Math 2070 Week 5

Group Homomorphisms, Rings

Claim 5.1. *Any cyclic group of finite order n is isomorphic to $\mathbb{Z}_n$.*

Proof of Claim 5.1. Sketch of Proof:

By definition, a cyclic group G is equal to $\langle g \rangle$ for some $g \in G$. Moreover, $\operatorname{ord} g = \operatorname{ord} G$.

Define a map $\phi : \mathbb{Z}_n \longrightarrow G$ as follows:

$$\phi(k) = g^k, \quad k \in \{0, 1, 2, \ldots, n-1\}.$$

Show that ϕ is a group isomorphism.

(For reference, see the discussion of Example 4.15.) $\square$

Corollary 5.2. *If G and G' are two finite cyclic groups of the same order, then G is isomorphic to G'.*

Exercise 5.3. An infinite cyclic group is isomorphic to $(\mathbb{Z}, +)$.

Exercise 5.4. Let G be a cyclic group, then any group which is isomorphic to G is also cyclic.

5.1 Product Group

Let $(A, *_A), (B, *_B)$ be groups. The direct product:

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

has a natural group structure where the group operation $*$ is defined as follows:

$$(a, b) * (a', b') = (a *_A a', b *_B b'), \quad (a, b), (a', b') \in A \times B.$$

The identity element of $A \times B$ is $e = (e_A, e_B)$, where e_A, e_B are the identity elements of A and B, respectively.

For any $(a, b) \in A \times B$, we have $(a, b)^{-1} = (a^{-1}, b^{-1})$, where a^{-1}, b^{-1} are the inverses of a, b in the groups A, B, respectively.

For any collection of groups $A_1, A_2, \ldots, A_n$, we may similarly define a group operation $*$ on:

$$A_1 \times A_2 \times \cdots \times A_n := \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i, i = 1, 2, \ldots n\}.$$

That is:

$$(a_1, a_2, \ldots, a_n) * (a_1', a_2', \ldots, a_n') = (a_1 *_{A_1} a_1', a_2 *_{A_2} a_2', \ldots, a_n *_{A_n} a_n')$$

The identity element of $A_1 \times A_2 \times \cdots \times A_n$ is:

$$e = (e_{A_1}, e_{A_2}, \ldots, e_{A_n}).$$

For any $(a_1, a_2, \ldots, a_n) \in A_1 \times A_2 \times \cdots \times A_n$, its inverse is:

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

Exercise 5.5. $\mathbb{Z}_6$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_3$.

Proof of Exercise 5.5. **Hint:**

Show that $\mathbb{Z}_2 \times \mathbb{Z}_3$ is a cyclic group generated by $(1, 1)$. □

Example 5.6. The cyclic group $\mathbb{Z}_4$ is not isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Proof of Example 5.6. Each element of $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ is of order at most 2. Since $|G| = 4$, G cannot be generated by a single element. Hence, G is not cyclic, so it cannot be isomorphic to the cyclic group $\mathbb{Z}_4$. □

Exercise 5.7. Let G be an abelian group, then any group which is isomorphic to G is abelian.

Example 5.8. The group D_6 has 12 elements. We have seen that $D_6 = \langle r_1, s \rangle$, where r_1 is a rotation of order 6, and s is a reflection, which has order 2. So, it is reasonable to ask if D_6 is isomorphic to $\mathbb{Z}_6 \times \mathbb{Z}_2$. The answer is no. For $\mathbb{Z}_6 \times \mathbb{Z}_2$ is abelian, but D_6 is not.

Claim 5.9. *The dihedral group D_3 is isomorphic to the symmetric group S_3.*

Proof of Claim 5.9. We have seen that $D_3 = \langle r, s \rangle$, where $r = r_1$ and s is any fixed reflection, with:

$$\operatorname{ord} r = 3, \quad \operatorname{ord} s = 2, \quad srs = r^{-1}.$$

In particular , any element in D_3 may be expressed as $r^i s^j$, with $i \in \{0,1,2\}$, $j \in \{0,1\}$.

We have also seen that $S_3 = \langle a, b \rangle$, where:

$$a = (123), \quad b = (12), \quad \operatorname{ord} a = 3, \quad \operatorname{ord} b = 2, \quad bab = a^{-1}.$$

Hence, any element in S_3 may be expressed as $a^i b^j$, with $i \in \{0,1,2\}$, $j \in \{0,1\}$.

Define map $\phi : D_3 \longrightarrow S_3$ as follows:

$$\phi(r^i s^j) = a^i b^j, \quad i, j \in \mathbb{Z}$$

We first show that ϕ is well-defined: That is, whenever $r^i s^j = r^{i'} s^{j'}$, we want to show that:

$$\phi(r^i s^j) = \phi(r^{i'} s^{j'}).$$

The condition $r^i s^j = r^{i'} s^{j'}$ implies that:

$$r^{i-i'} = s^{j'-j}$$

This holds only if $r^{i-i'} = s^{j'-j} = e$, since no rotation is a reflection.

Since $\operatorname{ord} r = 3$ and $\operatorname{ord} s = 2$, we have:

$$3|(i - i'), \quad 2|(j' - j),$$

by Theorem 2.2.

Hence,

$$\begin{aligned}
\phi(r^i s^j)\phi(r^{i'} s^{j'})^{-1} &= (a^i b^j)(a^{i'} b^{j'})^{-1} \\
&= a^i b^j b^{-j'} a^{-i'} \\
&= a^i b^{j-j'} a^{-i'} \\
&= a^{i-i'} && \text{since } \operatorname{ord} b = 2. \\
&= e && \text{since } \operatorname{ord} a = 3.
\end{aligned}$$

This implies that $\phi(r^i s^j) = \phi(r^{i'} s^{j'})$. We conclude that ϕ is well-defined.

We now show that ϕ is a group homomorphism:

Given $\mu, \mu' \in \{0,1,2\}$, $\nu, \nu' \in \{0,1\}$, we have:

$$\phi(r^\mu s^\nu \cdot r^{\mu'} s^{\nu'}) = \begin{cases} \phi(r^{\mu+\mu'} s^{\nu'}), & \text{if } \nu = 0; \\ \phi(r^{\mu-\mu'} s^{\nu+\nu'}), & \text{if } \nu = 1. \end{cases}$$

$$= \begin{cases} a^{\mu+\mu'} b^{\nu'}, & \text{if } \nu = 0; \\ a^{\mu-\mu'} b^{\nu+\nu'} = a^\mu b^\nu a^{\mu'} b^{\nu'}, & \text{if } \nu = 1. \end{cases}$$

$$= \phi(r^{\mu} s^{\nu})\phi(r^{\mu'} s^{\nu'}).$$

This shows that ϕ is a group homomorphism.

To show that ϕ is a group isomorphism, it remains to show that it is surjective and one-to-one.

It is clear that ϕ is surjective. We leave it as an exercise to show that ϕ is one-to-one. $\square$

Example 5.10. The group:

$$G = \left\{ g \in \mathrm{GL}(2, \mathbb{R}) \;\middle|\; g = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \text{ for some } \theta \in \mathbb{R} \right\}$$

is isomorphic to

$$G' = \{z \in \mathbb{C} : |z| = 1\}.$$

Here, the group operation on G is matrix multiplication, and the group operation on G' is the multiplication of complex numbers.

Each element in G' is equal to $e^{i\theta}$ for some $\theta \in \mathbb{R}$. Define a map $\phi : G \longrightarrow G'$ as follows:

$$\phi\left(\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}\right) = e^{i\theta}.$$

Exercise: Show that ϕ is a well-defined map. Then, show that it is a bijective group homomorphism.

5.1.1 WeBWorK

1. **WeBWorK**
2. **WeBWorK**
3. **WeBWorK**
4. **WeBWorK**
5. **WeBWorK**
6. **WeBWorK**

5.2 Rings

5.2.1 Basic Results in Elementary Number Theory

Theorem 5.11 (Division Theorem)**.** *Let $a, b \in \mathbb{Z}$, $a \neq 0$, then there exist unique q (called the quotient), and r (***remainder***) in $\mathbb{Z}$, satisfying $0 \leq r < |a|$, such that $b = aq + r$.*

Proof of Division Theorem. We will prove the case $a > 0$, $b \geq 0$. The other cases are left as exercises.

Fix $a > 0$. First, we prove the existence of the quotient q and remainder r for any $b \geq 0$, using mathematical induction.

The base step corresponds to the case $0 \leq b < a$. In this case, if we let $q = 0$ and $r = b$, then indeed $b = qa + r$, where $0 \leq r = b < a$. Hence, q and r exist.

The inductive step of the proof of the existence of q and r is as follows: Suppose the existence of the quotient and remainder holds for all non-negative $b' < b$, we want to show that it must also hold for b.

First, we may assume that $b \geq a$, since the case $b < a$ has already been proved. Let $b' = b - a$. Then, $0 \leq b' < b$, so by the inductive hypothesis we have $b' = q'a + r'$ for some $q', r' \in \mathbb{Z}$ such that $0 \leq r' < a$.

This implies that $b = b' + a = (q' + 1)a + r'$.

So, if we let $q = q' + 1$ and $r = r'$, then $b = qa + r$, where $0 \leq r < a$. This establishes the existence of q, r for b. Hence, by mathematical induction, the existence of q, r holds for all $b \geq 0$.

Now we prove the uniqueness of q and r. Suppose $b = qa + r = q'a + r'$, where $q, q', r, r' \in \mathbb{Z}$, with $0 \leq r, r' < a$.

Then, $qa + r = q'a + r'$ implies that $r - r' = (q' - q)a$. Since $0 \leq r, r' < a$, we have:

$$a > |r - r'| = |q' - q|\, a.$$

Since $q' - q$ is an integer, the above inequality implies that $q' - q = 0$, i.e. $q' = q$, which then also implies that $r' = r$. We have therefore established the uniqueness of q and r.

The proof of the theorem, for the case $a > 0, b \geq 0$, is now complete. □

Another Proof of the Theorem 5.11 (Division Theorem).

Proof of Division Theorem. We consider here the special case $b \geq 0$. Consider the set:

$$S = \{s \in \mathbb{Z}_{\geq 0} \ : \ s = b - aq \text{ for some } q \in \mathbb{Z}.\}$$

Since $b = b - a \cdot 0 \geq 0$, we have $b \in S$. So, S is a nonempty subset of $\mathbb{Z}$ bounded below by 0. By the Least Integer Axiom, there exists a minimum element $r \in S$. We claim that $r < |a|$:

Suppose not, that is, $r \geq |a|$. By assumption: $r = b - aq$ for some $q \in \mathbb{Z}$.

Consider the element $r' = r - |a|$. Then, $0 \leq r'$ and moreover:

$$r' = (b - aq) - |a| = b - (q \pm 1)a,$$

depending on whether $a > 0$ or $a < 0$. So, $r' \in S$. On the other hand, by construction we have $r' < r$, which contradicts the minimality of r. We conclude that $r < |a|$. This establishes the existence of the remainder r.

The existence of q in the theorem is now also clear. We leave the proof of the uniqueness of r and q as an exercise. □

Theorem 5.12. *Every subgroup of $\mathbb{Z}$ is cyclic.*

Proof of Theorem 3.7. First, we note that the group operation $*$ on $\mathbb{Z}$ is integer addition, with $e_{\mathbb{Z}} = 0$, and $z^{*-1} = -z$ for any $z \in \mathbb{Z}$.

Let H be a nontrivial (i.e. contains more than one element) subgroup of $\mathbb{Z}$. Since for any $h \in H$ we also have $-h \in H$, H contains at least one positive element.

Let d be the least positive integer in H. It exists because of the Least Integer Axiom.

We claim that $H = \langle d \rangle$:

For any $h \in H$, by the Division Theorem for Integers we have $h = dq + r$ for some $r, q \in \mathbb{Z}$, such that $0 \leq r < d$. Then,

$$r = h - dq = h - (\underbrace{d + d + \ldots + d}_{q \text{ times}})$$

if $q \geq 0$, or

$$r = h - dq = h - (\underbrace{(-d) + (-d) + \ldots + (-d)}_{q \text{ times}})$$

if $q < 0$.

In either case, since H is a subgroup we have $r \in H$. If $r > 0$, then we have a positive element in H which is strictly less than d, which contradicts the minimality of d. Hence, $r = 0$, from which it follows that any $h \in H$ is equal to $dq = d^{*q}$ for some $q \in \mathbb{Z}$. This shows that $H = \langle d \rangle$. □

Exercise 5.13. Let n be a positive integer. Every subgroup of $\mathbb{Z}_n$ is cyclic.

Corollary 5.14. *Every subgroup of a cyclic group is cyclic.*