Week 7

7.1 Classification of cyclic groups

Example 7.1.1. Let $H = \{r_0, r_1, r_2, \ldots, r_{n-1}\}$ be the subgroup of D_n consisting of all rotations, where r_1 denotes the anti-clockwise rotation by the angle $2\pi/n$, and $r_k = r_1^k$. Then, H is isomorphic to $\mathbb{Z}_n = (\mathbb{Z}_n, +_n)$.

Proof. Define $\phi : H \longrightarrow \mathbb{Z}_n$ as follows:

$$\phi(r_1^k) = \overline{k}, \quad k \in \mathbb{Z},$$

where $\overline{k}$ denotes the remainder of the division of k by n.

The map ϕ is well defined: If $r_1^k = r_1^{k'}$, then $r_1^{k-k'} = e$, which implies that $n = |r_1|$ divides $k - k'$. Hence, $\overline{k} = \overline{k'}$ in $\mathbb{Z}_n$.

For $i, j \in \mathbb{Z}$, we have $r_1^i r_1^j = r_1^{i+j}$; hence:

$$\phi(r_1^i r_1^j) = \phi(r_1^{i+j}) = \overline{i+j} = i +_n j = \phi(r_1^i) +_n \phi(r_1^j).$$

This shows that ϕ is a homomorphism. It is clear that ϕ is surjective, which then implies that ϕ is one-to-one, for the two groups have the same size. Hence, ϕ is a bijective homomorphism, i.e. an isomorphism. $\square$

In fact:

Theorem 7.1.2. *Any infinite cyclic group is isomorphic to* $(\mathbb{Z}, +)$. *Any cyclic group of finite order* n *is isomorphic to* $(\mathbb{Z}_n, +_n)$.

Proof. Write $G = \langle g \rangle$.

Suppose $|G| = \infty$. Consider the map

$$\phi : \mathbb{Z} \to G, \quad k \mapsto g^k.$$

ϕ is a homomorphism because $\phi(k_1 + k_2) = g^{k_1+k_2} = g^{k_1} \cdot g^{k_2} = \phi(k_1) \cdot \phi(k_2)$. ϕ is injective because $\phi(k_1) = \phi(k_2)$ implies that $g^{k_1} = g^{k_2}$ which forces $k_1 = k_2$

as $|g| = \infty$. ϕ is surjective because G is generated by g. We conclude that ϕ is an isomorphism.

If $|G| = n < \infty$, Claim 2.1.2 says that we can write

$$G = \langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}.$$

Consider the bijection

$$\phi : G \to \mathbb{Z}_n, \quad g^i \mapsto i.$$

We have

$$\begin{aligned}\phi(g^{i_1} \cdot g^{i_2}) &= \phi(g^{i_1+i_2}) \\ &= \begin{cases} \phi(g^{i_1+i_2}) & \text{if } i_1 + i_2 < n, \\ \phi(g^{i_1+i_2-n}) & \text{if } i_1 + i_2 \geq n \end{cases} \\ &= \begin{cases} i_1 + i_2 & \text{if } i_1 + i_2 < n, \\ i_1 + i_2 - n & \text{if } i_1 + i_2 \geq n \end{cases} \\ &= \phi(g^{i_1}) + \phi(g^{i_2}),\end{aligned}$$

so ϕ is an isomorphism. □

So for any $n \in \mathbb{Z} \cup \{\infty\}$, there is a unique (up to isomorphism) cyclic group of order n. In particular, we have the following:

Corollary 7.1.3. *If G and G' are two finite cyclic groups of the same order, then G is isomorphic to G'.*

For example, the multiplicative group of m-th roots of unity

$$U_m = \{z \in \mathbb{C} : z^m = 1\} = \{1, \zeta_m, \zeta_m^2, \ldots, \zeta_m^{m-1}\},$$

where $\zeta_m = e^{2\pi \mathbf{i}/m} = \cos(2\pi/m) + \mathbf{i}\sin(2\pi/m) \in \mathbb{C}$, is cyclic of order m. So it is isomorphic to $\mathbb{Z}_m$, and an isomorphism is given by

$$\phi : \mathbb{Z}_m \longrightarrow U_m, \quad k \mapsto \zeta_m^k.$$

7.2 Rings

Definition. A **ring** R (or $(R, +, \cdot)$) is a set equipped with two binary operations:

$$+, \cdot : R \times R \to R$$

which satisfy the following properties:

1. $(R, +)$ is an abelian group.
2. (a) The multiplication $\cdot$ is associative, i.e.

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

   for all $a, b, c \in R$.

   (b) There is an element $1 \in R$ (called the *multiplicative identity*) such that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$.

3. (Distributive laws:)

   (a) $a \cdot (b + c) = a \cdot b + a \cdot c$ and

   (b) $(a + b) \cdot c = a \cdot c + b \cdot c$

   for all $a, b, c \in R$.

Example 7.2.1. The following sets, equipped with the usual operations of addition and multiplication, are rings:

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.
2. $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$ (Polynomials with integer, rational, real, complex coefficients, respectively.)
3. $\mathbb{Q}[\sqrt{2}] = \{\sum_{k=0}^{n} a_k(\sqrt{2})^k : a_k \in \mathbb{Q}, n \in \mathbb{N}\} = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.
4. For a fixed n, the set of $n \times n$ matrices with integer coefficients.
5. $C[a, b] = \{f : [a, b] \to \mathbb{R} : f$ is continuous.$\}$
6. $(\mathbb{N}, +, \cdot)$ is *not* a ring because $(\mathbb{N}, +)$ is not a group.

Remark.

- For convenience's sake, we often write ab for $a \cdot b$.
- In the definition, commutativity is required of addition, but not of multiplication.
- Every element has an additive inverse, but *not necessarily* a multiplicative inverse. That is, there may be an element $a \in R$ such that $ab \neq 1$ for all $b \in R$.

Proposition 7.2.2. *In a ring R, there is a unique additive identity and a unique multiplicative identity.*

Proof. We already know that the additive identity is unique.

Suppose there is an element $1' \in R$ such that $1'r = r$ or all $r \in R$, then in particular $1'1 = 1$. But $1'1 = 1'$ since 1 is a multiplicative identity element, so $1' = 1$. □

Proposition 7.2.3. *For any r in a ring R, its additive inverse $-r$ is unique. That is, if $r + r' = r + r'' = 0$, then $r' = r''$.*

If r has a multiplicative inverse, then it is also unique. That is, if $rr' = 1 = r'r$ and $rr'' = 1 = r''r$, then $r' = r''$.

Proposition 7.2.4. *For all elements r in a ring R, we have $0r = r0 = 0$.*

Proof. By distributive laws,

$$0r = (0 + 0)r = 0r + 0r$$

Adding $-0r$ (additive inverse of $0r$) to both sides, we have:

$$0 = (0r + 0r) + (-0r) = 0r + (0r + (-0r)) = 0r + 0 = 0r.$$

The proof of $r0 = 0$ is similar and we leave it as an exercise. □

Proposition 7.2.5. *For all elements r in a ring, we have $(-1)(-r) = (-r)(-1) = r$.*

Proof. We have:

$$0 = 0(-r) = (1 + (-1))(-r) = -r + (-1)(-r).$$

Adding r to both sides, we obtain

$$r = r + (-r + (-1)(-r)) = (r + -r) + (-1)(-r) = (-1)(-r).$$

We leave it as an exercise to show that $(-r)(-1) = r$. □

Proposition 7.2.6. *For all r in a ring R, we have: $(-1)r = r(-1) = -r$*

Proof. **Exercise** □

Proposition 7.2.7. *If R is a ring in which $1 = 0$, then $R = \{0\}$. That is, it has only one element.*

We call such an R the **zero ring**.

Proof. **Exercise.** □

Definition. A ring R is said to be **commutative** if $ab = ba$ for all $ab \in R$.

Example 7.2.8.

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are all commutative rings, so are $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$.
- For a fixed natural number $n > 1$, the ring of $n \times n$ matrices with integer coefficients, under the usual operations of addition and multiplication, is not commutative.

Modulo m arithmetic

Example 7.2.9. Let m be a positive integer. Consider the set

$$\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}.$$

For any integer $n \in \mathbb{Z}$, we denote by $\overline{n}$ the remainder of the division of of n by m: $n = mq + r$.

On the other hand, two integers $a, b \in \mathbb{Z}$ are said to be **congruent modulo** m, denoted as $a \equiv b \mod m$, if $m \mid (a - b)$. This defines an equivalence relation on $\mathbb{Z}$, and $\mathbb{Z}_m$ can be regarded as parametrizing the equivalence classes, namely, every $a \in \mathbb{Z}$ is congruent modulo m to exactly one element in $\mathbb{Z}_m$.

Remark. Congruence modulo m is exactly the same as the relation defined by the subgroup $m\mathbb{Z} < \mathbb{Z}$, so the above partition is the same as that given by cosets of $m\mathbb{Z}$ in $\mathbb{Z}$.

We equip $\mathbb{Z}_m$ with addition $+_m$ and multiplication $\cdot_m$ defined as follows: For $a, b \in \mathbb{Z}_m$, let:

$$a +_m b = \overline{a + b},$$
$$a \cdot_m b = \overline{a \cdot b},$$

where the addition and multiplication on the right are the usual addition and multiplication for integers.

Proposition 7.2.10. *With addition and multiplication thus defined, $\mathbb{Z}_m$ is a commutative ring.*

Proof.

1. We already know that $(\mathbb{Z}_m, +_m)$ is an abelian group.

2. Note that If $a \equiv a' \mod m$ and $b \equiv b' \mod m$, then $ab \equiv a'b' \mod m$. So for $r_1, r_2 \in \mathbb{Z}_m$, we have

$$\overline{r_1 r_2} \equiv r_1 r_2 \equiv \overline{r_1} \cdot \overline{r_2} \equiv \overline{\overline{r_1} \cdot \overline{r_2}} \mod m.$$

For $a, b, c \in \mathbb{Z}_m$, we have:

$$a \cdot_m (b \cdot_m c) = a \cdot_m \overline{bc} = \overline{\overline{a} \cdot \overline{bc}} = \overline{a(bc)},$$

which by the associativity of multiplication for integers is equal to:

$$\overline{(ab)c} = \overline{\overline{ab} \cdot \overline{c}} = \overline{ab} \cdot_m c = (a \cdot_m b) \cdot_m c.$$

So, $\cdot_m$ is associative.

3. **Exercise:** We can take 1 to be the multiplicative identity.

4. For $a, b \in \mathbb{Z}_m$, $a \cdot_m b = \overline{a \cdot b} = \overline{b \cdot a} = b \cdot_m a$. So $\cdot_m$ is commutative.

5. Lastly, we need to prove distributivity. For $a, b, c \in \mathbb{Z}_m$, we have:

   $$a \cdot_m (b +_m c) = \overline{\overline{a} \cdot \overline{b + c}} = \overline{a \cdot (b + c)} = \overline{ab + ac} = \overline{\overline{ab} + \overline{ac}} = a \cdot_m b +_m a \cdot_m c.$$

   It now follows from the distributivity from the left, proven above, and the commutativity for $\cdot_m$, that distributivity from the right also holds:

   $$(a +_m b) \cdot_m c = a \cdot_m c + b \cdot_m c.$$

□