Part II
Permutations, Cosets and Direct Product

Satya Mandal

University of Kansas, Lawrence KS 66045 USA

January 22

8 Permutations

Definition 8.1. Let A be a set.

1. A **a permuation of** A is defined to be a bijective map $\varphi : A \xrightarrow{\sim} A$. (*Usually, we work with permutations of finite sets* A.)

2. Let $\mathcal{S}(A)$ denote the set of permuations of A.

3. The composition, defines a binary operation on $\mathcal{S}(A)$ as follows:

$$\forall \sigma, \tau \in \mathcal{S}(A) \quad define \quad \tau\sigma(x) = \tau(\sigma(x)) \quad \forall x \in A.$$

   It is obvious that

$$\tau, \sigma \in \mathcal{S}(A) \Longrightarrow \tau\sigma \in \mathcal{S}(A)$$

   So, $\mathcal{S}(A)$ is closed under composition.
   Further, as always, composition is associative.

The identity map $Id_A : A \longrightarrow A$ given by $Id_A(x) = x \ \forall x \in A$, is the identity for the composition operation.
Also, a bijectiion $\sigma \in \mathcal{S}(A)$ has an inverse $\sigma^{-1} \in \mathcal{S}(A)$, defined by

$$\sigma^{-1}(y) = x \qquad \text{if} \qquad \sigma(x) = y.$$

So, $\mathcal{S}(A)$ is a group under composition.

4. If A is a finite set with n elements, we can take $A = \{1, 2, \ldots, n\}$.

5. The the group of permutations of $A = \{1, 2, \ldots, n\}$ is denoted by S_n. It is called the **symmetric group on n letters**. Note S_n has $n!$ elements.

Example 8.2. Read examples 8.7 and 8.8. Example 8.7 gives the multiplication table for S_3. Note S_3 has $3! = 6$ elements. Read about **dihedral groups**. *You and I would write down all six elements of S_3 on the board.*

Definition 8.3. *For a positive integer $n \geq 2$, the* **Dihedral group** D_n *is defined to be the group of symmetries of an regular $n-$gon. By a* **symmetry**, *we mean rotation and reflection.*

1. *So, D_3 is the dihedral group of an equilateral triangle. In fact, $D_3 \approx S_3$.*

2. *So, D_4 is the dihedral group of square. For a square, four rotations $(0, \pi/2, \pi, 3\pi/2)$ are possible. With four reflections of the four, we get total of 8 elements. So, $|D_4| = 8$.*

   Each element $\rho \in D_4$ corresponds to a permuation in S_4. In fact, $D_4 \leq S_4$.

Like homomorphisms of binary structures, we define homomorphisms of groups.

Definition 8.4. Suppose $\varphi : G \longrightarrow G'$ be a mapping from a group G to another group G'.

1. We say, φ is a **homomorphism** if $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in G$.

2. Given a subgroup H of G, the **image of H under** φ is defined to be $\varphi(H) := \{\varphi(x) : x \in H\}$

Lemma 8.5. Suppose $\varphi : G \longrightarrow G'$ is a homomorphism of groups. Assume φ is injective. Then the image $\varphi(G)$ is a subgroup of G' and φ induces an isomorphism between G and $\varphi(G)$.

Proof. We do not have to check associativity. Suppose $x, y \in \varphi(G)$. Then $x = \varphi(a), y = \varphi(b)$ for some $a, b \in G$. So, $xy = \varphi(a) = \varphi(ab) \in \varphi(G)$. So, $\varphi(G)$ is closed under multiplication.

Let $e' \in G'$ denote the identity in G'. We calaim: $\varphi(e) = e'$. Because $\varphi(e) = \varphi(ee) = \varphi(e)\varphi(e)$. So, $e' = (\varphi(e)^{-1}(\varphi(e)\varphi(e)) = \varphi(e)$. So, it is established that $e' = \varphi(e)$. Therefore $e' \in \varphi(G)$.

Given $x \in \varphi(G)$, $x = \varphi(a)$ for some $a \in G$. So, $x\varphi(a^{-1}) = \varphi(a)\varphi(a^{-1}) = \varphi(aa^{-1}) = \varphi((e0 = e'$. Similarly, $\varphi(a^{-1})x = e'$. So inverse of x is $\varphi(a^{-1}) \in \varphi(G)$.

This establishes that $\varphi(G)$ is subgroup of G'. Let $f : G \longrightarrow \varphi(G)$ be the mapping induced by φ. Clearly, it is onto and it is also one to one. So, f is bijective. So, G is isomorphic to $\varphi(G)$. The proof is complete. ■

Now, we will prove any group is isomorphic to a group of permutations.

Theorem 8.6 (Cayley's Theorem)**.** Let G be a group. Then, G is isomorphic to a group of permutations.

Proof. Let $\mathcal{S}(G)$ denote the group of permutations of G. Given an element $a \in G$ define a mapping

$$L_a : G \longrightarrow G \qquad by \quad L_a(x) = ax \quad \forall\, x \in G.$$

(*We use notation L_a for left multiplication by a.*) It is easy to see L_a is a bijection. Hence $L_a \in \mathcal{S}(G)$. Define

$$\varphi : G \longrightarrow \mathcal{S}(G) \quad \forall\, a \in G \quad define \quad \varphi(a) = L_a$$

It is easy to see that $\varphi(ab) = \varphi(a)\varphi(b)$. So, φ is a a group homomorphism. Now we calim that φ is one to one. Suppose $\varphi(a) = \varphi(b)$. So, $L_a = L_b$. So, $a = L_a(e) = L_b(e) = b$. So, φ is injective. The theorem is established by lemma 8.5. The proof is complete. ■

Remark. In this proof, we could have tried to use right multiplication $R_a : G \longrightarrow G$, defined by $R_a(x) = xa$. We define

$$\psi : G \longrightarrow \mathcal{S}(G) \quad by \quad \psi(a) = R_a$$

Then, for $x \in G$, we have

$$\psi(ab)(x) = R_{ab}(x) = x(ab) = (xa)b = R_b(R_a(x)) = \psi(b)\psi(a)(x)$$

So, $\psi(ab) = \psi(b)\psi(a)$. ■ ■

Reading Assignment: Read Example 8.17.

9 Orbits, Cycles, the Altrnating group

9.1 Orbits

Definition 9.1. Let A be a set and σ be a (fixed) parmutation on A. We define an equivalence relation $\sim$ on A as follows:

$$for \quad a, b \in A \quad define \quad a \sim b \quad if \quad b = \sigma^n(a) \quad for\ some \quad n \in \mathbb{Z}.$$

Then, (1) $a \sim a$ $\forall a \in A$. So $\sim$ is reflexive. (2) If $a \sim b$ then $b = \sigma^n(a)$. So, $a = \sigma^{-n}(b)$. So, $b \sim a$. This means $\sim$ is symmetric. (3) In fact, σ is also transitive. To see this let $a \sim b \sim c$. Then $b = \sigma^n(a)$ and $c = \sigma^m(b)$ for some $m, n \in \mathbb{Z}$. Hence $c = \sigma^{m+n}(a)$. So, $a \sim c$.

Therefore, $\sim$ is an equivalence relation.

1. An equivalence class of this relation $\sim$ is called an **orbit** of σ.

2. For $a \in A$ the orbit of a is given by

   $$\overline{a} = \{\sigma^n(a) : r \in \mathbb{Z}\}.$$

   If $\overline{a}$ is finite, with r elements, then

   $$\overline{a} = \{\sigma^0(a), \sigma^1(a), \sigma^2(a), \ldots, \sigma^{r-1}(a)\}.$$

3. For example, the identity permutation ι of A, each orbit has one element.

4.

   Example 9.2 (9.3)**.** *Find the orbits of the permutation*

   $$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix}$$

   Solution:

   $$1 \to 3 \to 6 \to 1, \quad 2 \to 8 \to 2, \quad 4 \to 7 \to 5 \to 4$$

9.2 Cycles

Now we assume $A = \{1, 2, \dots, n\}$. As mentioned before, the groups of all its permutations is the symmetric group S_n.

Definition 9.3. Let $r_1, r_2, \dots r_k$ be k distinct elements in $A = \{1, 2, \dots, n\}$. The **notation** $(r_1, r_2, \dots r_k)$ denotes a permutation $\sigma \in S_n$ defined as follows:

$$\begin{cases} \sigma(r_1) = r_2, \sigma(r_2) = r_3, \dots, \sigma(r_{k-1}) = r_k, \sigma(r_k) = r_1, \\ \sigma(r) = r \quad \forall r \neq r_i \end{cases}$$

In particular,

$$\forall\ 2 \leq i \leq k \quad r_i = \sigma^{i-1}(r_1) \quad and \quad \sigma^k = I_A.$$

Definition 9.4. Let $\sigma \in S_n$.

1. We say σ is a **cycle**, if it has at most one orbit with more than one element.
2. Also, define **length** of a cycle to be the number of elements in the largest cycle.
3. Suppose $\sigma \in S_n$ is a cycle, with length k.
   (a) Fix any a in the largest orbit of σ. Then this largest orbit is
   $$\overline{a} = \{\sigma^0(a), \sigma^1(a), \sigma^2(a), \dots, \sigma^{k-1}(a)\}.$$
   (b) Since σ has only one orbit of length more than 1, $\sigma(r) = r$ for $r \neq \sigma^i(a)$.
   (c) We conclude
   $$\sigma = \left(\sigma^0(a), \sigma^1(a), \sigma^2(a), \dots, \sigma^{r-1}(a)\right)$$
   So, any cycle can be described in this form.

Reading Assignment: Examples 9.7

Theorem 9.5. Let $\sigma \in S_n$. Then

$$\sigma = \sigma_1\sigma_2\cdots\sigma_t$$

is a product of disjoint cycles σ_i.

Proof. Let $B_1, B_2, \ldots, B_r$ be the orbits of σ. Define cycles σ_i as follows:

$$\sigma_i(x) = \begin{cases} \sigma(x) & if\ x \in B_i \\ x & otherwise \end{cases}$$

Clearly, $\sigma = \sigma_1\sigma_2\cdots\sigma_r$. They are disjoint too. The proof is complete. ■

Example 9.6 (9.9)**.** *Find the orbits of the permutation*

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

Write σ as product of cycles.

Example 9.7 (9.10)**.** *Compute*

$$(1,4,5,6)(2,1,5) \quad and \quad (2,1,5)(1,4,5,6)$$

9.3 Even and odd Permutations

Definition 9.8. A cycle of length two is called a **transposition**.
So, $\sigma = (1,2) \in S_n$ is a transposition. It maps

$$\begin{cases} 1 \mapsto 2, & \\ 2 \mapsto 1 & \text{and} \\ r \mapsto r & \forall\ r \geq 3. \end{cases}$$

Lemma 9.9. Any cycle is a product of transpositions.

Proof. We have

$$(1, 2, \ldots, r) = (1, n)(1, n-1) \cdots (1, 3)(1, 2)$$

It goes as follows:

1. $1 \mapsto 2$
2. $2 \mapsto 1 \mapsto 3$
3. $3 \mapsto 1 \mapsto 4$
4. so on.

The proof is complete. ■

Corollary 9.10. Any permutation $\sigma \in S_n$ is product of transpostions.

Proof. σ is product of cycles and each cycle is product of transpostions. The proof is complete. ■

Theorem 9.11. Let $\sigma \in S_n$. Then, σ can be written as product of either **even number** of transpositions or **odd number** of transpositions, not both.

Proof. (This proof seems cheating.)
Let C be the matrix obtained by applying σ to the rows of the identity matrix. If σ is product of even number of transpositions, then $\det C = 1$. If σ is product of odd number of transpositions, then $\det C = -1$. So, it cannot be both. The proof is complete. ■

Definition 9.12. Let $\sigma \in S_n$. We say σ is an **even permutation**, if it is product of even number of transpositions. We say σ is an **odd permutation**, if it is product of odd number of transpositions.

9.4 Alternating Groups

Proposition 9.13. Let

$$A_n = \{\sigma \in S_n : \sigma \textit{ is an even permutation}\}$$

and

$$B_n = \{\sigma \in S_n : \sigma \textit{ is an odd permutation}\}.$$

Then, A_n and B_n have same number of elements.

Proof. We define a map

$$\lambda : A_n \longrightarrow B_n \qquad by \quad \lambda(\sigma) = (1,2)\sigma$$

Define

$$\mu : B_n \longrightarrow A_n \qquad by \quad \lambda(\sigma) = (1,2)\sigma$$

Then, $\mu\lambda(\sigma) = (1,2)(1,2)\sigma = \sigma$. So, $\mu\lambda = ID$. Similarly, $\lambda\mu = ID$. So, λ is bijective. The proof is complete. ■

Theorem 9.14. A_n is a subgroup of S_n. The order of A_n is $n!/2$.

Proof. A_n is closed under composition. The identity $\iota = (1,2)(2,1) \in A_n$. The inverse of an even permutation is even. So, A_n is a subgroup.

Also, $S_n = A_n \cup B_n$, $A_n \cap B_n = \phi$ and A_n, B_n have same number of elements. So, order of A_n is $n!/2$. The proof is complete. ■

Definition 9.15. A_n is called the **Alternating group on n objects**.

10 Coset and order of subgroups

Abstract

For (finite) groups $H \leq G$, we will provide a partition of G and prove the order of H divides order of G.

10.1 Cosets

Theorem 10.1. Let G be a group and H be a subgroup of G. Define relations $\sim_L$ and $\sim_R$ as follows:

$$\forall \quad a, b \in G \quad define \quad a \sim_L b \quad if \quad a^{-1}b \in H$$

and

$$\forall \quad a, b \in G \quad define \quad a \sim_R b \quad if \quad ab^{-1} \in H.$$

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

Proof. We only show $\sim_R$ is an equivalence relations on G (other one left as exercise).

1. (**Reflexive:**)

$$\forall\, a \in G, \quad aa^{-1} = e \in H. \quad So, \quad a \sim_R a.$$

   So, $\sim_R$ is reflexive.

2. (**Symmetric:**) For $a, b \in G$ we have

$$a \sim_R b \Longrightarrow ab^{-1} \in H \Longrightarrow (ab^{-1})^{-1} \in H \Longrightarrow ba^{-1} \in H \Longrightarrow b \sim_R a.$$

   So, $\sim_R$ is symmetric.

3. (**Transitive:**) For $a, b, c \in G$ we have

$$a \sim_R b \sim_R c \Longrightarrow ab^{-1}, bc^{-1} \in H \Longrightarrow ac^{-1} = (ab^{-1})(bc^{-1}) \in H \Longrightarrow a \sim_R c.$$

   So, $\sim_R$ is transitive.

So, $\sim_R$ is an equivalence relation. ■

Now we compute the equivalence classes (the cells) for $\sim_L$ and $\sim_R$.

1. For $a \in G$ define
$$\begin{cases} Ha = \{xa : x \in H\} & \text{called the right coset of } \ a \\ aH = \{ax : x \in H\} & \text{called the left coset of } \ a \end{cases}$$
2. The map $f : H \longrightarrow Ha$ defined by $f(x) = xa$ is bijective. Similalry, $g : H \longrightarrow aH$ defined by $g(x) = ax$ is bijective. So, H, Ha, aH have same cardinality. Notationally,
$$|H| = |Ha| = |aH|$$
3. If G is abelian then $Ha = aH$ for all $a \in G$.

Lemma 10.2. For the relation $\sim_R$, the equivalence class of $a \in G$ is the right coset Ha. For the relation $\sim_L$, the equivalence class of $a \in G$ is the left coset aH.

Proof. We will give a proof only for $\sim_R$ and the other one is left as an exercise. Let $\overline{a}$ denote the equivlence class of a, for the relation $\sim_R$. Now,
$$x \in \overline{a} \Longleftrightarrow x \sim_R a \Longleftrightarrow xa^{-1} \in H \Longleftrightarrow x \in Ha.$$
So, $\overline{a} = Ha$. The proof is complete. ■

It follows from properties of equivalence classes that the left cosets (*respectively right cosets*) partitions G. This means
$$G = \bigcup_{a \in G} aH \quad and \quad \forall\, a, b \in G \quad either \quad (aH = bH \quad or \quad aH \cap bH = \phi).$$

Theorem 10.3 (Theorem of Lagrange)**.** Let G be a finite group and H be subgroup of G. Then, the order of H divides the order of G.

Proof. Let r be the number of left cosets of H. Let $m = |H|, n = |G|$. Then $m = |aH|$ for all $a \in G$. Since the left cosets partions G we have
$$|G| = |H|\, r = mr.$$
The proof is complete. ■ ‘

Corollary 10.4. Suppose G is a group of prime order. Then G is cyclic.

Proof. Let $a \in G$ and $a \neq e$. Then, $H = \langle a \rangle$ is subgroup of order at least two. Since $|H|$ divides $|G|$, we have $|G| = |H|$. So, $G = H = \langle a \rangle$ is cyclic. The proof is complete. ■

Corollary 10.5. Suppose G is a group of prime order p. Then $G \approx \mathbb{Z}_p$.

Proof. First $G = \langle a \rangle$ is cyclic. We showed before, the map

$$\varphi : \mathbb{Z}_p \longrightarrow G \qquad \overline{r} \mapsto a^r$$

is an isomprphism. The proof is complete. ■

Definition 10.6. Let G be a group and $a \in G$. Then the **order of a** is defined to be the order of the cyclic group $\langle a \rangle$. Order of a is denoted by $o(a)$. So,

$$o(a) := |\langle a \rangle|.$$

In fact,

$$o(a) = \min\{n > 0 : a^n = 1\}$$

Corollary 10.7. Let G be a finite group and $a \in G$. The order of a divides the order of G.

Proof. Trivial.

Here is an important number.

Definition 10.8. Let G be a finite group and H be a subgroup of G. The number of left cosets of H in G is defined to be the **index of H in G**. The index of H in G, is denoted by $(G : H)$. So,

$$(G : H) = \frac{|G|}{|H|}.$$

Note this this is also the number of right cosets of H.

Theorem 10.9. Let G be a finite group and H, K are subgroup of G. Assume $K \leq H \leq G$. Then

$$(G : K) = (G : H)(H : K).$$

Proof. We have

$$(G : K) = \frac{|G|}{|K|}, \quad (G : H) = \frac{|G|}{|H|}, \quad and \quad (H : K) = \frac{|H|}{|K|}$$

The proof is complete. ∎

11 Direct Product

Direct product could be defined in any category. Here we do it in the category of groups.

Definition 11.1. We define direct product of groups.

1. Let G_1 and G_2 be two groups. We define a binary product on $G_1 \times G_2$ as follows:

   $$\forall\, (a_1, a_2), (b_1, b_2) \in G_1 \times G_2 \quad define \quad (a_1, a_2) \cdot (b_1, b_2) := (a_1 b_1, a_2 b_2)$$

   Then, $(G_1 \times G_2, \cdot)$ is a group, to be called the **direct product of G_1 and G_2**. Here

   (a) $e = (e_1, e_2) \in G_1 \times G_2$ is the identity of this product, where e_i is the identity of G_i.

   (b) Also $(a_1, a_2)^{-1} = \left(a_1^{-1}, a_2^{-1}\right)$.

2. More generally, let $G_1, G_2, \ldots, G_n$ be finitely many groups. Define a binary product on the cartesian product $G_1 \times G_2 \times \cdots \times G_n$ as follows

   $$\forall\ (a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n) \in G_1 \times G_2 \times \cdots \times G_n \quad define$$

   $$(a_1, a_2 \ldots, a_n) \cdot (b_1, b_2 \ldots, b_n) := (a_1 b_1, a_2 b_2, \ldots, a_n b_n)$$

   Then, $(G_1 \times G_2 \times \cdots \times G_n, \cdot)$ is a group, to be called the **direct product of $G_1, G_2, \ldots, G_n$**. Here

   (a) $e = (e_1, e_2, \ldots, e_n) \in G_1 \times G_2 \times \cdots \times G_n$ is the identity of this product, where e_i is the identity of G_i.

   (b) Also $(a_1, a_2, \ldots, a_n)^{-1} = \left(a_1^{-1}, a_2^{-1} \ldots, a_n^{-1}\right)$.

3. The direct product of $G_1, G_2, \ldots, G_n$ is also denoted by

   $$\prod_{i=1}^{n} G_i \qquad \text{OR} \qquad G_1 \times G_2 \times \cdots \times G_n$$

Proof. Trivial.

Example 11.2. 1. $\mathbb{Z}_2 \times \mathbb{Z}_3$ is a cyclic group. (see 11.3)

2. $\mathbb{Z}_3 \times \mathbb{Z}_3$ is not cyclic. (see 11.4)

Theorem 11.3. The group $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic if and only if m and n are relatively prime.

Proof. First, note that the order $|\mathbb{Z}_m \times \mathbb{Z}_n| = mn$.
($\Leftarrow$): Assume m and n are relatively prime. Write $o(\overline{1}, \overline{1}) = k$. (*Here, we use additive notation, unlike our default product notation.*) So

$$k(\overline{1}, \overline{1}) = (\overline{0}, \overline{0}). \quad \textit{or} \quad (\overline{k}, \overline{k}) = (\overline{0}, \overline{0})$$

[Recall, by notation $k(\overline{1}, \overline{1}) = (\overline{1}, \overline{1}) + \cdots + (\overline{1}, \overline{1})$.]
So, $\overline{k} = \overline{0}$ in $\mathbb{Z}_m$ and $\overline{k} = \overline{0}$ in $\mathbb{Z}_n$. So, k is divisible by m and n. Since, m, n are relatively prime, it follows mn divides k. Since

$$k = o(\overline{1}, \overline{1}) \leq mn = |\mathbb{Z}_m \times \mathbb{Z}_n|$$

it follows that $k = mn$. Therefore, $\langle(\overline{1}, \overline{1})\rangle = \mathbb{Z}_m \times \mathbb{Z}_n$. So, it is established that $\mathbb{Z}_m \times \mathbb{Z}_n$ cyclic, and is generated by $(\overline{1}, \overline{1})$. Since $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic of order mn, it is isomorphic to $\mathbb{Z}_{mn}$. This completes the proof of ($\Leftarrow$).

($\Rightarrow$): Now assume that $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic. Write $\gcd(m, n) = d$. We need to prove $d = 1$. Let $u = \frac{mn}{d}$. Both m and n divide u. So,

$$\forall \quad a = (\overline{r}, \overline{s}) \in \mathbb{Z}_m \times \mathbb{Z}_n \Longrightarrow ua = (\overline{ur}, \overline{us}) = (\overline{0}, \overline{0}).$$

So,

$$\forall \qquad a \in \mathbb{Z}_m \times \mathbb{Z}_n \quad \textit{we have} \quad o(a) \leq u.$$

Since $\mathbb{Z}_m \times \mathbb{Z}_n = \langle x \rangle$ is cyclic, its generator x has order mn.
So, $o(x) = mn \leq u = \frac{mn}{d}$. So, $d = 1$. The proof is complete. ∎

Inductively, it follows

Corollary 11.4. $\prod_{i=1}^{n} \mathbb{Z}_{m_i}$ is cyclic if and only if the integers $m_1, m_2, \ldots, m_n$ are pair wise relatively prime.

Example 11.5 (11.7)**.** Let $n = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$, where p_i are distinct primes. Then,

$$\mathbb{Z}_n = \prod_{i=1}^{r} \mathbb{Z}_{p_i^{n_i}}$$

Exercise 11.6. Find the order of $(8, 4, 10)$ in $\mathbb{Z}_{12} \times \mathbb{Z}_{60} \times \mathbb{Z}_{24}$. (see 11.10)

Answer is the lcm of the order of these three.

11.1 Extra

We discusss some properties direct product, which applies to other categories.

Lemma 11.7. Let G_1, G_2 be two groups.

1. Then, the projections

$$\begin{cases} \pi_1 : G_1 \times G_2 \longrightarrow G_1 & \textit{sending} \quad (g_1, g_2) \mapsto g_1 \\ \pi_2 : G_1 \times G_2 \longrightarrow G_2 & \textit{sending} \quad (g_1, g_2) \mapsto g_2 \end{cases}$$

   are group homomorphisms.

2. Also, the maps

$$\begin{cases} \iota_1 : G_1 \longrightarrow G_1 \times G_2 & \textit{sending} \quad g \mapsto (g, e_2) \\ \iota_2 : G_2 \longrightarrow G_1 \times G_2 & \textit{sending} \quad g \mapsto (e_1, g) \end{cases}$$

   are injective group homomorphism.

More Generally:

Example 11.8. Suppose $G_1, G_2, \ldots, G_n$ are groups.

1. Prove the projection map

$$\pi_i : G_1 \times G_2 \times \cdots \times G_n \mapsto G_i \qquad \textit{sending} \quad (g_1, g_2, \cdots, g_n) \mapsto g_i$$

   is a group homomorphism.

2. Consider the map

$$\iota_i : G_i \longrightarrow: G_1 \times G_2 \times \cdots \times G_n \qquad \textit{sending} \quad g \mapsto (e_1, e_2, \ldots, g, \ldots e_n)$$

where g is at the $i^{th}-$coordinate. Prove ι_i is an injective homomorphism.

Proof.

1. Let $x = (g_1, g_2, \ldots, g_n), y = (h_1, h_2, \ldots, h_n)$ be in $G_i \longrightarrow: G_1 \times G_2 \times \cdots \times G_n$. Then

$$\pi_i(xy) = \pi(g_1h_1, g_2h_2, \ldots, g_nh_n) = g_ih_i = \pi(x)\pi(y).$$

So, by definition, π is a homomorphism.

2. Let $g, h \in G_i$. Then

$$\iota_i(gh) = ((e_1, e_2, \ldots, gh, \ldots e_n) = (e_1, e_2, \cdots, g, \ldots e_n)(e_1, e_2, \cdots, h, \ldots e_n) = \iota(g)\iota(h).$$

So, by definition, ι is a homomorphism. To prove injectivity, let

$$\iota_i(g) = \iota(h). \quad \textit{Then}, \quad (e_1, e_2, \cdots, g, \ldots e_n) = (e_1, e_2, \cdots, h, \ldots e_n)$$

So, $g = h$.

The proof is complete. ■

The direct product has the following "universal property":

Lemma 11.9. Let G_1, G_2 and H be groups. For $i = 1, 2$, let

$$\text{For } i = 1, 2 \quad \begin{cases} \pi_i : G_1 \times G_2 \longrightarrow G_i & \text{be the projections} \\ p_i : H \longrightarrow G_i & \text{any two group homomorphims} \end{cases}$$

Then, there is a a unique group homomorphims $\Delta : H \longrightarrow G_1 \times G_2$ such that $\pi_1\Delta = p_1$ and $\pi_2\Delta = p_2$. Diagramtically:

$$\begin{tikzcd}
H \arrow[dr, dashed, "\Delta", "\exists!"'] \arrow[drr, bend left, "p_1"] \arrow[ddr, bend right, "p_2"'] & & \\
& G_1 \times G_2 \arrow[r, "\pi_1"'] \arrow[d, "\pi_2"] & G_1 \\
& G_2 &
\end{tikzcd}$$

commutes.

11.2 Structure of finitely generate abelian groups

Usually, theory of abelian groups is easier than that of non-commutative groups. We can say more about abelian groups.

Theorem 11.10 (Fundamental Theorem of Abelian Groups)**.** Let G be a finitely generated abelian groups. Then G is isomorphis to the product of cyclic groups:

$$\mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \cdots \times \mathbb{Z}_{p_r^{n_r}} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$

where p_i are prime numbers, not necessarily distinct and n_i are positive integers.

Proof. Omitted. ∎

12 Plane Isometries

We skip.