Plan

- Review of Last Lecture
- Section 14. Factor Groups (continued)

Theorem

*(**Theorem 14.4 + Corollary 14.5**) Let G be a group, H be a normal subgroup of G, G/H be the set of all left cosets of H, then*
(1) the binary operation on G/H given by

$$(aH)(bH) = (ab)H$$

is well-defined.
(2). G/H is a group under the above binary operation.

The symbol G/H denotes the set of all left cosets of H.

Example. $G = \mathbb{Z},\ H = 6\mathbb{Z}$,

$$\mathbb{Z}/6\mathbb{Z} = \{0 + 6\mathbb{Z},\ 1 + 6\mathbb{Z},\ 2 + 6\mathbb{Z},\ 3 + 6\mathbb{Z},\ 4 + 6\mathbb{Z},\ 5 + 6\mathbb{Z}.\ \}$$

$$(4 + 6\mathbb{Z}) + (5 + 6\mathbb{Z}) = (4 + 5) + 6\mathbb{Z} = 9 + 6\mathbb{Z} = 3 + 6\mathbb{Z}$$

We can write

$$\mathbb{Z}/6\mathbb{Z} = \{0, 1, 2, 3, 4, 5\}$$

$\mathbb{Z}/6\mathbb{Z} = \mathbb{Z}_6$.

The group G/H in the Theorem 14.4 is called the **factor group** (or **quotient group**) of G by H.

For every positive integer n, the factor group $\mathbb{Z}/n\mathbb{Z}$ of $\mathbb{Z}$ by $n\mathbb{Z}$ is just $\mathbb{Z}_n$.

Theorem

*(**Theorem 14.9**) Let H be a normal subgroup of G. Then $\gamma : G \to G/H$*

$$\gamma(a) = aH$$

is a homomorphism with kernel H.

Theorem

(**Theorem 14.11. The Fundamental Homomorphism Theorem.** *Let* $\phi : G \to G'$ *be a group homomorphism with kernel* $Ker(\phi) = H$. *Then*
(1) $\phi(G)$ *is a subgroup of* G'.
(2) The map $\mu : G/H \to \phi(G)$ *given by*

$$\mu(gH) = \phi(g)$$

is well-defined and is an isomorphism.
(3) If $\gamma : G \to G/H$ *is the homomorphism given by* $\gamma(g) = gH$, *then* $\phi(g) = (\mu\gamma)(g)$ *for each* $g \in G$.

Proof. (1) follows Part (3) of Theorem 13.12
(2). To prove μ is well-defined. Let $g_1H = g_2H$, we want to prove $\phi(g_1) = \phi(g_2)$. The condition $g_1H = g_2H$ implies that $g_1 = g_2h$ for some $h \in H$, so

$$\phi(g_1) = \phi(g_2h) = \phi(g_2)\phi(h) = \phi(g_2)e = \phi(g_2)$$

This proves μ is well-defined. It is easy to prove μ is a homomorphism and is onto. It remains to prove μ is one-to-one.

$$\begin{aligned} Ker(\mu) &= \{gH \in G/H \,|\, \mu(gH) = e'\} \\ &= \{gH \in G/H \,|\, \phi(g) = e'\} \\ &= \{gH \in G/H \,|\, g \in H\} \\ &= \{eH\} \end{aligned}$$

is trivial. So Theorem 13.15, μ is one-to-one.
(3) is easy.

Example. Prove that $\mathbb{C}^*/U_n$ is isomorphic to $\mathbb{C}^*$.

Proof. Let $\phi : \mathbb{C}^* \to \mathbb{C}^*$ be given by $\phi(a) = a^n$. Then ϕ is a homomorphism, because

$$\phi(ab) = (ab)^n = a^n b^n = \phi(a)\phi(b).$$

ϕ is onto. So

$$\phi(\mathbb{C}^*) = \mathbb{C}^*$$

$$Ker(\phi) = \{a \in \mathbb{C}^* \mid \phi(a) = 1\} = \{a \in \mathbb{C}^* \mid a^n = 1\} = U_n.$$

By Theorem 14.11, $\mathbb{C}^*/U_n$ is isomorphic to $\mathbb{C}^*$.

Example. Prove that the factor group $\mathbb{C}^*/U$ is isomorphic to $\mathbb{R}_{>0}$.

Sketch of Proof. Consider the homomorphism $\phi : \mathbb{C}^* \to \mathbb{R}_{>0}$ given by

$$\phi(z) = |z|$$

Then apply Theorem 14.11.

Theorem

*(**Theorem 14.13**) Let G be a group and $H \subseteq G$ is a subgroup. Then the following two conditions are equivalent.*
(1) $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$.
(2) H is a normal subgroup.

This theorem was proved when we discussed Section 13.

Definition 14.15. An isomorphism $\phi : G \to G$ is called an **automorphism** of G.

Given $g \in G$, $i_g : G \to G$ given by

$$i_g(x) = gxg^{-1}$$

is an automorphism.

i_g is called the **inner automorphism of** G by g.

Example. Find all the homomorphisms $\phi : \mathbb{Z} \to \mathbb{Z}$ and find all the automorphisms from $\mathbb{Z}$.

Suppose $\phi : \mathbb{Z} \to \mathbb{Z}$ is a homomorphism, we know $\phi(0) = 0$ (Theorem 13.12 (1)). For a positive integer n,

$$\begin{aligned}\phi(n) \quad &= \phi(1 + \cdots + 1) \;\; (n \text{ copies } 1)\\ &= \phi(1) + \cdots + \phi(1) \;\; (n \text{ copies } \phi(1)) = n\phi(1)\end{aligned}$$

$$\phi(-n) = -\phi(n) = -n\phi(1)$$

We proved

$$\phi(m) = \phi(1)m$$

for arbitrary $m \in \mathbb{Z}$. $\phi(1)$ can be every integer. (continued next page)

For every integer a, we define a map $T_a : \mathbb{Z} \to \mathbb{Z}$ by

$$T_a(m) = am$$

It is easy to prove T_a is a homomorphism. Every homomorphism from $\mathbb{Z}$ to $\mathbb{Z}$ itself is T_a for some $a \in \mathbb{Z}$.

Among all the homomorphisms T_a, T_1, T_{-1} are the only automorphism of $\mathbb{Z}$.

$$T_1(a) = a, \qquad T_{-1}(a) = -a$$

The concept of factor group has a linear algebra analog called factor vector space or quotient vector space.

We take the this opportunity to recall the definition.

We first recall the definition of a vector space over the real number.

Definition of Vector Space. A vector space over real number is a set V with a binary operation $+$ (called the vector addition) and a scalar multiplication that send $k \in \mathbb{R}$ and $v \in V$ to $kv \in V$ such that the following axioms hold

(1) $+$ is commutative and associative.
(2) there is a zero vector $0 \in V$ satisfying $v + 0 = 0 + v = v$ for all $v \in V$.
(3) For every $v \in V$, there exists $-v \in V$ satisfying $v + (-v) = 0$.
(4) $1v = v$
(5) For $k_1, k_2 \in \mathbb{R}$, $v \in V$,

$$(k_1 k_2)v = k_1(k_2 v)$$

(6) For $k_1, k_2 \in \mathbb{R}$, $v \in V$,

$$(k_1 + k_2)v = k_1 v + k_2 v$$

(7) For $k \in \mathbb{R}$, $v_1, v_2 \in V$,

$$k(v_1 + v_2) = kv_1 + kv_2$$

The conditions (1) (2) (3) can be combined to one condition: V is an abelian group under $+$.

A subset S of a vector space V is called a **subspace** if S is non-empty and is closed under $+$ and scalar multiplication.

Every vector space V is an abelian group under $+$. Every subspace S is a subgroup. Since $(V, +)$ is an abelian subgroup, so S is a normal subgroup of V. We have factor group

$$(V/S, +)$$

An element in V/S is a coset $a + S$.

The scalar multiplication on V/S is defined as

$$k(a+S) = ka + S$$

One checks that V/S is a vector space, called the factor space of V by S (or quotient space of V by S).

One can prove if V is finite dimensional, then

$$\dim(V/S) = \dim(V) - \dim(S).$$

The end