Abstract Algebra
: Lecture 5

Leo

2024.09.26

Let A, B two groups, then we can get a bigger group by Direct Product, i.e. $A \times B$.

Example 1. *$G = (\mathbb{Z}_{15}, +)$, $|G| = 15$, $G =< 1 >$, cyclic group. $A \leqslant G$ s.t $A =< 3 >$, and $B \leqslant G$ s.t $B =< 5 >$. Claim: $G = A \times B$?*

Theorem 2. *Let $H, K \lhd G$ s.t. $G = HK$, then the folowing statements are equivalent:*

(1). $\phi : H \times K \to G$ s.t. $(h, k) \mapsto hk$ is an isomorphism.

(2). $H \cap K = \{e\}$, where e is the identity.

证明. (1) $\to$ (2): Assume ϕ is an isomorphism. Suppose $x \in H \cap K$ s.t. $x \neq e$. Then $\phi : (x, e) \to xe = e$ and $(e, x) \to ex = x$, which is impossible since ϕ is an bijection. Thus $H \cap K = \{e\}$.

(2) $\to$ (1): Assume $H \cap K = \{e\}$. Define $\phi : H \times K \to G$ s.t. $(h, k) \mapsto hk$. We need to show that ϕ is a homomorphism, injective and surjective. Claim: $hk = kh$ for all $h \in H$ and $k \in K$. Consider $[h, k] = hkh^{-1}k^{-1} = k_1k^{-1} \in K$, and $[k, h] = khk^{-1}h^{-1} = h_1h^{-1} \in H$. Since $H \cap K = \{e\}$, we have $k_1k^{-1} = h_1h^{-1} = e$. Thus $hk = kh$.

Homomorphism: $\phi((h_1, k_1)(h_2, k_2)) = \phi(h_1h_2, k_1k_2) = h_1h_2k_1k_2 = h_1k_1h_2k_2 = \phi(h_1, k_1)\phi(h_2, k_2)$.

Injective: Suppose $\phi(h_1, k_1) = \phi(h_2, k_2)$. Then $h_1k_1 = h_2k_2$. Since $H \cap K = \{e\}$, $h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K$, we have $h_1 = h_2$ and $k_1 = k_2$. Thus ϕ is injective.

Surjective: For any $g \in G$, since $G = HK$, there exist $h \in H$ and $k \in K$ s.t. $g = hk$. Thus $\phi(h, k) = hk = g$. Thus ϕ is surjective. $\square$

In a word, $H \times K \simeq HK$, HK is called a inner product of H and K. i.e. $G = H \times K = HK$.

Example 3. *$G = H \times H$ where $H = \mathbb{Z}_3$, $G \neq HH$ since $HH = H$.*

Example 4. *Let $G = \{\begin{bmatrix} a & 0 & 0 \\ 0 & b_1 & b_2 \\ 0 & b_3 & b_4 \end{bmatrix} | a \in \mathbb{F}_p - \{0\}, b_1b_4 \neq b_2b_3\}$. Then G is a group with matrix multiplication where $G < \mathrm{GL}_3(\mathbb{F}_p)$. Claim: $G \simeq \mathbb{Z}_{p-1} \times \mathrm{GL}_2\,\mathbb{F}_p$.*

Let $A = \{\begin{bmatrix} a & 0 \\ 0 & I_2 \end{bmatrix} | a \in \mathbb{F}_p - \{0\}\}$ and $B = \{\begin{bmatrix} 1 & 0 & 0 \\ 0 & b_1 & b_2 \\ 0 & b_3 & b_4 \end{bmatrix} | b_1b_4 \neq b_2b_3\}$, then $G = A \times B$.

Definition 5. *A subgroup H of G is called a maximal subgroup if H is not contained in any other proper subgroup of G. i.e. If $H \leqslant K \leqslant G$, then $K = G$ or $K = H$.*

Definition 6. *Subgroups of $\mathrm{Sym}(\Omega)$ are called permutation groups. Let $G \leqslant \mathrm{Sym}(\Omega)$. Then G is transitive on Ω if for all $\alpha, \beta \in \Omega$ there exists $\gamma \in G$ such that $\alpha^\gamma = \beta$. Otherwise G is intransitive.*

Homework 7. *(1). Let $G = S_n$. Describe maximal intransitive subgroups of G.*

(2). Let $G = \mathrm{GL}_n(\mathbb{F}_p)$. Describe maximal subgroups of G which fixes a 1 dimensional subspace of $\mathbb{F}_p^n$.

Let G be a cyclic group of order n. Then G is generated by a single element g. i.e. $G =< g >= \mathbb{Z}_n$.
(1). If $n = lm$ s.t. $\gcd(l, m) = 1$, then $\mathbb{Z}_n = \mathbb{Z}_l \times \mathbb{Z}_m$.
(2). If $n = p_1^{e_1} \dots p_r^{e_r}$, then $\mathbb{Z}_n = \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_r^{e_r}}$.

Theorem 8. *Let G be a group of order p^2, where p is a prime number. Then either $G \simeq \mathbb{Z}_{p^2}$ or $G \simeq \mathbb{Z}_p \times \mathbb{Z}_p$. In particuar G is abelian.*

证明. Let G be a group of order p^2. $e \neq g \in G$ has order p or p^2. If g has order p^2, then $G =< g >$. Suppose G does not have elements of order p^2. Let $a \in G - e$. Then $< a >\simeq \mathbb{Z}_p$. Let $b \in G- < a >$. Then $< b >\simeq \mathbb{Z}_p$. Furthermore $< a > \cap < b >= \{e\}$. Then $G \simeq< a > \times < b >\simeq \mathbb{Z}_p \times \mathbb{Z}_p$. □

Homework 9. *Prove $G \simeq< a > \times < b >\simeq \mathbb{Z}_p \times \mathbb{Z}_p$.*

Theorem 10. *(Fundemental Theorem of Finite Abelian Groups) Let G be a finite abelian group of order n. Let $n = p_1^{e_1} \dots p_r^{e_r}$. Then:*
(1). $G = G_1 \times \cdots \times G_r$ where $|G_i| = p_i^{e_i}$.
(2). G is a direct product of cyclic groups.

证明. (1). Let $n = p^e m$ s.t. p is a prime and $(p, m) = 1$. Let $H = \{g^m | g \in G\}$. Then H is a subgroup and every element of H has order p-power. Moreover $|H| = p^e$, and $G = H \times K$ where K has order m. By induction K we can prove (1).

(2). Assume that $|G| = p^e$. Let $g \in G$ which has the largest order. i.e. $|g| \leqslant |h|$ for any $h \in G$. If $G =< g >$, we are done. Suppose $G \neq< g >$. Claim: $G =< g > \times H$ for some $H < G$. Let $h \in G- < g >$ s.t. $h^p \in< g >$, so $h^p = g^k$ for some integer k. Since $|g| \leqslant |h|$, $k = pl$. Let $x = h^{-1} g^l$. Them $|x| = p$ as $x^p = h^{-p} g^{lp} = 1$. And $x \notin< g >$.

Let $\bar{G} = G/ < h >$. Then $|\bar{G}| \leqslant |G|$. By induction we may assume $\bar{G} =< \bar{g} > \times \bar{H}$, where $\bar{g}$ is the image of g in $\bar{G}$, and $|\bar{g}| = |g|$ is the largest order in $\bar{G}$.

Let H be the full preimage of $\bar{H}$ under $\pi : G \to \bar{G}$, i.e. $H = \{h \in G | \bar{h} \in \bar{H}\}$. Then $H < G$ and $H \cap G = \{e\}$. Thus $G =< g > H =< g > \times H$, as claimed. □