§ 4 Groups

Groups

Definition 4.1

A group is a set G equipped with a binary operation $*$ that satisfies

$G1)$ (Associativity) For all $a,b,c \in G$, we have $(a*b)*c = a*(b*c)$.

$G2)$ (Existence of Identity) There exists $e \in G$ such that for all $a \in G$, we have $a*e = e*a = a$.

$G3)$ (Existence of Inverse) For all $a \in G$, there exists $b \in G$ such that $a*b = b*a = e$.

Caution: For simplicity, some simply write ab instead of $a*b$ and readers may misunderstand that a group operation must be a multiplication.

If G is a group, then the order of G is defined as the cardinality of G, which is denoted by $|G|$. In particular, if G has finite number of elements, $|G|$ is just the number of elements of G.

Example 4.1

$\mathbb{Z}$ with usual addition $+$ is a group and the identity element 0.

$\mathbb{Z}$ with usual multiplication $\cdot$ is NOT a group (identity $= 1$, but 0 has no inverse)

$\mathbb{Z}^\times = \mathbb{Z} \setminus \{0\}$ with usual multiplication $\cdot$ is a NOT group (identity element $= 1$, we know $2 \cdot \frac{1}{2} = \frac{1}{2} \cdot 2 = 1$, but $\frac{1}{2} \notin \mathbb{Z}$!)

In fact, $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ with usual additions are groups.

Similarly, $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$ and $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$ with usual multiplication are groups.

Example 4.2

$\mathbb{Z}/n\mathbb{Z} = \{[0],[1],\cdots,[n-1]\}$ with addition $+$ is a group and the identity element $[0]$

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

Remark: Sometimes, for simplicity, the bracket [ ] may be dropped.

Example 4.3

$(\mathbb{Z}/n\mathbb{Z})^\times = \{[a] \in \mathbb{Z}/n\mathbb{Z} : \gcd(a,n) = 1\}$ with multiplication $\cdot$ is a group and the identity element $[1]$.

1) Prove that if $[a], [b] \in (\mathbb{Z}/n\mathbb{Z})^\times$, then $[ab] \in (\mathbb{Z}/n\mathbb{Z})^\times$.

   (i.e. if $\gcd(a,n) = \gcd(b,n) = 1$, then $\gcd(ab,n) = 1$)

2) If $\gcd(a,n) = 1$, then there exist $b, q \in \mathbb{Z}$ such that $ab + nq = 1$.

   Therefore, $\gcd(b,n) = 1$ and so $[b] \in (\mathbb{Z}/n\mathbb{Z})^\times$ with $[a][b] = [1]$

$|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$.

Example 4.4

$M_{n\times n}(\mathbb{R})$ = the set of all $n\times n$ real matrices with matrix addition is a group and the identity element is the zero matrix O_n.

$GL_n(\mathbb{R})$ = the set of all $n\times n$ real matrices with nonzero determinant with matrix multiplication is a group and the identity element is the identity matrix I_n.

$SL_n(\mathbb{R})$ = the set of all $n\times n$ real matrices with determinant 1. with matrix multiplication is a group and the identity element is the identity matrix I_n.

Example 4.5

Let A be a nonempty set and let $S_A = \{f : A \to A \text{ bijective}\}$.

Then S_A with the composition of functions forms a group and the identity element is the identity function on A.

In particular, if $|A| = n$, then $|S_A| = n!$

Definition 4.2

A group $(G, *)$ is abelian if $a * b = b * a$ for all $a, b \in G$ (i.e. $*$ is commutative).

Note that : $GL_n(\mathbb{R})$ and $SL_n(\mathbb{R})$ are not abelian.

Proposition 4.1

Let $(G,*)$ be a group and let $a,b,c \in G$.

1) (Left cancellation) If $a*b = a*c$, then $b=c$.

2) (Right cancellation) If $b*a = c*a$, then $b=c$.

proof:

Suppose that $a*b = a*c$.

By $\mathcal{G}3$, there exists $a' \in G$ such that $a'*a = a*a' = e$. Then,

$$a*b = a*c$$

$$a'*(a*b) = a'*(a*c)$$

$$(a'*a)*b = (a'*a)*c \qquad (\because \mathcal{G}1)$$

$$e*b = e*c$$

$$b = c \qquad (\because \mathcal{G}2)$$

Corollary 4.1

Let $(G,*)$ be a group. Then inverse of an element in G is unique.

proof:

Let $a \in G$. Suppose that $b,c \in G$ are inverse of a, then

$$b*a = c*a = e$$

$$b = c \qquad \text{(Right cancellation)}$$

Remark: Since inverse of an element $a \in G$ must be unique, we denote it as a^{-1}.

Think: Is the inverse of a square matrix with nonzero determinant unique?

Is the inverse function of a bijective function $f: A \to A$ unique?

Do we need to prove the above one by one?

Exercise 4.1

Let $(G,*)$ be a group. Show that identity element in G is unique

Remark: The unique identity element in G is usually denoted by e.

Definition 4.3

If a subset H of a group $(G, *)$ is closed under $*$ and if H with the induced operation from G is itself a group, then H is said to be a subgroup of G.

In particular, every group has a trivial subgroup $\{e\}$.

Example 4.6

Let $n \in \mathbb{Z}^+$ and $n\mathbb{Z} = \{na \in \mathbb{Z} : a \in \mathbb{Z}\}$. Then $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ (with $+$).

If $n > 1$ and let $H = \{na+1 \in \mathbb{Z} : a \in \mathbb{Z}\}$, then H is not a group since there is no identity element.

Example 4.7

$SL_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$.

Proposition 4.2

A subset H of a group G is a subgroup of G if and only if

1) H is closed under the group operation of G,

2) the identity element e of G is in H.

3) for all a in H, a^{-1} is also in H.

Exercise 4.2

Let $P = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} : a, b \in \mathbb{R},\ a^2 + b^2 \neq 0 \right\}$

Show that P with matrix multiplication is a subgroup of $GL_2(\mathbb{R})$.

Group Isomorphisms

Definition 4.4

Let G, G' be groups.

A function $f : G \to G'$ is said to be a group homomorphism from G to G' if

$f(ab) = f(a)f(b)$ for all $a, b \in G$.

In particular, if a bijective group homomorphism is said to be an group isomorphism.

" isomorphism = same structure "

Example 4.8

Let $f: GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^\times$ defined by $f(A) = \det(A)$

Then $f(AB) = \det(AB) = \det(A) \cdot \det(B) = f(A) \cdot f(B)$,

so f is a group homomorphism.

Example 4.9

Let $f: \mathbb{C}^\times \longrightarrow P$ defined by $f(a+bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$

$$f((a+bi)\cdot(c+di)) = f((ac-bd)+(ad+bc)i) = \begin{pmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{pmatrix} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}\begin{pmatrix} c & -d \\ d & c \end{pmatrix} = f(a+bi)\cdot f(c+di)$$

$\therefore f$ is a group homomorphism.

Also, f is bijective (exercise), so f is a group isomorphism.

Proposition 4.4

Let $f: G \to G'$ be a group homomorphism

1) f sends the identity element e of G to the identity element e' of G'.

2) $f(a^{-1}) = f(a)^{-1}$ for all $a \in G$.

3) If H is a subgroup of G, then the image of H under f is a subgroup of G'.

4) If H' is a subgroup of G', then the preimage of H' under f is a subgroup of G.

Cyclic Groups

Let $(G, *)$ be a group and let $a \in G$.

We denote $a * a$ by a^2, a by a^1, e by a^0, $a^{-1} * a^{-1}$ by a^{-2} and so on, then

Proposition 4.5

$\langle a \rangle := \{a^n : n \in \mathbb{Z}\}$ is a subgroup of G and it is said to be the cyclic subgroup generated by a.

Example 4.10

Let $R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \in SL_2(\mathbb{R})$

Note $R_\theta^n = R_{n\theta}$, so $\langle R_\theta \rangle = \{R_{n\theta} : n \in \mathbb{Z}\}$

In particular, if $\theta = \frac{2a\pi}{b}$ where $a, b \in \mathbb{Z}^+$ and $\gcd(a,b) = 1$, $\langle R_\theta \rangle$ has ab elements.

Example 4.11

Recall: $(\mathbb{Z}/15\mathbb{Z})^\times = \{[1],[2],[4],[7],[8],[11],[13],[14]\}$ with multiplication is a group.

Note that $[7]^2 = [4]$, $[7]^3 = [13]$, $[7]^4 = [1]$

$\therefore \langle [7] \rangle = \{[1],[7],[4],[13]\}$

$[1]$ is the identity element and $[7][7]^3 = [7]^3[7] = [7]^4 = [1] \Rightarrow [7]^{-1} = [7]^3 = [13]$ and $[13]^{-1} = [7]$

$[7]^2[7]^2 = [7]^4 = [1] \Rightarrow [4] = [4]^{-1}$

Caution: If the group operation of G is an addition, then we have $a * a = a + a$, instead of writing a^2, we write $2a$

Example 4.12

Recall. $\mathbb{Z}/15\mathbb{Z} = \{[0],[1],[2],\cdots,[14]\}$ with addition is a group.

$\langle [3] \rangle = \{n[3] : n \in \mathbb{Z}\} = \{[0],[3],[6],[9],[12]\}$.

$\langle [4] \rangle = \{n[4] : n \in \mathbb{Z}\} = \mathbb{Z}/15\mathbb{Z}$ (Why?)

Exercise 4.3

Show that $\gcd(a,n) = 1$ if and only if $\langle [a] \rangle = \mathbb{Z}/n\mathbb{Z}$.

(Hint: There exist $s,t \in \mathbb{Z}$ such that $as + nt = 1$.

If $0 \le b \le n-1$, then $asb + ntb = b$ and so $[b] \in \langle [a] \rangle$ (why?))

Definition 4.5

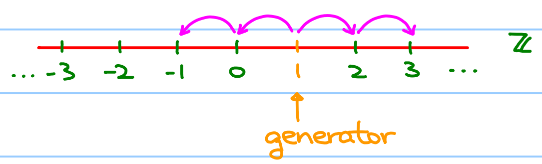
A group G is said to be a cyclic group if $G = \langle a \rangle$ for some $a \in G$.

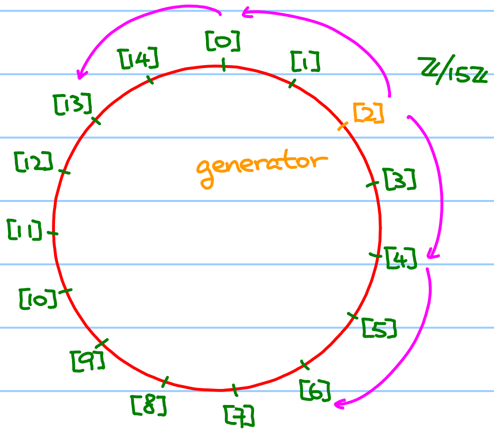
In this case, a is said to be a generator of G.

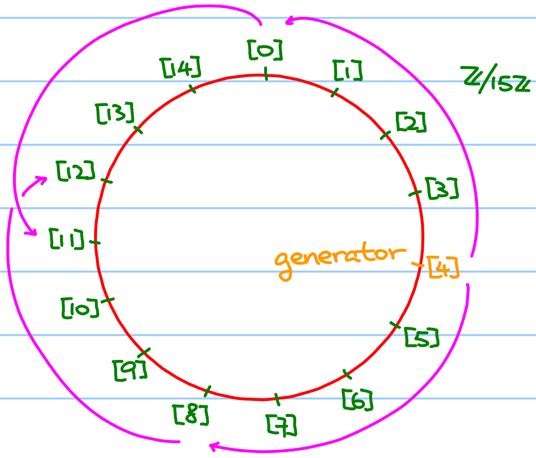
Example 4.13

1 and -1 are the only generator of $\mathbb{Z}$.

$[a]$ is a generator of $\mathbb{Z}/n\mathbb{Z}$ if and only if $\gcd(a,n) = 1$







Example 4.14

$(\mathbb{Z}/15\mathbb{Z})^\times$ is not a cyclic group.

$(\mathbb{Z}/5\mathbb{Z})^\times = \langle [2] \rangle = \langle [3] \rangle$

(See example 3.11)

In general, $(\mathbb{Z}/n\mathbb{Z})^\times$ is a cyclic group if and only if it has a primitive root.

Proposition 4.5

Let G be a cyclic group.

1) If G is a finite group and $|G| = n$, then G is isomorphic to $\mathbb{Z}/n\mathbb{Z}$

2) If G is an infinite group, then G is isomorphic to $\mathbb{Z}$.

(i.e. It suffices to study $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}$ if we would like to study cyclic groups.

Idea of proof of (1):

Let $G = \langle a \rangle$ and $|G| = n$ Define $f: G \to \mathbb{Z}/n\mathbb{Z}$ by $f(a^j) = [j]$ for all $j \in \mathbb{Z}$.

Show that f is a group isomorphism.

Example 4.15

$(\mathbb{Z}/5\mathbb{Z})^\times$ is isomorphic to $\mathbb{Z}/4\mathbb{Z}$.

$[2] \mapsto [1]$	$[3] \mapsto [1]$
$[2]^2 = [4] \mapsto [2] = 2[1]$	$[4] \mapsto [2]$
$[2]^3 = [3] \mapsto [3] = 3[1]$	$[2] \mapsto [3]$
$[2]^4 = [1] \mapsto [0] = 4[1]$	$[1] \mapsto [0]$

However, there are two different isomorphisms.

Cosets and Lagrange's Theorem

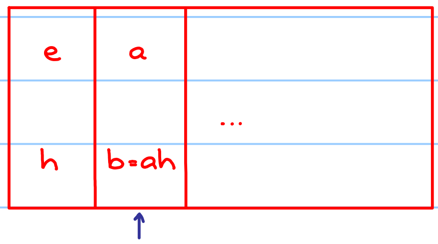
Proposition 4.6

Let H be a subgroup of a group G. Let $\sim_L$ and $\sim_R$ be relation defined on G by

$a \sim_L b$ if and only if $a^{-1}b \in H$, and $a \sim_R b$ if and only if $ab^{-1} \in H$.

Then $\sim_R$ and $\sim_L$ are equivalence relations on G.

$a \sim_L b \Leftrightarrow a^{-1}b \in H \Leftrightarrow b = ah$ for some $h \in H$



Idea. Elements in the equivalence class $[a]$ are in form of ah, where $h \in H$

Definition 4.6

$aH = \{ah : h \in H\}$ and $Ha = \{ha : h \in H\}$ are said to be the left and right coset of H containing a respectively (In fact, aH and Ha are just equivalence classes of a with respect to $\sim_L$ and $\sim_R$.)

In particular, if G is an abelian group, $\sim_L$ and $\sim_R$ gives the same relation on G ($a^{-1}b \in H \Leftrightarrow (a^{-1}b)^{-1} = b^{-1}a = ab^{-1} \in H$) and $aH = Ha$.

Example 4.16

Let $n \in \mathbb{Z}^+$ and let $n\mathbb{Z} = \{nb : b \in \mathbb{Z}\}$ be a subgroup of $\mathbb{Z}$.

All left coset are $a + n\mathbb{Z} = \{a + nb : b \in \mathbb{Z}\}$ where $a = 0, 1, 2, \dots, n-1$

Idea: If each equivalence class has the same number of elements, then

elements in G = # equivalence classes $\times$ # elements of an equivalence class

$$|G| = [G:H] \times |H| \quad \text{(The equivalence class of } e \text{ is } H.)$$

Lemma 4.1

Let H be a subgroup of a group G and let $a \in G$.

Then $f: H \to aH$ defined by $f(h) = ah$ is a bijective function.

(so $|aH| = |H|$ for all $a \in G$.)

Theorem 4.1 (Lagrange's Theorem)

Let G be a finite group and let H be a subgroup of G. Then $|H| \,\big|\, |G|$.

Immediate consequence:

Proposition 4.7

If G is a group of order p, where p is a prime, then G is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

proof:

Since $|G| = p \geq 2$, we can take $a \in G$ such that $a \neq e$.

Note that $e, a \in \langle a \rangle$ and so $|\langle a \rangle| > 1$.

By Lagrange's theorem, $|\langle a \rangle| = p$ and so $G = \langle a \rangle$ which is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

Application to $(\mathbb{Z}/n\mathbb{Z})^\times$:

Let $a \in \mathbb{Z}$ with $\gcd(a,n)$, then $[a] \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Consider the cyclic subgroup $\langle [a] \rangle$ of $(\mathbb{Z}/n\mathbb{Z})^\times$. Then we have $|\langle [a] \rangle| \,\Big|\, |(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$

Therefore, the order of $a = |\langle [a] \rangle| \,\big|\, \varphi(n)$ which proves Euler's theorem.

Exercise 4 4

Show that $\mathbb{Z}/n\mathbb{Z}$ has exactly one subgroup of order d dividing n, and that these are all the subgroups it has.

(Hint: If $d|n$, let $m = \frac{n}{d}$.

Show that $\langle [m] \rangle$ is the only subgroup of order d in $\mathbb{Z}/n\mathbb{Z}$.

The last statement is guaranteed by Lagrange's theorem.)

Example 4.17

$\mathbb{Z}/12\mathbb{Z}$ is a cyclic group and 1, 2, 3, 4, 6, 12 are all divisors of 12.

Therefore, it has 6 subgroups:

subgroups of $\mathbb{Z}/12\mathbb{Z}$	isomorphic to	Number of generator(s)
$\{[0]\}$	trivial group	$\varphi(1)=1$
$\{[0],[6]\}$	$\mathbb{Z}/2\mathbb{Z}$	$\varphi(2)=1$
$\{[0],[4],[8]\}$	$\mathbb{Z}/3\mathbb{Z}$	$\varphi(3)=2$
$\{[0],[3],[6],[9]\}$	$\mathbb{Z}/4\mathbb{Z}$	$\varphi(4)=2$
$\{[0],[2],[4],[6],[8],[10]\}$	$\mathbb{Z}/6\mathbb{Z}$	$\varphi(6)=2$
$\{[0],[1],[2],[3],[4],[5],[6],[7],[8],[9],[10],[11]\}$	$\mathbb{Z}/12\mathbb{Z}$	$\varphi(12)=4$

Those marked in red are generators of the corresponding cyclic subgroups.

Observation: Each element in $\mathbb{Z}/12\mathbb{Z}$ is a generator of exactly one subgroup.

Proposition 4.8

$n=\sum_{d|n}\varphi(d)$.

proof:

Claim: Each element in $\mathbb{Z}/n\mathbb{Z}$ is a generator of exactly one subgroup.

Let $0\leq a\leq n-1$.

Note that $\langle[a]\rangle$ is one of the subgroup of $\mathbb{Z}/n\mathbb{Z}$ and $[a]$ itself is a generator

Also $[a]$ cannot be a generator of two distinct subgroups since

their orders must be distinct.

Therefore the sum of number of generators equals to the number of elements in $\mathbb{Z}/n\mathbb{Z}$,

which implies $n=\sum_{d|n}\varphi(d)$.

Corollary 4.2

If p and q are primes, then $\varphi(pq)=(p-1)(q-1)$.

proof:

By proposition 4.8, $pq=\sum_{d|pq}\varphi(d)=\varphi(1)+\varphi(p)+\varphi(q)+\varphi(pq)$

$=1+(p-1)+(q-1)+\varphi(pq)$

$\therefore \varphi(pq)=pq-p-q+1$

$=(p-1)(q-1)$

Corollary 4.3

If p is a prime and $k \in \mathbb{Z}^+$, then $\varphi(p^k) = p^k - p^{k-1}$

proof:

1) When $k=1$, $\varphi(p) = p-1$

2) Assume that $\varphi(p^r) = p^r - p^{r-1}$ for $r = 1, 2, \cdots, k$.

Then, by proposition 4.8,

$$p^{k+1} = \sum_{d \mid p^{k+1}} \varphi(d) = \sum_{r=0}^{k+1} \varphi(p^r) = \varphi(p^{k+1}) + \left(\sum_{r=1}^{k} p^r - p^{r-1}\right) + \overset{\varphi(1)}{\overset{\shortparallel}{1}} = \varphi(p^{k+1}) + p^k$$

$$\therefore \quad \varphi(p^{k+1}) = p^{k+1} - p^k$$

$\therefore$ By mathematical induction, $\varphi(p^k) = p^k - p^{k-1}$ for all $k \in \mathbb{Z}^+$.

Classification of Finitely Generated Abelian Groups

Proposition 4.9

Let $(G_i, *_i)$ be groups for $i = 1, 2, \cdots, n$

Let $G = \prod_{i=1}^{n} G_i = \{(g_1, g_2, \cdots, g_n) : g_i \in G_i\}$ and define a binary operation $*$ on G

such that $(a_1, a_2, \cdots, a_n) * (b_1, b_2, \cdots, b_n) = (a_1 *_1 b_1, a_2 *_2 b_2, \cdots, a_n *_n b_n)$.

Then $(G, *)$ is a group.

Definition 4.7

An abelian group G is said to be finitely generated if there exist finitely many $g_1, \cdots, g_n \in G$

such that every $x \in G$ can be expressed as $x = g_1^{m_1} g_2^{m_2} \cdots g_n^{m_n}$ for some $m_1, m_2, \cdots, m_n \in \mathbb{Z}$.

In this case, $\{g_1, g_2, \cdots, g_n\}$ is said to be a generating set.

Remark: A finite abelian group must be finitely generated.

Example 4.18

$(\mathbb{Z}/15\mathbb{Z})^* = \{[1], [2], [4], [7], [8], [11], [13], [14]\}$ is a finitely generated abelian group generated

by $[2]$ and $[7]$ since

$[2]^0[7]^0 = [1]$, $[2]^1[7]^0 = [2]$, $[2]^2[7]^0 = [4]$, $[2]^3[7]^0 = [8]$

$[2]^0[7]^1 = [7]$, $[2]^1[7]^1 = [14]$, $[2]^2[7]^1 = [13]$, $[2]^3[7]^1 = [11]$

Example 4.19

$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}$ is a finitely generated abelian group generated by $(1,0)$ and $(0,1)$.

Example 4.20

$\mathbb{Q}^{\times}$ is not finitely generated. (Why?)

Proposition 4.10

Let $m, n \in \mathbb{Z}^{+}$. The group $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is cyclic and is isomorphic to $\mathbb{Z}/mn\mathbb{Z}$ if and only if m, n are relatively prime.

proof:

"$\Leftarrow$" If m, n are relatively prime, the $\operatorname{lcm}(m,n) = mn$.

Consider the subgroup $\langle (1,1) \rangle$,

if r is the least positive integer such that $r(1,1) = 0$, then $r = \operatorname{lcm}(m,n) = mn$.

Therefore, $|\langle 1,1 \rangle| = mn$ and $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} = \langle (1,1) \rangle$.

"$\Rightarrow$" Suppose that $\gcd(m,n) = d > 1$, then $\frac{mn}{d}$ is divisible by both m and n.

Then for any $(r,s) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, we have $\frac{mn}{d}(r,s) = (0,0)$.

(i.e. none of them is a generator!)

Corollary 4.4

The group $\prod_{i=1}^{n} \mathbb{Z}/m_i\mathbb{Z}$ is cyclic and is isomorphic to $\mathbb{Z}/m_1 m_2 \cdots m_n\mathbb{Z}$ if and only if $\gcd(m_i, m_j) = 1$ for all $i \neq j$.

Example 4.21

$72 = 8 \times 9$ and $\gcd(8,9) = 1$, so $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ is isomorphic to $\mathbb{Z}/72\mathbb{Z}$ which is a cyclic group.

Example 4.22

$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is not a cyclic group as $\gcd(4,2) = 2 > 1$.

Exercise 4.5

Let $m_1, m_2, \cdots, m_n \in \mathbb{Z}^{+}$ and let $d = \operatorname{lcm}(m_1, m_2, \cdots, m_n)$.

Prove that $d(g_1, g_2, \cdots, g_n) = (0, 0, \cdots, 0)$ for all $(g_1, g_2, \cdots, g_n) \in \prod_{i=1}^{n} \mathbb{Z}/m_i\mathbb{Z}$.

Theorem 4.2

Every finitely generated abelian group G is isomorphic to $\mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \mathbb{Z}/p_2^{k_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_m^{k_m}\mathbb{Z} \times \mathbb{Z}^r$ where $p_1, \cdots, p_m$ are primes (but not necessary to be distinct), $k_1, \cdots, k_m \in \mathbb{Z}^+$ and $r \geq 0$.

The product is unique up to rearrangement of factors.

Example 4.23

Note that $360 = 2^3 \times 3^2 \times 5$, so an abelian group of order 360 is isomorphic to exactly one of the below:

1) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

2) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

3) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

4) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

5) $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

6) $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

Example 4.24

$(\mathbb{Z}/15\mathbb{Z})^\times = \{[1], [2], [4], [7], [8], [11], [13], [14]\}$ is an abelian group of order $\varphi(15) = 8 = 2^3$

$(\mathbb{Z}/15\mathbb{Z})^\times$ is isomorphic to one of the below:

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}$.

However, we have

$[2]^0[7]^0 = [1]$, $[2]^1[7]^0 = [2]$, $[2]^2[7]^0 = [4]$, $[2]^3[7]^0 = [8]$

$[2]^0[7]^1 = [7]$, $[2]^1[7]^1 = [14]$, $[2]^2[7]^1 = [13]$, $[2]^3[7]^1 = [11]$

and we can see $f: \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to (\mathbb{Z}/15\mathbb{Z})^\times$ defined by $f(m,n) = [2^m \cdot 7^n]$ gives a group isomorphism.