Lecture 3: Sylow Theorems & Group Theory Story Time

In this lecture we survey many results from intermediate group theory. Many of these are improvements on Cauchy's Th$\underline{m}$ or sort of partial converses to Lagrange's Th$\underline{m}$. The big idea here is exploring the landscape of finite groups and their structure. I'll also present isomorphism theorems and hopefully we will prove those (but to be clear, I'm not proving most of the results here, I've taken these from §1.7 and 4.2 of Rotman's Advanced Modern Algebra, 2$^{\text{nd}}$ Ed.) (the master, his book is a treasure)

Th$\underline{m}$ 1.113 If p is prime and $G \neq \{1\}$ is a finite p-group, then the center of G is not trivial; $Z(G) \neq \{1\}$.

Def$\underline{n}$ If p is prime, then a group is called a p-group iff $|G| = p^n$ for some $n \geq 0$

Corollary 1.114 If p is prime, then every group G of order p^2 is abelian.

Prop. 1.116 If G is group of order p^ℓ, then G has normal subgroup of order p^k for every $k \leq \ell$.

In abelian groups every subgroup is normal, well a simple group is in some sense opposite,

Def$\underline{n}$ A group G is called simple if $G \neq \{1\}$ and G has no normal subgroups except G and $\{1\}$.

Prop. 1.117 An abelian group G is simple iff it is finite and prime order.

Cor. 1.118 A finite p-group G is simple iff $|G| = p$.

(FIRST BOOK ON GROUP THEORY)

History: • Jordan's "Traité des Substitutions et des Équations Algebriques" published 1870 on "theory of eq^{n}'s (Galois Theory)

over half of it on Galois theory

• 1868, Schering proved the "Basis Th^{m}"; every finite abelian group is direct product of primary cyclic groups.

• 1870, Kronecker also proves Basis Th^{m}

• 1878, Frobenius and Stichelbergen proved the Fundamental Th^{m} of Finite Abelian Groups

• 1872, Sylow showed for every finite group G and every prime p, if p^e is largest power dividing $|G|$ then G has a subgroup of order p^e (we call these Sylow p-subgroups)

Def^{n}/ Let p be prime. A sylow p-subgroup of a finite group G is a maximal p-subgroup P. Here maximal means if Q is a p-subgroup of G with $P \subseteq Q$ then $P = Q$

The conjugate of a subgroup $H \leq G$ is another subgroup of G of the form aHa^{-1}.

Def^{n}/ The normalizer of $H \leq G$ is $N_G(H) = \{a \in G \mid aHa^{-1} = H\}$

The # of conjugates of H in G is $[G : N_G(H)]$.

Lemma 4.36 Let P be a Sylow p-subgroup of finite group G

(i) every conjugate of P is also a Sylow p-subgroup of G

(ii.) $|N_G(P)/P|$ is prime to p

(iii.) If $a \in G$ has order some power of p and $aPa^{-1} = P$, then $a \in P$.

Th^{m} 4.37 (Sylow) Let G be a finite group of order $p_1^{e_1} \cdots p_t^{e_t}$ and let P be the Sylow p-subgroup of G for some prime $p = p_j$

(i.) Every Sylow p-subgroup is conjugate to P

(ii.) If there are r_j Sylow p_j-subgroups then r_j is a divisor of $|G|/p_j^{e_j}$ and $r_j \equiv 1 \mod p_j$

Coro. 4.38 A finite group G has unique Sylow p-subgroup P for some prime p iff $P \triangleleft G$.

Th^{m} (4.39) (Sylow) If G is finite group of order $p^e m$ where p is prime and $p \nmid m$, then every Sylow p-subgroup of G has order p^e

Th^{m} 4.41 (Wielandt) If G is finite group of order $p^e m$ where p prime and $p \nmid m$ then G has subgroup of order p^e

Prop 4.42 A finite group G all of whose Sylow subgroups are <u>normal</u> is the direct product of its Sylow subgroups.

this makes G nilpotent (def^{n} of nilpotent would take a minute... maybe later)

Lemma 4.43 $\nexists$ nonabelian simple group G of order $|G| = p^e m$ where p prime and $p \nmid m$ and $p^e \nmid (m-1)!$

Prop. 4.4.4 $\nexists$ nonabelian simple groups of order less than 60.

Th^{m} 1.121 A_5 is a simple group $(|A_5| = 60)$

Galois Theory : Why Solvable & Simple Matters

The goal of Galois Theory is to solve polynomial equations via radicals (like the quadratic formula). In 1827, Abel proved $f(x)$ is solvable by radicals if (what we later termed) the Galois group is commutative. Then in 1830 Galois showed $f(x)$ solvable only if it had a solvable Galois group (hence the terminology)

Defn/ A <u>normal series</u> of a group G is a finite sequence of subgroups $G = G_0, G_1, G_2, \dots, G_n$ with $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = \{1\}$ and $G_{j+1} \triangleleft G_j$ for $j = 0, 1, \dots, n-1$. The <u>factor groups</u> of the series are $G_0/G_1, \; G_1/G_2, \dots, \; G_{n-1}/G_n$ and the length of the series is the # of strict inclusions (or if you prefer the # of nontrivial factor groups)

Defn/ G is <u>solvable</u> if it has a normal series whose factor groups are cyclic of prime order

Defn/ A <u>composition series</u> is a normal series all of whose nontrivial factor groups are <u>simple</u>

<u>Remark</u>: Suppose we know K is normal subgroup and $Q = G/K$ is given then what can we say about G? Can we reconstruct G from knowing K and Q?

$\boxed{E1}$ $K \times Q$ is an extension of K by Q

$\boxed{E2}$ S_3 and $\mathbb{Z}_6$ are extensions of $\mathbb{Z}_3$ by $\mathbb{Z}_2$

$\boxed{E3}$ $\mathbb{Z}_6$ is an extension of $\mathbb{Z}_2$ by $\mathbb{Z}_3$
Yet S_3 is not an extension of $\mathbb{Z}_2$ as S_3 has no normal subgroup of order 2.

Rotman explains on p. 257 that the extension problem is solved in a certain sense, but some questions are not computationally understood. A key result towards surveying the structure of all finite groups was:

$\boxed{\text{CLASSIFICATION THEOREM OF FINITE SIMPLE GROUPS}}$

(completed in 1980's, proof spans multiple papers totalling something like 10,000 pages)

(1963) <u>Feit - Thompson Theorem</u>: (proof 250 pages I believe)
"Every finite group of odd order is solvable" or
"Every nonabelian finite simple group has even order"

conjectured in 1911

<u>BURNSIDE'S Th^m</u>: no group of order p^2q^2 is simple when p and q are primes.

<u>Th^m/ A simple group is solvable iff it is abelian</u> (of prime order).

DUMMIT AND FOOTE, p. 104 give this

> Th^m/ There is a list consisting of 18 (infinite) families of simple groups and 26 simple groups not belonging to these families (the sporadic simple groups) such that <u>every</u> finite simple group is isomorphic to <u>one</u> of the groups in this list.

> Th^m (Feit-Thompson) If G is simple group of odd order then $G \cong \mathbb{Z}_p$ for some prime p.

(The classification problem took a century to solve, you can read more about the Hölder program if interested obviously much more to say... but now the importanter part)

On Quotients, Products, Homomorphisms and Isomorphisms

We should review the essentials and add a few deeper things

Prop. 1.62 Let $f : G \to H$ be group homomorphism.

(i.) $\ker(f) \leq G$ and $\mathrm{im}(f) \leq H$.

(ii.) if $x \in \ker(f)$ and $a \in G$ then $axa^{-1} \in \ker(f)$

(iii.) f is an injection iff $\ker(f) = \{1\}$.

Defn/ A subgroup K of group G is called a <u>normal</u> <u>subgroup</u> if $k \in K$ and $g \in G$ imply $gkg^{-1} \in K$. We write $K \triangleleft G$.

A normal subgroup is closed under conjugation. Note $\underbrace{\ker(f) \triangleleft G}$.

If $K \triangleleft G$ then G/K has natural group structure Prop. 1.62 (ii.)

Defn/ $G/K = \{aK \mid a \in G\}$ where $(aK)(bK) = abK$

Corollary 1.75 Every normal subgroup $K \triangleleft G$ is the kernel of some homomorphism

<u>Proof</u>: construct the <u>natural map</u> $\pi : G \to G/K$ by $\pi(a) = aK$. Notice, if $aK \in G/K$ then $\pi(a) = aK$ and

$$aK\, bK = abK \implies \pi(a)\pi(b) = \pi(ab)$$

thus π is <u>surjective</u> <u>homomorphism</u>. Notice $K = 1_{G/K}$ that is K is the identity element in G/K,

$$\begin{aligned} \ker(\pi) &= \{g \in G \mid \pi(g) = gK = K\} \\ &= \{g \in G \mid g \in K\} \\ &= K. \end{aligned}$$

Th^m(1.76) [FIRST ISOMORPHISM Th^m]

If $f : G \to H$ is homomorphism of groups then $\ker(f) \trianglelefteq G$ and $G/\ker(f) \cong im(f)$.
In particular, if $\ker(f) = K$ then $\varphi : G/K \to im(f) \subseteq H$ given by $\varphi : aK \mapsto f(a)$ is an isomorphism

Proof: it is known $K = \ker(f) \trianglelefteq G$. Observe, if $aK = bK$ then $a = bk$ for some $k \in K$ thus

$$f(a) = f(bk) = f(b)f(k) = f(b)$$

since $f(k) = 1$. Consequently, $\varphi : aK \mapsto f(a)$ meaning $\varphi(aK) = f(a)$ is a well-defined map. Next, we check that φ is homomorphism,

$$\begin{aligned} \varphi(aK\, bK) &= \varphi(abK) \\ &= f(ab) \\ &= f(a)f(b) \\ &= \varphi(aK)\varphi(bK) \end{aligned}$$

Since $\varphi(aK) = f(a) \in im(f)$ we see $im(\varphi) \subseteq im(f)$. Let $y \in im(f)$ then $y = f(a) = \varphi(aK)$ thus $y \in im(\varphi)$ and so $im(f) \subseteq im(\varphi)$ $\therefore$ $im(f) = im(\varphi)$. But, we define $\varphi : G/K \to im(f)$ $\therefore$ φ surjective.
Finally, suppose $\varphi(aK) = \varphi(bK) \Rightarrow f(a) = f(b)$ then $1 = f(b)^{-1}f(a) = f(b^{-1}a)$ $\therefore$ $b^{-1}a \in \ker(f) = K$ and so $aK = bK$ and we find φ injective.

$\therefore$ $\varphi : G/K \longrightarrow im(f)$ is group isomorphism. //

$\boxed{\text{Def}^{\text{n}}/ \text{ Suppose } H, K \leq G \text{ then } HK = \{hk \mid h \in H, k \in K\}}$

$\underbrace{\phantom{HK = \{hk \mid h \in H, k \in K\}}}_{\text{internal product of subgroups}}$

In fact, HK may not be a subgroup even if H and K are subgroups (we could define ST for $S \subseteq G$, $T \subseteq G$ the same as above)

$\boxed{E4}$ $G = S_3$ has $H = \langle (1,2) \rangle$ and $K = \langle (1,3) \rangle$ both subgroups of order two and

$$HK = \{(1), (12), (13), (132)\} \not\leq S_3$$

since $|HK| = 4$ and $4 \nmid 6 = |S_3|$.

Neither H nor K are normal subgroups of S_3 above.

Prop 1.72

(i.) If $H, K \leq G$ and at least one of H & K is normal then $HK \leq G$. Moreover, $HK = KH$.

(ii.) If both H and K are normal subgroups then $HK \trianglelefteq G$

Prop 1.79 (Product Formula)

If $H, K \leq G$ for finite group G then

$$\boxed{|HK||H \cap K| = |H||K|} \leftarrow *$$

Proof summary: $f : H \times K \longrightarrow HK$ given by $f(h,k) = hk$ is surjection with fibers all the size of $H \cap K$. But, the non-empty fibers of a function partition the domain and thus $\dfrac{|H \times K|}{|H \cap K|} = |HK|$ and as $|H \times K| = |H||K|$ we have the desired result.

Remark: $HK \not\leq G$ but argument is not bothered by this. That said, the formula $*$ is easily derived when $HK \leq G$

Thm (1.80) (2nd Isomorphism Thm)

$$\boxed{\text{If } H, K \leq G \text{ and } H \triangleleft G \text{ then } HK \leq G \text{ and } H \cap K \triangleleft K \text{ and } K/_{H\cap K} \cong HK/_{H}}$$

Proof: since $H \triangleleft G$ and $K \leq G$ we have $HK \leq G$.
We leave normality of H within HK as exercise.
We can show every coset $xH \in HK/H$ as the form kH for some $k \in K$. Why? Let $x \in HK$ then $x = hk$ for $h \in H$ and $k \in K$. Thus $xH = hkH$.

$$hk = k(k^{-1}hk) = kh'$$

usual coset absorption rule.

for some $h' \in H \triangleleft G$. Thus $hkH = kh'H = kH$.

$$f : K \longrightarrow HK/H \text{ given by } f : k \longmapsto kH$$

is thus surjective. Notice f is homomorphism since $\pi : G \longrightarrow G/H$ restricts to f. (claim)
But, $\ker(\pi) = H$ and hence $\ker(f) = H \cap K \triangleleft K$ and by 1st Isomorphism Thm, $\underline{K/_{H\cap K} \cong HK/_H}$. //

Easy Counting?

$$\left| K/_{H\cap K} \right| = \frac{|K|}{|H\cap K|} \quad \text{and} \quad \left| \frac{HK}{H} \right| = \frac{|HK|}{|H|}$$

$$\therefore \frac{|K|}{|H\cap K|} = \frac{|HK|}{|H|} \Rightarrow \underline{|H\cap K|\,|HK| = |H|\,|K|}.$$

Thm (1.8) (THIRD ISOMORPHISM THEOREM)

If $H, K \trianglelefteq G$ with $K \subseteq H$ then $H/K \trianglelefteq G/K$ and $\dfrac{(G/K)}{(H/K)} \cong \dfrac{G}{H}$

Proof: Let $\underbrace{f : G/K \to G/H \text{ be defined by } aK \mapsto aH}_{\text{"enlargement of coset"}}$.

If $\bar{a} \in G$ and $\bar{a}K = aK$ then $a^{-1}\bar{a} \in K \subseteq H$ $\therefore$ $a^{-1}\bar{a} \in H$ and hence $aH = \bar{a}H$ so f is well-defined. If $bH \in G/H$ then $f(bK) = bH$ thus f is surjective. Also,

$$\begin{aligned} f(aKbK) &= f(abK) \\ &= abH \\ &= aHbH \\ &= f(aK)f(bK) \quad \therefore \ f \text{ homomorphism.} \end{aligned}$$

Notice,
$$\begin{aligned} \ker(f) &= \{ aK \mid f(aK) = aH = H \} \\ &= \{ aK \mid a \in H \} \\ &= H/K \end{aligned}$$

Hence $H/K \trianglelefteq G/K$ and $\dfrac{G/K}{H/K} \cong \dfrac{G}{H}$ by 1st Isomorphism Thm. //

$\boxed{E5}$ $G = \mathbb{Z}$ has $\langle 3 \rangle, \langle 6 \rangle \trianglelefteq \mathbb{Z}$ and $\langle 6 \rangle \subseteq \langle 3 \rangle$ then $\dfrac{\mathbb{Z}/\langle 6 \rangle}{\langle 3 \rangle / \langle 6 \rangle} \cong \dfrac{\mathbb{Z}}{\langle 3 \rangle} = \mathbb{Z}_3$.

The proof and statement of the following extended isomorphism $Th^{\underline{m}}$ is found on p. 53 of Rotman's Advanced Modern Algebra, 2^{nd} Ed.

Prop. 1.82 (Correspondence $Th^{\underline{m}}$)

Let G be group, let $K \trianglelefteq G$, and let $\pi : G \to G/K$ be the natural quotient map. Then

$$S \longmapsto \pi(S) = S/K$$

is a bijection between $\mathrm{Sub}(G; K)$ (family of all subgroups S of G which contain K) and $\mathrm{Sub}(G/K)$ (the family of all subgroups of G/K). Moreover,

$$T \subseteq S \subseteq G \iff T/K \subseteq S/K$$

in which case $[S : T] = [S/K : T/K]$ and $T \trianglelefteq S$ iff $T/K \trianglelefteq S/K$ in which case

$$S/T \cong \frac{S/K}{T/K}$$

$$\begin{tikzcd}
G \arrow[d, dash] \arrow[dr] & \\
S \arrow[d, dash] \arrow[dr] & G/K \arrow[d, dash] \\
T \arrow[d, dash] \arrow[dr] & S/K \arrow[d, dash] \\
K \arrow[dr] & T/K \arrow[d, dash] \\
 & \{1\}
\end{tikzcd}$$

Remark: $Th^{\underline{m}}$ 20 on p. 99 of Dummit & Foote's 3^{rd} Ed. gives an extended version of the Correspondence $Th^{\underline{m}}$ which D&F call the LATTICE ISOMORPHISM $Th^{\underline{m}}$

PROPOSITION 1.85

Let G and G' be groups with $K \lhd G$ and $K' \lhd G'$. Then $(K \times K') \lhd (G \times G')$ and

$$\frac{G \times G'}{K \times K'} \cong \left(\frac{G}{K}\right) \times \left(\frac{G'}{K'}\right)$$

Proof: $f : (g, g') \longmapsto (\pi(g), \pi'(g')) = (gK, g'K')$ defines a surjective homomorphism with $\ker(f) = K \times K'$ then the proposition follows by 1^{st} isomorphism Th^{m}. //

PROPOSITION 1.86

If G is a group with normal subgroups H & K with $H \cap K = \{1\}$ then $G \cong H \times K$

Proof Sketch: $\varphi : G \longrightarrow H \times K$ given by $\varphi(g) = (h, k)$ where $g = hk$ for $h \in H$ and $k \in K$. Then φ is an isomorphism //

Remark: need H and K normal. Notice S_3 has $H = \langle (123) \rangle$ where $[S_3 : H] = |S_3|/|H| = 6/3 = 2$ $\therefore$ $H \lhd S_3$ and $K = \langle (12) \rangle$ where $K \ntriangleleft S_3$ and $H \cap K = \{1\}$ and $HK = S_3$ however $S_3 \ncong H \times K \cong \mathbb{Z}_3 \times \mathbb{Z}_2$ (abelian)

Th^{m} (5) Schur - ZASSENHAUS (NICHOLSON, p. 374 of Intro to Abstract Alg., 3^{rd} Ed)

Let G be group of order kn where $\gcd(k, n) = 1$. Assume $K \lhd G$ and $|K| = k$. Then G has subgroup H of order n and so is semidirect product $K \times_\theta H$

(I'll probably give homework which explores what ↗ means)

§ 8.5 of Nicholson has nice introduction