Lecture Note of Week 3

6. Normality, Quotients and Homomorphisms

(5.7) A subgroup \( N \) satisfying any one properties of (5.6) is called a normal subgroup of \( G \). Denote this fact by \( N \trianglelefteq G \). The homomorphism \( \pi \) in the proof of (v) \( \implies \) (vi) in (5.6) is called the natural projection or canonical homomorphism of \( G \) onto \( G/N \).

(5.8) Let \( \phi : G \to H \) be a homomorphism.

(i) if \( H' \leq H \), then \( \phi^{-1}(H') \leq G \).

(ii) If \( G' \leq G \), then \( \phi(G') \leq H \).

Proof (i) Use (2.3) and (ii) of (5.1). (ii) of (5.8) = (v) of (5.1).

(5.9) For any \( \bar{H} \leq G/N \), \( N \leq \pi^{-1}(\bar{H}) \leq G \).

Proof It suffices to show that \( \pi^{-1}(\bar{H}) \leq G \). Use (i) of (5.8).

(5.10) (Thm 5.6) Let \( f : G \to H \) be a group homomorphism and \( N \leq G \) such that \( N < \ker(f) \). Then there exists a unique homomorphism \( \bar{f} : G/N \to H \) such that

(i) \( \bar{f}(aN) = f(a) \), \( \forall a \in G \).

(ii) \( \text{Im}(f) = \text{Im}(\bar{f}) \) and \( \ker(\bar{f}) = \ker(f)/N \).

Moreover, (First Isomorphism Theorem) \( \bar{f} \) is an isomorphism iff \( f \) is an epimorphism and \( N = \ker(f) \).

(5.11) (Second Isomorphism Theorem) If \( K \leq G \) and \( N \leq G \), then \( K/(N \cap K) \cong NK/N \).

PF: Verify \( N \leq HK \). Find a homomorphism \( f : K \to HK/N \) with \( \ker(f) = (N \cap K) \).

(5.12) (Third Isomorphism Theorem) If \( K \leq G \) and \( N \leq G \) and if \( K < H \) then \( H/K \leq G/K \) and \( (G/K)/(H/K) \cong G/H \).

PF: Verify \( H/K \leq G/K \). Find a homomorphism \( f : G/K \to G/H \) with \( \ker(f) = H/K \).

(5.13) (Thm 5.11) Let \( f : G \to H \) be an epimorphism (onto homomorphism) of groups. Then the assignment \( K \mapsto f(K) \) is

(i) a bijection between the set \( S_f(G) = \{ K \leq G : \ker(f) \leq K \leq G \} \) and the set \( S(H) = \{ N \leq H \} \); and

(ii) a bijection between the set \( S_f(G) = \{ K \leq G : \ker(f) \leq K \leq G \} \) and the set \( S(H) = \{ N \leq H \} \).
(5.14) \( Z(G) \trianglelefteq G \).

(5.14a) If \( G/Z(G) \) is cyclic, then \( G \) is abelian.

(5.15) A group \( G \) is simple if \( |G| > 1 \) and if \( H \in \{ <1>, G \} \) whenever \( H \trianglelefteq G \).

(5.15a) The only simple abelian groups are \( Z_p \), for prime \( p \)'s.

Proof (5.1).

(5.16) An example: being normal is not a transitive relation. Let \( G = D_8 = \langle r, s | r^4 = 1, s^2 = 1, rs = sr^{-1} \rangle \). Let \( H = \{1, r^2, s, sr^2\} \), and \( K = \{1, s\} \). Then since \( |G : H| = 2 \), and \( |H : K| = 2 \), both \( K \trianglelefteq H \) and \( H \trianglelefteq G \). However, \( rsr^{-1} = r^2s \notin K \) and so \( K \not\trianglelefteq G \).

6. Symmetric, Alternating, and Dihedral Groups

(6.1) Review of symmetric group on \( n \) elements. Any permutation \( \phi \in S_n \) is a product of cycles (called the cycle decomposition of \( \phi \)). A 2-cycle is a transposition. Any permutation can be written as a product of transpositions.

\[
(i_1i_2\cdots i_k) = (i_1i_k)(i_1i_{k-1})\cdots(i_1i_3)(i_1i_2).
\]

(6.2) For each \( n \geq 3 \), the dihedral group \( D_n \) is a subgroup permutations of order \( 2n \) generated by

Any group with two generator \( a, b \) with the relations \( a^n = e \), \( b^2 = e \) and \( ba = a^{-1}b \) is isomorphic to \( D_n \), and is also called the dihedral group of order \( 2n \).

Example: \( D_4 \).

(6.3) No \( \phi \in S_n (n \geq 2) \) can be expressed both as a product of an even number of transpositions and as a product of an odd number of transpositions.

Proof We use \( e \) to denote the identity of \( S_n \).

(Step 1) (6.2) holds for \( \phi = e \).

Suppose that \( S_n \) is the set of all permutations on the set \( \{1, 2, \cdots, n\} \), and that \( e = \tau_k \cdots \tau_1 \), where each \( \tau_i \) is a transposition. Let \( X = \{x : 1 \leq x \leq n \) and \( x \) is involved in some of the \( \tau \)'s \}, and \( s = |X| \).
Argue by induction on $s$. If $s = 2$, then we may assume that the involved letters are 1 and 2, and $e = \tau_k \cdots \tau_1$, where each $\tau_i = (1,2)$. Since $e = (1,2)(1,2)$, $k$ must be even.

Assume that $s \geq 3$ and that (Step 1) holds for smaller values of $s$. Suppose that $e = \tau_k \cdots \tau_1$, where each $\tau_i$ is a transposition, and where the involved letters are in $\{1,2,\ldots,s\}$. We further argue by induction on $k$. (Step 1) holds trivially if $k = 2$, and so we assume further that (Step 1) holds for smaller values of $k$.

Pick $m \in X$. Let $\tau_j$ be the 1st transposition (from R to L) that contains $m$. Then $\tau_{j+1}\tau_j$ must be one in the left side of

\[
(x,m)(x,m) = e \\
(m,y)(m,x) = (m,x)(y,z) \\
(y,z)(m,x) = (m,x)(y,z) \\
(x,y)(x,m) = (y,z)(m,x)
\]

Hence the substitution of the left by the right either reduces the number of transpositions by 2; whence by induction on $k$, (Step 1) holds; or moves the 1st transposition containing $m$ to the left by one step. Repeat this process (assuming that $k$ remains unchanged) until the first $\tau_j$ containing $m$ is $\tau_{k-1}$. Then $\tau_{k-1} \tau_k \cdots \tau_1$ must be one of the four cases listed above. In this case, only the case $\tau_k = \tau_{k-1} = (x,m)$ will occur, as otherwise, after the process of pushing $m$ to the left, the right most transposition of a factoring of $e$ is the only transposition in the factorization of $e$ contains the element $m$, and so $m$ must be moved, contrary to the fact that $e \in S_n$ is the identity permutation.

Therefore, such a process can eliminate the element $m$, without introducing any new elements involved in the factorization, and without changing the parity of $k$. Now $X$ becomes $|X| - 1$, and so by induction on $|X|$, (Step 1) holds also for all values of $k$.

(Step 2) General Case: Suppose $\phi \in S_n$ has two factorizations:

\[
\phi = \tau_1 \tau_2 \cdots \tau_r = \tau'_1 \tau'_2 \cdots \tau'_t,
\]

where $\tau_i$’s and $\tau'_j$’s are transpositions. Then $\phi^{-1} = \tau_r^{-1} \cdots \tau_1^{-1}$ and so $e = \phi \phi^{-1} = \tau_r^{-1} \cdots \tau_1^{-1} \tau'_1 \tau'_2 \cdots \tau'_t$. Hence $r + t$ must be even, and so $r$ and $t$ must have the same parity.

(6.4) (Even and Odd Permutations) A permutation in $S_n$ is even (or odd) if it can be expressed as a product of an even (or odd) number of transpositions. The set of all even permutations in $S_n$ is denoted by $A_n$. $A_n$ is a subgroup of $S_n$, called the Alternating Group of degree $n$.

Proof Use (2.3) to show $A_n \leq S_n$. 

3
(6.5) Let \( a = (123 \cdots n) \) and
\[
b = \begin{cases}
(1n)(2(n-1)) \cdots \left( \frac{n}{2} \left( \frac{n}{2} + 1 \right) \right) & \text{if } n \text{ is even}, \\
(1n)(2(n-1)) \cdots \left( \frac{n-1}{2} \frac{n+3}{2} \right) \left( \frac{n+1}{2} \right) & \text{if } n \text{ is odd}.
\end{cases}
\]
The subgroup \( D_{2n} = \langle a, b \rangle \) is called the dihedral group of order \( 2n \). The presentation of \( D_{2n} \) is
\[
a^n = b^2 = 1, \text{ and } ba = a^{-1}b.
\]
We denote that \( D_{2n} = \langle a, b | a^n = b^2 = 1, \text{ and } ba = a^{-1}b \rangle \).

8. Direct Products and Direct Sums

(8.1) The direct product (also refereed as complete direct sum) of a collection of groups \( G_i, i \in I \) consists of the Cartesian product (of sets)
\[
\prod_{i \in I} G_i = \{ f : I \mapsto \cup_{i \in I} G_i \text{ such that for each } i \in I, f(i) \in G_i \}
\]
in which the binary operation is defined “componentwise”. That is, if \( f, g \in \prod_{i \in I} G_i \), then for each \( i \in I \), \( fg(i) = f(i)g(i) \) with the multiplication taking place in \( G_i \). One can routinely verify that this is a group.

Elements in \( \prod_{i \in I} G_i \) are also commonly written in a vector form \( a = \{ a_i \} \), where \( a_i = a(i) \). In this case, the product (sum, if in additive notation) of \( \{ a_i \} \) and \( \{ b_i \} \) will be \( \{ a_i b_i \} \) (or respectively, \( \{ a_i + b_i \} \), in additive notation.)

(8.2) For a fixed \( i \in I \), let \( J = I - \{ i \} \). Define a map \( \iota_i : G_i \mapsto \prod_{j \in I} G_j \) by defining \( \iota_i(g) \) to be the element in \( \prod_{j \in I} G_j \) such that for any \( j \in I \),
\[
\iota_i(g)(j) = \begin{cases} 
g & \text{if } j = i \\
e_{G_j} & \text{otherwise}
\end{cases}
\]
Then \( \iota_i \) is an injective homomorphism, (referred as the inclusion map, or the canonical injection), which is an isomorphism between \( G_i \) and a subgroup \( \iota_i(G_i) \).

(8.2A) Let \( \phi_i : \prod_{j \in I} G_j \mapsto \prod_{j \in J} G_j \) by \( \phi(f)(j) = f(j) \) if \( j \neq i \) and \( \phi(f)(j) = e_{G_i} \) if \( j = i \). Then \( \phi_i \) is an onto homomorphism with kernel \( \iota_i(G_i) \). Therefore, \( \prod_{j \in I} G_j / \iota_i(G_i) \cong \prod_{j \in J} G_j \).

(8.3) Fix \( i \in I \). Define \( \pi_i : \prod_{j \in J} G_j \to G_i \) by \( \pi_i(f)(j) = f(i) \) if \( j = i \) and \( \pi_i(f)(j) = e_{G_j} \) if
\( j \neq i \). Then \( \pi_i \) is also a homomorphism, (referred as the \textbf{canonical projection} map onto the \( i \)th component).

(8.4) Let
\[
\prod_{i \in I} G_i = \{ f \in \prod_{i \in I} G_i : \text{for all but finitely many } i \in I, f(i) = e_{G_i} \}.
\]
Then \( \prod_{i \in I} G_i \) is also a group, called the \textbf{(external) weak direct product} (also referred as the \textbf{(external) direct sum}) of the \( G_i \)'s.

(8.5) Let \( \{N_i | i \in I \} \) be a collection of normal subgroups of a group \( G \). If each of the following holds:

(i) \( G = \langle \cup_{i \in I} N_i \rangle \).
(ii) for each \( k \in I \), \( N_k \cap \langle \cup_{i \in I - \{k\}} N_i \rangle = \{ e \} \). Then \( G \cong \prod_{i \in I}^w N_i \).

\textbf{Proof} For each \( f \in \prod_{i \in I}^w N_i \), there is a finite set \( I_f \subseteq I \) such that if \( j \in I - I_f \), then \( f(j) = e_{N_j} \).

Define a map \( \phi : \prod_{i \in I}^w N_i \rightarrow G \) by \( \phi(f) = \prod_{i \in I_f} f(i) \). As \( |I_f| < \infty \), \( \phi(f) \) is a well-defined product in \( G \).

By (ii), when \( i \neq j \), \( \forall a_i \in N_i \) and \( \forall a_j \in N_j \), \( a_i a_j = a_j a_i \). This, together with (i), implies that \( \phi \) is an onto homomorphism.

Note \( \ker \phi = \{ f \in \prod_{i \in I}^w N_i | \prod_{i \in I_f} f(i) = e_G \} \). Apply (ii) again to see that \( \ker \phi = \{ e \} \), where \( e(i) = e_{N_i}, \forall i \in I \).

(8.6) Let \( G \) and the \( N_i \)'s satisfy the hypotheses (i) and (ii) in (1.4). Then \( G \) is called the \textbf{internal weak direct product} (also referred as the \textbf{internal direct sum}) of the \( N_i \)'s.

(8.7) Let \( \{ f_i : G_i \rightarrow H_i \} \) be a collection of group homomorphisms, and let \( f = \prod_{i \in I} f_i \) denote the map \( f : \prod_{i \in I} G_i \rightarrow \prod_{i \in I} H_i \) such that for every \( \{ a_i \} \in \prod_{i \in I} G_i \), \( f(\{ a_i \}) = \{ f_i(a_i) \} \in \prod_{i \in I} H_i \). Then \( f \) is a homomorphism. such that \( f(\prod_{i \in I}^w G_i) \subseteq \prod_{i \in I}^w H_i \), \( \ker f = \prod_{i \in I} \ker f_i \), and \( \text{Im } f = \prod_{i \in I} \text{Im } f_i \).

\textbf{Proof} Routine verification.

(8.8) Let \( \{ G_i | i \in I \} \) and \( \{ N_i | i \in I \} \) be collections of groups such that for each \( i \in I \), \( N_i \triangleleft G_i \). Then each of the following holds.

(i) \( \prod_{i \in I} N_i \triangleleft \prod_{i \in I} G_i \), and \( \prod_{i \in I} G_i / \prod_{i \in I} N_i \cong \prod_{i \in I} G_i / N_i \).
\[ \prod_{i \in I} N_i \triangleleft \prod_{i \in I} G_i, \text{ and } \prod_{i \in I} G_i/\prod_{i \in I} N_i \cong \prod_{i \in I} G_i/N_i. \]

**Proof** Let \( \pi_i : G_i \mapsto G_i/N_i \) be canonical epimorphism. Then \( \prod_{i \in I} \pi_i : \prod_{i \in I} G_i \mapsto \prod_{i \in I} G_i/N_i \) is also an epimorphism with kernel \( \prod_{i \in I} N_i \). Then apply the 1st isomorphism theorem.