Chapter 1. GROUP FAMILIES

§1T. Cyclic groups $\mathbb{Z}_n$ and $\mathbb{Z}$

(1.1.1) Definition.

- A **cyclic group** is a group G that contains an element $g \in G$ such that the group generated by g is G, $\langle g \rangle = G$.

The following facts follow from the definition.

1) If G is cyclic with generator g then all elements of G are of the form

$$g^k = \underbrace{g \cdot g \cdots g}_{k \text{ times}} \qquad \text{or} \qquad g^{-k} = \underbrace{g^{-1} g^{-1} \cdots g^{-1}}_{k \text{ times}}$$

for some nonnegative integer k.

2) If G is cyclic with generator g and G is finite and $| G | = n$ then

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

3) If G is cyclic then G is abelian since $g^i g^j = g^{i+j} = g^j g^i$ for all $i, j \in \mathbb{Z}$.

4) If G is cyclic then all subgroups of G are normal since G is abelian.

HW: Let G be a group of order p, where p is a prime. Show that G is cyclic.

The integers, $\mathbb{Z}$

(1.1.2) Definition.

- The group of **integers** $\mathbb{Z}$ is the set $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ with the operation of addition.

HW: Show that $\mathbb{Z}$ is an abelian group.

HW: Show that both the element $1 \in \mathbb{Z}$ and the element $-1 \in \mathbb{Z}$ generate $\mathbb{Z}$.

HW: Show that $\mathbb{Z}$ is a cyclic group.

HW: Show that every element of $\mathbb{Z}$ is in a conjugacy class by itself.

(1.1.3) Theorem.

a) Let H be a subset of the integers $\mathbb{Z}$. Then H is a subgroup of $\mathbb{Z}$ if and only if $H = m\mathbb{Z}$ for some nonnegative integer m.

b) Let m and n be positive integers. Then $m\mathbb{Z} \subseteq n\mathbb{Z}$ if and only if n divides m.

c) Let n be a positive integer. Then the quotient group $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$.

HW: Show that every subgroup of $\mathbb{Z}$ is normal subgroup of $\mathbb{Z}$.

Example. The subgroup $5\mathbb{Z}$ of the integers $\mathbb{Z}$ consists of all multiples of 5.

$$5\mathbb{Z} = \{\ldots, -10, -5, 0, 5, 10, \ldots\}.$$

The subgroup $15\mathbb{Z}$ is contained in the subgroup $5\mathbb{Z}$.

$$5\mathbb{Z} = \{\ldots, -10, -5, 0, 5, 10, 15, \ldots\} \quad \supseteq \quad 15\mathbb{Z} = \{\ldots, -30, -15, 0, 15, 30, \ldots\}.$$

The sets

$$0+5\mathbb{Z} = 5+5\mathbb{Z} = 10+5\mathbb{Z} = \{\ldots,-10,-5,0,5,10,\ldots\} = 5\mathbb{Z},$$
$$1+5\mathbb{Z} = -4+5\mathbb{Z} = -9+5\mathbb{Z} = \{\ldots,-9,-4,1,6,11,16,\ldots\},$$
$$2+5\mathbb{Z} = 32+5\mathbb{Z} = -23+5\mathbb{Z} = \{\ldots,-13,-8,-3,2,7,12,17,22,27,32,\ldots\},$$
$$3+5\mathbb{Z} = -7+5\mathbb{Z} = 8+5\mathbb{Z} = \{\ldots,-7,-2,3,8,13,\ldots\},$$
$$4+5\mathbb{Z} = 404+5\mathbb{Z} = -236+5\mathbb{Z} = \{\ldots,-6,-1,4,9,14,\ldots\}.$$

are all cosets of the subgroup $5\mathbb{Z}$ in the group $\mathbb{Z}$. In fact

$$\mathbb{Z}/5\mathbb{Z} = \{0+5\mathbb{Z}, 1+5\mathbb{Z}, 2+5\mathbb{Z}, 3+5\mathbb{Z}, 4+5\mathbb{Z}\}$$

is the set of cosets of $5\mathbb{Z}$ in $\mathbb{Z}$. As a group $\mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}_5$.

(1.1.4) Proposition. *Every homomorphism from $\mathbb{Z}$ to $\mathbb{Z}$ is of the form*

$$\begin{array}{rccc} \varphi_m\colon & \mathbb{Z} & \to & \mathbb{Z} \\ & n & \mapsto & mn, \end{array}$$

for some positive integer m.

HW: Show that $\ker\varphi_m = \mathbb{Z}$ if $m = 0$.
HW: Show that φ_m is injective if $m \neq 0$.
HW: Show that φ_m is bijective if and only if $m = 1$ or $m = -1$.
HW: Show that φ_1 is the identity mapping.
HW: Show that the automorphism group of $\mathbb{Z}$, $\mathrm{Aut}(\mathbb{Z}) = \{\varphi_1, \varphi_{-1}\} \simeq \mathbb{Z}_2$.
HW: Show that inner automorphisms of $\mathbb{Z}$ are $\mathrm{In}(\mathbb{Z}) = \{\varphi_1\}$.

(1.1.5) Proposition. *The group of integers $\mathbb{Z}$ is isomorphic to the free group on one generator.*

The finite cyclic groups $\mathbb{Z}_n$, $n \geq 1$.

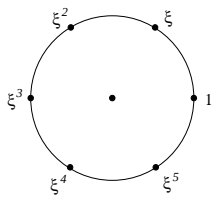
(1.1.6) Definition.

- The **cyclic group of order** n, $\mathbb{Z}_n$, is the set $\mathbb{Z}_n = \{1, g, g^2, \ldots, g^{n-1}\}$ with the operation given by

$$g^i g^j = g^{(i+j) \bmod n}.$$

There are other representations of the group $\mathbb{Z}_n$ which are useful.

1) Let Z_n be the group given by $Z_n = \{1, \xi, \xi^2, \ldots, \xi^{n-1}\}$, where $\xi = e^{\frac{2\pi i}{n}} \in \mathbb{C}$, with the operation of multiplication of complex numbers. In the complex plane the elements of Z_n all lie on the circle $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$.



2) Let $\mathbb{Z}_n$ be the group given by $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ with operation given by $\bar{i} + \bar{j} = \overline{(i+j) \bmod n}$. This operation is called **addition modulo** n.

HW: Show that the group homomorphism $\phi: \mathbb{Z}_n \to Z_n$ given by $\phi(g^i) = \xi^i$ is an isomorphism.

HW: Show that the group homomorphism $\varphi: \mathbb{Z}_n \to \mathbb{Z}_n$ given by $\varphi(g^i) = \bar{i}$ is an isomorphism.

(1.1.7) Theorem.

a) The subgroups of the cyclic group $\mathbb{Z}_n$ are the subgroups generated by the elements g^m, $\langle g^m \rangle$, $0 \leq m \leq n-1$.

b) Let $0 \leq m \leq n-1$ and let $d = \gcd(m,n)$. Then $\langle g^m \rangle = \langle g^d \rangle$ where $d = \gcd(m,n)$ and $|\langle g^d \rangle| = n/d$.

c) Let $0 \leq m, k \leq n-1$. Then $\langle g^m \rangle \subseteq \langle g^k \rangle$ if and only if $\gcd(k,n)$ divides $\gcd(m,n)$.

d) Let $0 \leq d \leq n$ and suppose that d divides n. Then the quotient group

$$\mathbb{Z}_n / \langle g^d \rangle \simeq \mathbb{Z}_{n/d}.$$

Example. The subgroup lattice of the group $\mathbb{Z}_{12}$ is given by:

Orders	**Inclusions**
12	$\mathbb{Z}_{12} = \langle g \rangle$
6	$\langle g^2 \rangle = \{1, g^2, g^4, g^6, g^8, g^{10}\}$
4	$\langle g^3 \rangle = \{1, g^3, g^6, g^9\}$
3	$\langle g^4 \rangle = \{1, g^4, g^8\}$
2	$\langle g^6 \rangle = \{1, g^6\}$
1	(1)

The set of cosets $\mathbb{Z}_{12}/\langle g^3 \rangle = \{H, gH, g^2H\}$ where

$$H = \{1, g^3, g^6, g^9\}, \qquad gH = \{g, g^4, g^7, g^{10}\}, \qquad \text{and} \qquad g^2H = \{g^2, g^5, g^8, g^{11}\}.$$

(1.1.8) Proposition. *Let $\mathbb{C}^\times = \mathbb{C} - \{0\}$ with the operation of multiplication of complex numbers and let n be a positive integer. Every homomorphism from $\mathbb{Z}_n$ to $\mathbb{C}^\times$ is of the form*

$$\varphi_k: \begin{array}{ccc} \mathbb{Z}_n & \to & \mathbb{C}^\times \\ g & \mapsto & \xi^k \end{array}, \qquad \text{where} \qquad \xi = e^{\frac{2\pi i}{n}}.$$

(1.1.9) Proposition.

a) The cyclic group $\mathbb{Z}_n = \{1, g, g^2, \ldots, g^{n-1}\}$ *of order* n *is generated by the element* g *and* g *satisfies the relation*

$$g^n = 1.$$

b) The cyclic group $\mathbb{Z}_n$ *has a presentation by generators and relations of the form*

$$\mathbb{Z}_n = \langle x \mid x^n = 1 \rangle.$$

(1.1.10) Proposition. *Let* S *be a circular necklace with* n *equally spaced beads* $b_0, b_1, \ldots, b_{n-1}$*, numbered counterclockwise around* S*.*

a) There is an action of the cyclic group $\mathbb{Z}_n$ *on the necklace* S *such that* g *acts by rotating* S *counterclockwise by an angle of* $2\pi/n$*.*

b) This action has one orbit, $\mathbb{Z}_n b_0 = \{b_0, b_1, \ldots, b_{n-1}\}$ *and the stabilizer of each bead is the subgroup* (1)*.*