Plan

- Section 10. Cosets and the Theorem of Lagrange (Review)
- Section 11. Direct Products and Finitely Generated Abelian Groups (Review and Continue)
- Section 13. Homomorphisms

Theorem

(Theorem 10.10. Lagrange Theorem) If H is a subgroup of a finite group G, then $|H|$ is a divisor of $|G|$.

$\frac{|G|}{|H|}$ is equal to the number of left cosets of H.

Corollary 10.11. *Every group of prime order is a cyclic.*

Theorem

(**Theorem 10.12**) *The order of an element of a finite group is a divisor of the order of the group.*

Section 11. Direct Products and Finitely Generated Abelian Groups.

Theorem

*(**Theorem 11.2**) Let $G_1, G_2, \ldots, G_n$ be groups, we define a binary operation on $G_1 \times G_2 \times \cdots \times G_n$ by*

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

*Then $G_1 \times G_2 \times \cdots \times G_n$ is a group under this operation. This group is called the **direct product of the groups** G_i.*

Example. $\mathbb{Z}_2 = \{0, 1\}$
The direct product group $\mathbb{Z}_2 \times \mathbb{Z}_2$ has 4 elements. Every non-identity element in $\mathbb{Z}_2 \times \mathbb{Z}_2$ has order 2.

Similarly in $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ (n copies), there are 2^n elements, all of them except e have order 2.

Exercise. If G is a group such that $a^2 = e$ for all $a \in G$, prove that G is abelian.

Proof. We want to prove $ab = ba$ for all $a, b \in G$. Since $(ab)^2 = e$, we have $abab = e$. So we have

$$a(abab)b = aeb, \ a^2(ba)b^2 = ab,$$

Using $a^2 = b^2 = e$, we get $ba = ab$.

Definition. Let G be a group, S be a subset of G, we say S **generates** G if every element $g \in G$ can be written as

$$g = a_1^{k_1} a_2^{k_2} \cdots a_m^{k_m}$$

for some m and $a_1, \ldots, a_m \in S$ (not necessarily distinct) and $k_1, \ldots, k_m \in \mathbb{Z}$.

Example. $\mathbb{Z} \times \mathbb{Z}$. $S = \{(1,0),(0,1)\}$, then S generates $\mathbb{Z} \times \mathbb{Z}$.

Definition. A group G is called a **finitely generated group** if there exists a finite subset S that generates G.

Example. Every cyclic group is finitely generated, because a cyclic group can be generated by one element.

Example. $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$, $\ldots$, $\mathbb{Z}^n$ (the direct product of n copies of $\mathbb{Z}$) are all finitely generated groups.

Example. If $C_1, \ldots, C_n$ are cyclic groups, then the direct product group

$$C_1 \times C_2 \times \cdots \times C_n$$

is a finitely generated group. And it is abelian.

Theorem

(Theorem 11.12. Fundamental Theorem of Finitely Generated Abelian Groups) Every finitely generated abelian group G is isomorphic to a direct product of cyclic groups in the form

$$\mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \cdots \times \mathbb{Z}_{p_n^{r_n}} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$

where $p_1, p_2, \ldots, p_n$ are primes, not necessarily distinct, and r_i are positive integers.

The group G is finite iff there is no $\mathbb{Z}$ in the decomposition.

Definition 13.1. A map $\phi : G \to G'$ from a group G to a group G' is a **homomorphism** if it satisfies the property

$$\phi(ab) = \phi(a)\phi(b)$$

for all $a, b \in G$.

The concept of homomorphism is used to compare different groups.

If group G has operation $*$ and group G' has operation $\star$, the condition for $\phi : G \to G'$ being a homomorphism is

$$\phi(a * b) = \phi(a) \star \phi(b)$$

for all $a, b \in G$.

Example. $\phi : \mathbb{C}^* \to \mathbb{C}^*$ given by

$$\phi(z) = z^3$$

is a homomorphism

Example. $\phi : \mathbb{C}^* \to \mathbb{R}^*$ given by, for $z = x + iy \in \mathbb{C}^*$,

$$\phi(z) = \phi(x + iy) = |z| = \sqrt{x^2 + y^2}$$

is a homomorphism.

Example. $\phi : \mathbb{R}^* \to \mathbb{R}^*$ given by

$$\phi(x) = |x|$$

is a homomorphism.

Example. $\det : GL(n, \mathbb{R}) \to \mathbb{R}^*$, the determinant map, is a homomorphism because of the following property of the determinant:

$$\det(AB) = \det(A)\det(B)$$

Example. $f : \mathbb{R} \to \mathbb{R}$ given by

$$f(x) = 2020x$$

is a homomorphism.

Example. $f : \mathbb{Z} \to \mathbb{Z}_{10}$ given by

$$f(n) = n \bmod 10$$

is a homomorphism.

Example. Every vector space V is a group under the vector addition $+$. If W, V are vector spaces,then every linear map $T : W \to V$ is a group homomorphism.

Example. Let $C[0,2]$ be the space of continuous function on the interval $[0,2]$, then the integration map $\sigma : C[0,2] \to \mathbb{R}$

$$\sigma(f) = \int_0^2 f(x)dx$$

is a linear map, so it is a homomorphism.

Example. The map

$$f : \mathbb{R} \to \mathbb{R}^*, \quad f(x) = e^x$$

is a homomorphism because

$$e^{x+y} = e^x e^y$$

The end