\!\shortmid [z]_{mn}$ where z is an integer coprime to mn.

Proof: Let z be any integer. Then z is coprime to mn if and only if z is coprime to both m and n. So, by the previous theorem, there exists a bijection $\phi(\mathbb{Z}/m)^\times \times (\mathbb{Z}/n)^\times \leftarrow (\mathbb{Z}/mn)^\times$ given by $([z]_m, [z]_n) \leftarrow\!\shortmid [z]_{mn}$. Now let x and y be integers coprime to mn. Then

$$\phi([x]_{mn}[y]_{mn}) = \theta([xy]_{mn}) = ([xy]_m, [xy]_n)$$
$$= ([x]_m, [x]_n)([y]_m, [y]_n) = \phi([x]_{mn}, [y]_{mn}) = \phi([x]_{mn})\phi([y]_{mn}) \ .$$

So the bijection ϕ is an isomorphism. □

Let us combine the latest two theorems, and express the conclusions in a form that is sometimes convenient.

Theorem 3.16: (Chinese Remainder Theorem, group-theoretic version.) *Let n_1, ..., n_r be mutually coprime positive integers. Then:*
(1) *There is an isomorphism of abelian groups*

$$\mathbb{Z}/n_1 \times ... \times \mathbb{Z}/n_r \leftarrow \mathbb{Z}/n_1...n_r$$

given by $([z]_{n_1}, [z]_{n_r}) \leftarrow\!\shortmid [z]_{n_1...n_r}$ for $z \in \mathbb{Z}$.
(2) *There is an isomorphism of abelian groups*

$$(\mathbb{Z}/n_1)^\times \times ... \times (\mathbb{Z}/n_r)^\times \leftarrow (\mathbb{Z}/n_1...n_r)^\times$$

given by $([z]_{n_1}, [z]_{n_r}) \leftarrow\!\shortmid [z]_{n_1...n_r}$ for $z \in \mathbb{Z}$ such that $n_1..., n_r$ and z are coprime.

Proof: This holds by repeated application of the previous two theorems. □

Sylow's Theorem for finite abelian groups: In this section, we shall be discussing a special case of the theorem, called Sylow's Theorem, which will be presented in full generality in Chapter 7.

For a prime p, an element a of an abelian group A is called a **p-element** provided a has finite order and $|\langle a \rangle|$ is a power of p.

Theorem 2.X: (Sylow's Theorem in the case of finite abelian groups.) *Let A be a finite abelian group. Write*

$$|A| = p_1^{\alpha_1}...p_m^{\alpha_r}$$

where p_1, ..., p_r are mutually distinct primes and α_1, ..., α_r are natural numbers. For each integer i in the range $1 \leq i \leq r$, let A_i be the set of p_i-elements of A. Then A_i is a subgroup of A and

$$A \cong A_1 \times ... \times A_r \ .$$

Proof: It is clear that each A_i is a subgroup of A. Let $a \in A$. Define $n = |\langle a \rangle|$. By the Additive Chinese Remainder Theorem,

$$\langle a \rangle \cong \mathbb{Z}/n \cong \mathbb{Z}/n_1 \times ... \times \mathbb{Z}/n_r$$

where n_i is the largest power of p_i dividing n. Therefore, a can uniquely be expressed in the form $a = a_1...a_r$ where each a_i is a p_i-element. The uniqueness condition, here, is that if $a = a'_1...a'_r$ where each a'_i is a p_i-element, then each $a_i = a'_i$. $\square$