Group Theory
Week #6, Lecture #21

Lemma If a group G has a subgroup H of index n, then G also has a normal subgroup N (contained in H) such that the index of N divides $n!$

$$\boxed{[G:H]=n \implies \exists\, N \subset H,\ N \trianglelefteq G,\ [G:N] \mid n!}$$

Comments
(1) Solves problem in the book with $n=3$, with sharper conclusion
(2) When $n=2$, this recovers result: $[G:H]=2 \implies H \trianglelefteq G$

[since Lemma shows $\exists N \subset H$ s.t. $N \trianglelefteq G$ and $[G:N] \mid 2! = 2 \implies N = H$

$\left(\text{since } \begin{matrix} N \subset H \subset G \\ [G:N]=[G:H] \end{matrix} \implies N=H\right)$]

Proof Consider the group action of G on the set

$$S = \{\text{left cosets of } H\}$$

by left multiplication:

$$G \times S \longrightarrow S \qquad (g, xH) \longmapsto (gx)\cdot H$$

Recall: $|S| =: [G:H]$, so S has size n

Associated to this action there is a homomorphism

$$\varphi : G \longrightarrow \mathrm{Sym}(S) = S_n$$
$$\varphi(g)(xH) = (gx)H$$

Let $N = \ker(\varphi)$. Then

(i) $N \trianglelefteq G$ ✓

(ii) $N \subseteq H$; $g \in N \implies gxH = xH,\ \forall x \in G$
$\overset{\text{take } x=e}{\implies} gH = H \implies g \in H$ ✓

(iii) By the FTH: $G/N \xrightarrow[\varphi]{\cong} \mathrm{im}(\varphi) \leq S_n$

But
- $|G/N| = [G:N]$
- $\underbrace{|\mathrm{im}(\varphi)| \mid |S_n|}_{\text{by Lagrange's theorem (since } \mathrm{im}(\varphi) \text{ is a subgroup of } S_n)} = n!$

$\therefore \quad [G:N] = |G/N| \underset{FTH}{=} |\mathrm{im}(\varphi)| \mid |S_n| = n!$ $\boxed{\text{QED}}$

Corollary Let G be a finite group, and let p be the smallest prime dividing the order of G. Then every subgroup $H < G$ of index p is normal.

Particular cases:
- $|G| = 2m$, and $[G:H] = 2 \Rightarrow H \trianglelefteq G$
- $|G|$ odd, $3 \mid |G|$, then $[G:H] = 3 \Rightarrow H \trianglelefteq G$
- Informs on sizes of subgroups of finite simple groups

Proof Let $N \subseteq H$ be the normal subgroup of G constructed in the Lemma. Then:
- $[G:N] \mid p!$ (by Lemma)
- $[G:N] \mid |G|$ (by Lagrange)
- p smallest prime dividing $|G|$ (by assumption)
- $[G:N] \geq [G:H] = p$ (by assumption & $N \subseteq H$)

Hence: $\boxed{[G:N] = p}$

[Since all prime factors of $p! = p(p-1)\cdots 3\cdot 2\cdot 1$ are either p or smaller than p, and, if one of those smaller primes (say, q) were to divide $[G:N]$, then $q \mid |G|$ — contradiction!]

Now since $N \subseteq H \subseteq G$ and $[G:N] = [G:H]$ $(=p)$ we conclude that $N = H$, and so $H \trianglelefteq G$.

QED

Application If G is a p-group (i.e. $|G| = p^n$, $n \geq 1$) and H is a subgroup of index p, then $H \trianglelefteq G$.

Product of subgroups

Definition (1) Let S and T be two subsets of a group G. Define their product to be

$$\boxed{ST := \{x \in G : x = st \text{ for } s \in S, t \in T\}}$$

(a subset of G)

(2) If H and K are subgroups of G, we call HK the product of these subgroups

* WARNING: HK is not necessarily a subgroup of G.

Example: $G = S_3$, $H = \langle (12) \rangle$, $K = \langle (13) \rangle$ (two subgroups - not normal!)

then $HK = \{(\,), (12), (13), (123)\}$ - not a subgroup!

(since $(123)^{-1} = (132) \notin HK$, or since $|HK| = 4 \nmid 6$, so by Lagrange $HK \not\leq G$)

* On the other hand, if $(G,+)$ is abelian, then the product of H & K (called in this setting the sum, and denoted $H+K$) is a subgroup of G:

$$H + K := \{x \in G : x = h + k, \ h \in H, k \in K\}$$

check: $x_1, x_2 \in H+K$, then $x_1 = h_1 + k_1$, $x_2 = h_2 + k_2$

so $x_1 - x_2 = h_1 + k_1 - (h_2 + k_2) = (h_1 - h_2) + (k_1 - k_2) \in H+K$ ✓

Example $G = \mathbb{Z}$, $H = 4\mathbb{Z}$, $K = 6\mathbb{Z}$ $\Rightarrow$ $H + K = 2\mathbb{Z}$

more generally : $m\mathbb{Z} + n\mathbb{Z} = \gcd(m,n)\cdot\mathbb{Z}$

Proposition $\boxed{HK \leq G \iff HK = KH}$

i.e., HK is a subgroup of G if and only if

$$\left[\forall h_1 \in H, \forall k_1 \in K, \exists k_2 \in K, h_2 \in H \text{ such that } h_1 k_1 = k_2 h_2\right]$$

Proof ($\Longrightarrow$) If HK is a subgroup, then, $\forall h_1, k_1, h_2, k_2$

(i) $\exists h_3, k_3$ s.t. $(h_1 k_1)\cdot(h_2 k_2) = h_3 k_3$

(ii) $\exists h_4, k_4$ s.t. $(h_1 k_1)^{-1} = \boxed{k_1^{-1} h_1^{-1} = h_4 k_4}$

$\boxed{HK \subseteq KH}$: $h_1 k_1 \in HK \Rightarrow h_1 k_1 = (k_1^{-1} h_1^{-1})^{-1} = (h_4 k_4)^{-1} = k_4^{-1} h_4^{-1} \in KH$

$\boxed{KH \subseteq HK}$ – symmetric argument

($\Longleftarrow$) If $HK = KH$, then $(\forall h_1, k_1, \exists h_2, k_2 \text{ s.t. } h_1 k_1 = k_2 h_2)^{(*)}$

take $x_1 = h_1 k_1$ and $x_2 = h_2 k_2$ in H; then:

$$x_1 x_2^{-1} = (h_1 k_1)\cdot(h_2 k_2)^{-1} = h_1 \underbrace{k_1 k_2^{-1}} \underbrace{h_2^{-1}}$$

$$\underset{(*)}{=} h_1 \cdot h_3 \cdot k_3$$

$$= (h_1 h_3)(k_3^{-1})^{-1} \in HK$$

$\therefore HK \leq G$ $\boxed{\text{QED}}$

Corollary If $H \subseteq N(K)$, then $HK \leq G$

Comment the condition $\boxed{H \subseteq N(K)}$ means:

$\boxed{hKh^{-1} \subseteq K \quad , \forall h \in H}$

or $\boxed{hkh^{-1} \in K \quad , \forall h \in H, \forall k \in K}$

Proof $H \subseteq N(K) \iff hKh^{-1} \subseteq K \quad \forall h \in H$

$\iff hKh^{-1} = K \quad \forall h \in H$

since orbits of K under conj. action are either equal or disjoint

$\iff hK = Kh \quad \forall h \in H$

$\implies HK = KH$

$\overset{\text{Prop}}{\iff} HK \leq G$ $\square$

Prop Let G be a finite group and H, K two subgroups. Then

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

Proof (next time)

Corollary If $H \leq G$ and $K \trianglelefteq G$, then $HK \leq G$

(reason: $K \trianglelefteq G$ means $N(K) = G \Rightarrow H \subseteq N(K)$)

Corollary If $H \trianglelefteq G$, $K \trianglelefteq G \implies HK \trianglelefteq G$

Proof We have $N(H) = N(K) = G$. Hence

$\forall g \in G$: $\forall h \in H, k \in G$

$$g(hk)g^{-1} = gh(g^{-1}g)kg^{-1} = \underbrace{(ghg^{-1})}_{\in H}\underbrace{(gkg^{-1})}_{\in K} \in HK$$

← since H, K normal

$\square$
