1 Sylow's Theorems

The Lagrange's Theorem states that if G is a finite group and H is a subgroup of G, then $|H|$, the order of H divides $|G|$, the order of G. We explore the following question: If G is a finite group, and k is an integer which divides $|G|$, does there exist a subgroup H of order k? This is, in a way, the converse of Lagrange's Theorem.

By the Theorem on structure of finite abelian groups, we know that this is indeed true for finite abelian groups. However, it fails for non abelian groups. For example, $|A_4| = 12$, has no subgroup of order 6.

Lemma 1 (Binomial Coefficients modula a prime)**.** *Let $n = p^\alpha m$ where p is a prime. Then $\binom{n}{p^\alpha} \equiv m(\mod p)$.*

Proof. From Fermate-Euler's Theorem, we know that for any positive integer x, $(x+1)^{p^\alpha} \equiv x^{p^\alpha} + 1(\mod p)$ Applying this to x^m instead of x, we get
$(x+1)^{p^\alpha m} \equiv x^{p^\alpha m} + 1(\mod p)$.

□

Theorem 1 (Sylow's Existence Theorem)**.** *Let G be a finite group of order $p^\alpha m$, where p is prime and $p \nmid m$. Then G has a subgroup H of order p^α.*

Proof. Let Ω be the collection of all subsets X of G of size p^α. Then,

$$|\Omega| = \binom{|G|}{p^\alpha} = \binom{p^\alpha m}{p^\alpha} \equiv m \not\equiv 0(\mod p).$$

Let G act on Ω via right regular action. Since $p \nmid |\Omega|$, there exists an orbit O such that $p \nmid |O|$, for the orbits of the action partition Ω.

Let $X_o \in O$ and H be $G_{X_o} \leq G$, the stabiliser of X_o. By the orbit stabiliser theorem, the size of this orbit is $|O| = \frac{|G|}{|H|}$, the number of cosets of H. Since $p \nmid |O|$ but $p^\alpha \,|\, |G| = |H||O|$, we must have $p^\alpha | \,|H|$. For each $x \in X_o$ and $h \in H$, we have $xh \in X_o$. So, we have $xH \subset X_o$. Then, $|H| = |xH| \leq |X_o| = p^\alpha$. As $H \leq G$, we get $|H| = p^\alpha$.

□

Definition 1 (Sylow $p-$subgroup)**.** *Let G be a finite group and p be a prime integer. A Sylow p-subgroup of G is a subgroup $P \leq G$ such that $|P| = p^\alpha \,|\, |G|$ but $|p^{\alpha+1}| \nmid |G|$. The set of all Sylow p-subgroups of G is denoted by $Syl_p(G)$.*

For each prime integer $p||G|$, $Syl_p(G) \neq \{\phi\}$. For prime integers p such that $p \nmid |G|$, set $Syl_p(G) = \{\{1_G\}\}$.

Corollary 1 (Cauchy's Theorem)**.** *Let G be a finite group with $p||G|$ where p is some prime integer. Then, G has an element of order p.*

Proof. By Sylow's Existence theorem, there exists a Sylow p- subgroup H of G. Since $p||G|$, P is a nontrivial subgroup of G. That means there exists $x \in P \backslash \{1_G\}$ having order $o(x) = p^e$, where $1 \leq e$. Set $y = x^{p^{e-1}}$. Then, $o(y) = p$. □

Each $P \in Syl_p(G)$ is a maximal subgroup of G.

Theorem 2 (Sylow Development)**.** *Let G be a finite group and $P \leq G$ be a p-subgroup, then there exists some $S \in Syl_p(G)$ with $P \leq S$.*

Theorem 3 (Sylow Conjugacy)**.** *Let G be a finite group. The set $Syl_p(G)$ is a single conjugacy class of Sylow subgroups of G.*

Theorem 4 (Conjugacy of Sylow p-subgroups)**.** *Let G be a finite group and suppose $P \leq G$ is a p-subgroup and $S \in Syl_p(G)$. Then $P \leq S^x = x^{-1}Sx$ for some x in G.*

Proof. Let $\Omega = \{Sx \mid x \in G\}$ be the set of right cosets of X in G. as S is in $Syl_p(G)$, p does not divide $|\Omega|$. Let P act on Ω via right regular action. The size of Ω is the sum of sizes of all orbits in it. Hence there exists an orbit O whose size is not divisible by p. Let H be the stabiliser of Sg, some element in the orbit O. As P is a p-group, $|P|$ is p^α for some positive integer α. Also, $H \leq P$, so $|H| = p^e$ for some positive integer $e \leq \alpha$. As $p \not| \, |O|, = \frac{|P|}{|H|}$, we get that $|H| = p^\alpha$, whence $H = P$. This means for any element x in P, we get $Sg \cdot x = Sgx = Sg$, or gxg^{-1} is in S. This shows that $P \leq g^{-1}Sg$. □

The collection of all Sylow p-subgroups, $Syl_p(G)$, is quite interesting.

Corollary 2 (Number of Sylow p-subgroups)**.** *Let G be a finite group and let $P \in Syl_p(G)$. Then, $|Syl_p(G)| = [G : N_G(P)]$, where $N_G(P)$ is the normaliser of P in G. In particular, $|Syl_p(G)|$ divides $[G : P] = \frac{|G|}{|P|}$.*

Proof. Let P act on $Syl_p(G)$ by conjugation. The number of conjugate subgroups of P is exactly the number of elements in $Syl_p(G)$ because each Sylow p-subgroup of G is conjugate to P. Let Ω be the set of all conjugates of P in G and let G act on Ω by conjugation. The size of Ω, which is the number of conjugates of P in G is $[G : N_G(H)]$ because $N_G(P)$ is the stabiliser of P in G. □

Corollary 3 (Normal Sylow p-subgroups)**.** *Let S be a Sylow p-subgroup of G. The following statements are equivalent*

1. *S is normal in G.*
2. *S is the unique Sylow p-subgroup of G.*
3. *Every p-subgroup of G is contained in S.*
4. *S is a characteristic subgroup of G.*

Definition 2 (Characteristic subgroups)**.** *If G is a group, then a subgroup H of G is said to be characteristic in G if for any $\sigma \in \mathrm{Aut}(G)$, $\sigma(S) = S$.*

Proof. (1) $\implies$ (2) As any two Sylow p-subgroups of G are conjugate to each other, we conclude that there is only one Sylow p-subgroup of G because it has only one conjugate.

(2) $\implies$ (3) As each p-subgroup is ocntained in some Sylow p-subgroup, we get that any given p-subgroup P is contained in S.

(3) $\implies$ (4). For each $\sigma \in \mathrm{Aut}(G)$, $\sigma(S)$ is a p-subgroup of G. From (3), we get that $\sigma(S) \leq S$. Moreover, $\sigma(S) = S$. Then S is characteristic in G.

(4) $\implies$ (1) This is true because conjugation is an inner automorphism. □

Lemma 2 (p-subgroups of normaliser)**.** *Let G be a finite group and let $S \in Syl_p(G)$. Suppose P is a p-subgroup of $N_G(S)$. Then $P \leq S$.*

Proof. By the Sylow's Development Theorem, we know that $P \leq S^x = x^{-1}Gx$ for some $x \in G$. Since $P \leq N_G(S)$, we know that $PS = SP$. From previous knowledge, we know that this happens if and only if SP is a subgroup of G. So, we get that $S \leq SP \leq G$. For any two groups H, K of a group G, we have $|HK| = \frac{|H||K|}{|H \cap K|}$. As SP is also a p-subgroup and S is a maximal p-subgroup in G, we get that $SP = S$ which happens if and only if $S = P$. □

Alternative Proof. Since $S \in Syl_p(G)$ and $S \leq N_G(S) \leq G$, we must have S is a Sylow p-subgroup of $N_G(S)$. Moreover, P is a p-subgroup of $N_G(S)$ and $S \triangleleft N_G(S)$ so applying the corollary about normal Sylow p-subgroups, we get that $P \leq S$. □

Lecture 08 *19 Sep 24, Thu*

Theorem 5 (Sylow Counting Theorem)**.** *Let G be a finite group. Denote the size of the set of all Sylow p-groups in G by $n_p(G)$. In other words, $n_p(G) = |Syl_p(G)|$. Then $n_p(G) \equiv 1(\mod p^e)$ if $p^e \leq [S : S \cap T]$ for all distinct $S, T \in Syl_p(G)$.*

Proof. Let $P \in Syl_p(G)$. Let P act on $Syl_p(G)$ act on $Syl_p(G)$ via conjugation. Then $\{P\}$ is one orbit of the action. Now it suffices to show all the other orbits have size divisible by p^e. Suppose $S \in Syl_p(G)$ with $S \neq P$. The orbit O_S of S under this action has size equal to $\frac{|P|}{|N_P(S)|} = [P : N_P(S)]$.

Since $N_P(S)$ is a subgroup of $N_G(S)$, we have $N_P(S) \leq S$ by the Lemma 2. Further, we also know that $N_P(S) \leq P$. So, we get $N_P(S) \leq S \cap P$. WHY IS $S \cap P \leq N_P(S)$?

□

Theorem 6 (order pq group not simple)**.** *Let $|G| = pq$, where $p > q$ and p, q are prime integers. Then G has a normal Sylow p-subgroup, Also, if G is non abelian, then $q \mid p - 1$ and G has exactly p Sylow q-subgroups.*

Proof. By corollary 2, we know that $n_p(G) \mid [G : P]$, where $P \in Sylow_p(G)$. Moreover, $n_p(G)$ is either 1 or q. If $n_p(g) = 1$, then by the **??**, we know that this means p is normal in G. If $n_p(G) = q$, then by Sylow Counting Theorem, **??**, we know that $p \mid q - 1$ but this cannot happed because $p > q$. By **??**, we

also know that $n_p(G) = 1$ or p. Since G/P is a group of order q, G/P is abelian and consequently $G' \subseteq P$. This means that $G' \subseteq P \cap Q = \{1_G\}$ which happens exactly when G is abelian. □

Theorem 7 (order p^2q group is not simple)**.**

Proof. By the Corollary on number of Sylow p-subgroups, **??** we know that the number of Sylow$q$-subgroups is $n_q(G) \in \{1, p, p^2\}$ and $n_p(G) \in \{1, q\}$. By Sylow counting Theorem, $n_p(G) \equiv 1(\mod p), n_q(G) \equiv 1(\mod q)$. If $n_q(G) = 1$, then we know that there is exactly one Sylow q-subgroup and it is normal. If $n_q(g) = p$, then $q|p-1$ and $q < p$. So, $q \not\equiv 1(\mod p)$. Therefore $n_p(G) = 1$ and the unique Sylow p-subgroup in G is normal. If $n_q(G) = p^2$, then there are p^2 many distinct subgroups of order q. If Q_1 and Q_2 in $Syl_q(G)$ are distinct Sylow q-subgroups, then $Q_1 \cap Q_2 = \{1_G\}$. The p^2 elements of order q cover $p^2(q-1)$ elements of order q. Then, consider $X = G \backslash \bigcup_{Q \in Syl_q(G)} Q \backslash \{1_G\}$. Then X contains all elements in G whose order is not equal to q. $|X| = p^2q - p^2(q-1) = p^2$. Then, X must be the Sylow p-subgroup. This shows that $n_p(G) = 1$. □

Remark 1 (Burnside)**.** *If $|G| = p^a q^b$ where p, q are distinct primes, G cannot be simple unless it has order prime power.*

Lemma 3 (Sylow p-subgroup of simple groups)**.** *Suppose $|G| = p^\alpha m$ where $a > 0, m > 1$ and $p \not| m$. If G is simple, then $n = n_p(G)$ satisfies $|G| \,|\, n!$.*

Proof. Set $P \in Syl_p(G)$. By Corollary on Number of Sylow$p$-subgroups, **??**, $n = n_p(G) = [G : N_G(P)]$. Since G is simple, $N_G(P) < G$ hence $n > 1$. By the Theorem on search for normal subgroups, we know that there exists $N \leq N_G(P)$ such that $N \triangleleft G$ and $[G : N] \,|\, n!$. Since G is simple and $N \leq N_G(P) < G$, then $n = \{1_G\}$. Consequently, □

Example 1. *If $|G| = 2376 = 2^3 \times 3^3 \times 11$, then G is not simple.*

Proof. Assume G is simple. We prove this theorem by contradiction. The number of Sylow 11-subgroups, $n_{11}(G) \equiv 1(\mod 11)$. we have $n_{11}(G)$ is $1, 12$ but not $23, 34, 45, 56, 67, 78, 89, 100$ or 112. This is because $n_{11}(G)$ also divides $[|G| : |S|] = 2^3 \times 3^3 = 216$. We want to find a subgroup $H \leq G$ such that $n = [G : H]$ and $1 < n < 11$. This would suffice because by Theorem on Search for Normal Subgroups, we know that there must exist $K \leq H$ such that $K \triangleleft G$ and $[G : K] \,|\, n!$. This would be a contradiction because $11||G|$ but $11 \not| n!$ for $n < 11$. Let $S \in Syl_{11}(G)$ and $N = N_G(S)$. Since $n_{11}(G) = 12 = [G : N]$, we have $|N| = 2 \times 3^2 \times 11$. Let $C = C_G(S)$. As the centraliser of a subgroup is normal in the normaliser of it, we get that N/C is isomorphic to a subgroup of $\mathcal{A}(S)$. Since $S \equiv Z_{11}$, then $\mathrm{Aut}(S) \equiv Z_{10}$. So N/C is isomorphic to a subgroup of Z_{10}. This means $[N : C] \,|10$ and $\mathrm{GCD}([N : C], 3) = 1$. and $3^2||C|$. Let $P \in Syl_3(C)$. Then $|P| = 3^2$. Since G is simple, then $H = N_G(p) < G$. □

Lecture 09 *24 Sep 24, Tue*

2 Semidirect Product

Propositions 1 (Number of Representations)**.** *Let H and K be subgroups of a group G. The number of distinct ways of writing any given element in HK in the form hk, where h is in H and k is in K, is $|H \cap K.|$.*

Direct Product Suppose H and K are groups embedded in $H \times K$ in the standard way

$$H \to H \times K \qquad h \mapsto (h, 1)$$

and

$$K \to H \times K \qquad k \mapsto (1, k).$$

1 in the first, respectively second, coordinate represents the identity in H, respectively K. Then the following properties hold

1. $H \times 1$ and $1 \times K$ generate $H \times K$. For (h, k) in $H \cap K$, we have $(h, k) = (h, 1)(1, k)$.
2. $(H \times 1) \cap (1 \times K) = \{(1, 1)\}$.
3. Commutativty:
$$(h, 1)(1, k) = (1, k)(h, 1).$$

Theorem 8 (Direct Product Recognition)**.** *Let G be a group with subgroups H and K, where*

1. *$G = HK$.*
2. *$H \cap K = \{1\}$.*
3. *H lies in the centre of K, or, equivalently, K lies in the centre of H.*

Then the map $H \times K \to G$ defined by $(h, k) \mapsto hk$ is an isomorphism. In other words, G is the direct product of H and K.

Example 2. *Let I be an m-subset of $\{1, 2, \ldots, m\}$ and let G be the setwise stabiliser of I in S_n,*

$$G = \{\sigma \in S_n \mid \mid \sigma(I) = I\}.$$

Write $J = \{1, 2, \ldots, n\} \setminus I$. G is also the setwise stabiliser of J. Suppose

$$H = \{\sigma \in G \mid \sigma(i) = i, \quad \forall i \in I\}$$

and

$$K = \{\sigma \in G \mid \sigma(i) = i, \quad \forall i \in J\}.$$

be the pointwise stabiliser of H. We know that $H \triangleleft G$ and $K \triangleleft G$. Moreover, $H \cap K = \{1_G\}$. Then $HK \cong H \times K$. Let $h \in H$ and $k \in K$. We want to prove that $hk = kh$. We have $h \in Sym(\{1, 2, \ldots, n\} \setminus I) = Sym(J)$ and $k \in Sym(\{1, 2, \ldots, n\} \setminus J) = Sym(I)$. For each σ in G stabilising I and J, we can write $\sigma = \sigma_I \sigma_J$, where $\sigma_I \in Sym(J), \sigma_J \in Sym(I)$.

Example 3. *Let $G = S_n$ and $n \geq 3$. Let $H = A_n$ and $K = \langle (1\ 2) \rangle$. We have $H \triangleleft G, K \leq G$ and $H \cap K = \{1_G\}$. However as we know that H is not normal in G, we realise that G is not the direct product of H and K.*

Semidirect product Let H and K be subgroups of G. Suppose $H \triangleleft G$, then $HK \leq G$. For hk and $h'k'$ in hk, we have

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

which is in HK because khk^{-1} is in H. Also, $(hk)^{-1} = k^{-1}h^{-1} = k^{-1}h^{-1}kk^{-1}$. K acts on H via conjugaction. Since $H \triangleleft G$, this conjugation is an automorphism of K on H.

Consider two groups H and K not necessarily related. Suppose there is a group homomorphism $\phi \colon K \to \mathrm{Aut}(H)$ is an action of K on H via ϕ. $\phi_k \mapsto \phi_k \in \mathrm{Aut}(H)$. Since ϕ is a group homomorphism, $\phi_{k_1} \circ \phi_{k_2} = \phi_{k_1 k_2}$ and $\phi_k^{-1} = \phi_{k^{-1}}$.

Definition 3 (Semidirect Product)**.** *For two groups H nad K and an action (a group homomorphism) $\phi \colon K \to \mathrm{Aut}(H)$. The corresponding semidirect product $H \rtimes_\phi K$ is defined as follows*

1. *as a set $H \rtimes_\phi k = \{(hk) \mid h \in H, k \in K\}$*
2. *operation $(h,k)(h',k') = (h\phi_k(h')kk')$*

If $H, K \leq G$ and $\phi_k(h') = kh'k^{-1}$. To show that $H \rtimes_\phi K$ is a subgroup, we need to verifiy that the operation is closed, $(1_H, 1_K)$ is the identity, the inverse of h, k is $(\phi_{k^{-1}}(h^{-1}), k^{-1})$ and the operation is associative.

Example 4. *Let $H = \{\pm 1\}$ be a multiplicative group of two elements acting on $\mathbb{Z}$, the additive group of all integers by automorphisms. Then there is a homomorphism $\phi \colon \{\pm 1\} \mapsto \mathrm{Aut}(\mathbb{Z})$. We write $\phi(1) = \phi_1$) where $\phi_1(n) = n$ for all n in $\mathbb{Z}$ and $\phi(-1) = \phi_{-1}$ where $\phi_{-1}(n) = -n$ for all n in $\mathbb{Z}$. Then the semidirect product $\mathbb{Z} \rtimes_\phi \{\pm 1\}$ with operatiions defined as*

$$(a, \epsilon)(a', \epsilon') = (1 + \phi_\epsilon(a'), \epsilon\epsilon') = (a + \epsilon a', \epsilon\epsilon')$$

where the operation in the first coordinate is addition in $\mathbb{Z}$ and in the second coordinate is multiplication.

Moreover for any group homomorphism $\Theta \colon \mathbb{Z} \to \mathrm{Z}$ given by $\Theta_n \in \mathrm{Aut}(\mathbb{Z})$, the semidirect product $\mathbb{Z} \rtimes_\Theta \mathbb{Z}$ with operation

$$(n, m)(n', m') = (n + \Theta_m(n'), m + m') = (n + (-1)^m n', m + m').$$

The relation between HK and $\rtimes_\phi K$.

Theorem 9 (Constructing Semidirect Products)**.** *Inside $H \rtimes_\phi K$, we have*

$$H \equiv H \times 1 = \{(h, 1) \mid h \in H\}$$

by $h \mapsto (h,1)$ *and*

$$K \equiv 1 \times K = \{(1,k) \mid k \in K\}$$

for each $h \in H$ *and* $k \in K$

$$(h,k) = (h,1)(1,k) = (1,k)(\phi^{-1}(h),1).$$

$H \rtimes_\phi K$ *is generated by* $H \times 1$ *and* $1 \times K$. $H \times 1$ *is a normal subgroup of* $H \rtimes_\phi K$ *with conjugation*

$$(1,k)(h,1)(1,k)^{-1} = (\phi_k(h),1) \in H \times 1.$$

In particular, for every h *in* H *and* k *in* K, $(h,1)$ *and* $(1,k)$ *commutative iff* $\phi\colon K \to \mathrm{Aut}(H)$ *is the trivial action where* $\phi_k = \phi(k)$ *is the identity mapping for each* k *in* K.

Lecture - 11 *26 Sep 2024*

Firs Mid Term Exam on 03 Oct 24, Thu. 05 questions will be asked and the test will be for 75 minutes. Syllabus will include Group Actions, Sylow Theorems, Semidirect product.

Relationship between action and automorphisms.

We ask when a semidirect product is a direct product.

$H \rtimes K = H \times K$ iff ϕ is trivial iff $\phi_k = \mathrm{id}_H$ for each $k \in K$ iff $1 \times K \triangleleft H \rtimes_\phi K$.

Theorem 10. *In* $H \rtimes_\phi K$, *the subgroup* $1 \times K \triangleleft H \rtimes_\phi K$ *iff* $\phi\colon K \to \mathrm{Aut}(H)$ *is trivial.*

Proof. Recall that $H \rtimes_\phi K$ is generated by $H \times 1$ and $1 \times K$. Also, $1 \times K$ is normal in $H \rtimes_\phi$ iff $(h,1)(1,k)(h^{-1},1)^{-1}$ is in $t \times K$ for all $hinH$ and $kinK$. Namely, $(h,k)(h^{-1},k) = (h\phi_k(h^{-1}),k)$ is in $1 \times K$. The latter is possible if and only if $h\phi_k(h^{-1}) = 1$, that is $\phi_k(h) = h$ for each h in H and k in K. That means, $\phi_k = \mathrm{id}_H$ for each k in K. □

Example 5 (Affine transformations as a semidirect product)**.** *Let* $H = (\mathbb{R},+), K = (\mathbb{R}^*,\cdot)$ *and* $\phi\colon \mathbb{R}^* \to \mathrm{Aut}(\mathbb{R})$ *defiend by* $\phi(x) = \phi_x$ *where* $\phi_x(y) = xy$ *for all* y *in* $\mathbb{R}$. *Then* $\mathbb{R} \rtimes_\phi \mathbb{R}$ *has operation* $(a,b)(a',b') =)a + \phi_b(a'), bb') = (a + ba', bb')$. *We have*

$$\mathbb{R} \rtimes_\phi \mathbb{R} \equiv \mathrm{Aff}(\mathbb{R}) = \left\{ \begin{pmatrix} b & a \\ 0 & 1 \end{pmatrix} \ : \ a \in \mathbb{R}, b \in \mathbb{R}^* \right\}.$$

Theorem 11 (Semidirect Product Recognition)**.** *Let* G *be a group with subgroups* H *and* K *satisfying*

1. $G = HK$,
2. $H \cap K = \{1_G\}$
3. $H \triangleleft G$.

THEN WHAT???

Let $\phi\colon K \operatorname{Aut}(H)$ be defind where ϕ_k acts on H by conjugation for each k in K with $\phi(k)(h) = kh^{-1}k$ for h in H. Then ϕ is a group homomorphism and the mapping $f\colon H \rtimes_\phi K \to G$ with $f(h,k) = hk$ is an isomorphism. To check that ϕ is a homomorphism, we take x, y in K and check that

$$\phi_{xy}(h) = yxhx^{-1}y^{-1} = \phi_y(xhx^{-1}) = \phi_y(\phi_x(h)) = \phi_y \circ \phi_x(h)$$

for any h in H. Given, h, h' in H and k, k' in K, we check that f is a homomorphism:

$$f((h,k)(h',k')) = f(h\phi_k(h'), kk') = h\phi_k(h')kk' = hkhk^{-1}kk' = hkh'k'.$$

Example 6 (Permutation group S_n as a semidirect product)**.** *Let $H = S_n, G = S_n$ for some integer $n \geq 3$, and $K = \langle (1,2) \rangle$. We have $G = H \cup H(1,2) = HK$, $H \cap K = \{1_G\} = \{\mathrm{id}\}$, $H \lhd G$ because it has index 2. We can then express $G = H \rtimes_\phi K$, where $\phi_k(h) = khk^{-1}$.*

Example 7. *In $G = S_4$, with $|G| = 24 = 2^3 \times 3$, $H \in Syl_2(G)$, $K \in Syl_3(G)$. Then H has order 8 and some elements of order 2 and 4. So $H \equiv D_4$, $K \equiv Z_3$. G is not a semidirect product of H and K. We have $G = HK$ and $H \cap K = \{1_G\}$ but $H \not\lhd G$ and $K \not\lhd G$.*

Example 8 (Groups of order pq)**.** *We know that if G is a group of order p, q where p, q are prime integers and $p < q$, then either G is abelian with $G \equiv \mathbb{Z}_{pq}$ or G is not abelian and $p|q-1$. As $q > p$, there exists an element b of order q WHY????? So, there is a group $\langle b \rangle$ of order q. This group is normal because if $a^{-1} \langle b \rangle a \neq \langle b \rangle$ for some a in g, then the product of these groups has order q^2 and is contained in G. As this is not possible, we get that $\langle b \rangle \lhd G$. Thus $b^{-1}ab = a^d$ for some positive integer d. Then, we have $a = b^{-p}ab^p = a^{d^p}$ implying that $e = a^{d^p - 1}$*

Let $P \in Syl_p(G)$ and $Q \in Syl_q(G)$. We know that $Q \lhd G$ because WHY???? Then $G = PQ$ and $P \cap Q = \{1_G\}$. So that $G = Q \rtimes_\phi P$ for some group homomorphism $\phi\colon P \to \operatorname{Aut}(Q)$. The automorphism group of a cyclic group of order n is a cyclic group of order REALLY??? equal to the number of integers coprime to and less than n. So, $|\operatorname{Aut}(Q)| = q - 1$. If $p \not| q-1$, then $|\phi(P)| = 1$ and so G is abelian. This is because of the fact that $\phi(P) \leq \operatorname{Aut}(Q)$ implies that $|\phi| = \frac{|P|}{|\ker(\phi)|}$ is either 1 or p. If $p|q-1$, let $P = \langle y \rangle$ and $\langle \gamma \rangle$ be the unique order p subgroup of $\operatorname{Aut}(Q)$ and $\phi\colon P \to \operatorname{Aut}(Q)$ defined by $\phi(y) = r$. We have $\phi(P) = \langle \gamma \rangle$ for some γ in $\operatorname{Aut}(Q)$ because the latter is a cyclic group. If $1 \leq i \leq p-1, G = \ltimes_\phi Q$.

Lecture - 11 *01 Oct 24, Tue*

Today we will discuss the Schur Zassenhaus Theorem. Suppose N is a normal subgroup of G. Can we construct G from N and G/N? Say $G \equiv \mathbb{Z}_{p^2}$, and $N \lhd G$, with $N \equiv \mathbb{Z}_p$. Then $G/n \equiv \mathbb{Z}_p$, and constructing G from N and G/N is not straightforward.

Definition 4 (Complement)**.** *Let G be a group and $N \lhd G$. We say that a subgroup H of G is complement of N if $G = N \rtimes H$.*

Not every normal subgroup has a complement. For instance, $G = S_4$ has a normal subroup $H \equiv D_4$ which is the unique Sylow 2-subgroup. The unique REALLY??? Sylow 3-subgroup C_3 is not complement to D_4.

Definition 5 (Hall Subgroup)**.** *A subgroup H of a finite group G is a Hall subgroup if $(|H|, [G : H]) = 1$.*

For example, every Sylow p-subgroup is a Hall subgroup.

Theorem 12 (Schur Zassenhaus)**.** *Any normal Hall subgroup H of a finite group G has a complement and all the complements are conjugate in G.*

Example 9. *Let p be an odd prime and G be a group of order $2p$. There exists a subgroup H of G of order p. H is normal in G and also $(|H|, [G : H]) = 1$ so H is a Hall subgroup of G. Fill in the details. why are all elements of order 2 conjugate to each other?*

Lemma 4 (Frattini argument)**.** *Let G be a finite group, $N \triangleleft G$, and P be a Sylow p-subgroup of N. Then, $G = N_G(P)N$.*

Proof. Let g be in G. Then $g^{-1}Pg \leq g^{-1}Ng = N$. So, the action of G on $Syl_p(N)$ via conjugation is well-defined. This is because P is conjugate to each Sylow p-subgroup of N by Sylow Conjugacy Theorem. For each g in G, $g^{-1}Pg$ is in $Syl_p(N)$, so there exists n in N such that $n^{-1}g^{-1}Pgn = P$. Then gn is in $N_G(P)$. So $g \in N_G(P)n^{-1} \subseteq N_G(P)N$. Thus $G \subseteq N_G(P)N$. This proves the required equality. □

Proof of Schur Zassenhaus Theorem. Let N be a normal Hall subgroup of a finite group G with $n = [G : N]$. This means $\text{GCD}(|N|, n) = 1$. For this GCD to be well defined, G has to be finite.

Step 1 It suffices to show that G has a subgroup K of order n.

Note that $NK = \frac{|N||K|}{|N \cap K|} = |N||K| = |G|$ because $N \cap K = \{1_G\}$ because the order of this group divides the order of N as well as of K. By recognition of semidirect product theorem, we know that $G = N \rtimes K$.

We proceed to prove by induction. The induction hypothesis is that for each groupwith order less than $|G|$, which has a normal Hall subgroup H' also has a subgroup with order equal to the index of H'.

Step 2 Let P be a Sylow subgroup of N. We can assume that P is normal in G, for otherwise, we can find a subgroup in G of order n.

By Frattini argument, $G = N_G(P)N$. Observe that $N_N(P) = N_G(P) \cap N$ is a normal subgroup of $N_G(P)$ because N is normal in G. So we can apply the Second Isomorphism Theorem to conclude that

$$\frac{G}{N} \cong \frac{N_G(P)N}{N} \cong \frac{N_G(P)}{N_G(P) \cap N} = \frac{N_G(P)}{N_N(P)}$$

Thus $n = [G : N] = [N_G(P) : N_N(P)]$. If $N_G(P) < G$, that is $P \not\lhd G$, then we shall apply the induction hypothesis to $N_G(P)$. We know that $N_N(P) \triangleleft N_G(P)$ and it is also a Hall subgroup of G because $|N_N(P)| \,|\, |N|$ by Lagrange's Theorem.

We know $[N_G(P) : N_N(P)] = n$ and $GCD(|N|, n) = 1$ so GCD$(|N_N(P)|, n) = 1$. Thus, applying the induction hypothesis, we get that $N_G(P)$ contains a subgroup of order $[N_G(P) : N_N(P)] = n$. Thus G contains a subgroup of order n.

Step 3 Proceeding with the case that P is normal in G, we now show that we can assume that $N = P$.

If $P < N$, then $N/P \triangleleft G/P$ and $[G/P : N/P] = [G : N] = n$, by correspondence theorem and GCD$(|N/P|, n) = 1$ because GCD$(|N|, n) = 1$. So we now get that N/P is a normal Hall subgroup of G/P. By Correspondence Theorem, this group must be of the form L/P where L is some subgroup of G containing P. If we can show that $L < G$, then we can find a subgroup of G of order n by applyign the induction hypothesis to L. To show this, consider $L \cap N$. Its order divides $|N|$ as well as $|L| = n|P|$. As GCD$(n, |N|) = 1$, we get that $|L \cap N|$ divides $|P|$. So $|L \cap N| \leq |P|$. On the other hand, we have $|P| \leq |L \cap N|$ because P is contained in L as well as N. So, $P = L \cap N$.

If $P < N$, then there exists x in $N \setminus P$. So x is in N but not in L. This shows that $L < G$.

An alternative way to view this is to realise that if P is not N, then there is an element xP in N/P which is not P. As $o(xP)$ would divide $|N/P|$ and GCD$(|N/P|, |L/P|)$, we get that xP is not in L/P. So, we get that $L < G$.

For the next step, we assume that $N = P$ in addition to the assumption that $N \triangleleft G$.

Step 4 We assume for this case that N is not abelian and prove that in this case there exists a subgroup of order n in G.

Let N be non abelian and denote its center as $Z = Z(N)$. So, $1 \leq Z \triangleleft N$. Since Z is a characteristic subgroup of N and $N \triangleleft G$, we have $Z \triangleleft G$. Observing that $N/Z \triangleleft G/Z$, and $[G/Z : N/Z] = [G : N] = n$, we apply the induction hypothesis to G/Z whose order is less than $|G|$ because the centre of N is nontrivial. So, G/Z has a subgroup J/Z of order n.

We show that $J < G$ and then use the induction hypothesis to conclude that there is a subgroup of order n contained in J and thus in G. As GCD$(|J/Z|, |N/Z|) = 1$, we get that $(J \cap N)/Z = J/Z \cap N/Z$ is the trivial subgroup of G/Z. So, $J \cap N = Z$. There exists x in $N \setminus Z$ because N is not abelian. We get that x is in N and thus in G but not in J because x is not in $Z = J \cap N$.

WHY IS THE CENTER NONTRIVIAL? □

Corollary 4. *Fix a prime integer p. For a finite group G with order divisible by p, the following statements are equivalent*

1. $|\mathrm{Aut}(G)|$ *is not divisible by p.*
2. $G \cong \mathbb{Z}_p \times H$, *where p does not divide $|H|$ or $|\mathrm{Aut}(H)|$.*

Proof. (2 $\implies$ 1) For G, as given, we have $\mathrm{Aut}(G) \cong \mathrm{Aut}(\mathbb{Z}_p) \times \mathrm{Aut}(H) \cong \mathbb{Z}_p^* \times \mathrm{Aut}(H)$. As p does not divide $|\mathbb{Z}_p^*| = p - 1$, we see that p does not divide $\mathrm{Aut}(H)$.

(1 $\implies$ 2) Let $P \in Syl_p(G)$, we aim to show that $G = P \times H$. □

Lecture - 13 *08 Oct 24, Tue*

So far we studied some general properties about groups such as group actions, Sylow p-subgroups and the Schur-Zassenhauss Theorem. We will now switch to some concrete groups, the general linear groups. These are the source of many combinatorial concepts.

Let $\mathbb{F}$ be a field and n be a positive integer. Denote the set fo all $n \times n$ matrices over $\mathbb{F}$ by $M_n(\mathbb{F}$.

Definition 6 (General Linear Group)**.** *The egneral linear group $GL(n, \mathbb{F})$ consists of all invertible matrices in $M_n(\mathbb{F})$ with matric multiplication as teh group operation.*

Our goal is to decompose $GL(n, \mathbb{F})$. To do this we will study the action of this group on some combinatorial objects.

Remark 2. *Given an n-dimensional space V over $\mathbb{F}$ the general linear group $GL(V)$ is defined as the group of all invertible linear transformations of V with composition of mapping as the group operation.*

Unless mentioned otherwise, p, q denote positive prime integers and G may be considered to be $GL(n, p)$.

From our knowledge of linear algebra, we know that $GL(n, \mathbb{F}) \cong GL(V)$.

If $\mathbb{F}$ is a finite field, then its order must be of the form q^n where q is some prime number and n is some positive integer. In particular, if $n = 1$, then we shall write $GL(n, \mathbb{F})$ as $GL(n, q)$.

Propositions 2 (General linear group as automorphism gruop)**.** *Let E be an elementary abelian p-group with $|E| = p^n$. Then* $\mathrm{Aut}(E) \cong GL(n, p)$.

An *Elementary abelian p-group* E of order p^n is isomorphic to $\Pi_{i=1}^{n} \mathbb{Z}_p = \mathbb{Z}_p \times \mathbb{Z} \times \cdots \times \mathbb{Z}_p$.

Proof. Let $\mathbb{F}$ be a field of order p. Then, E can be regarded as an $n$nobreakdash-dimensional vector space over $\mathbb{F}$. Then every element in $\mathrm{Aut}(E)$ is an invertible linear transformation on E. □

Propositions 3 (order of $GL(n, q)$)**.** *The order of $G = GL(n, q)$ is*

$$\Pi_{k=0}^{n-1}(q^n - q^k) = q^{\frac{n(n-1)}{2}} \Pi_{k=1} n(q^k - 1).$$

Proof. We count the number of elements in G. The first row can be any element of $\mathbb{Z}_p^n$ but the zero element. There are q^n many choices for this. The second row can be any element except the q multiples of the first row. In general, the $k+1^{\text{th}}$ row can be any element of $\mathbb{Z}_q^p$ except one of the q^k linear combinations of the previous k rows. So the total number of choices here is $\Pi_{k=0}^{n-1}(q^n - q^k)$. □

Definition 7 (Borel Subgroup)**.** *The set B consisting of all invertible upper triangular matrices is a subgroup of $G = GL(n, \mathbb{F})$ is called the* Standar Borel Subgroup. *A Borel Subgroup is any conjugate of the Standard Borel Subgorup.*

Example 10 (Permutation matrix)**.** *Any matrix having exactly one nonzero entry in each row and each column, equal to 1 is called a* Permutation matrix. *For instance, let*

$$W = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$

and $\{v_1, v_2, v_3, v_4\}$ *be the standard ordered basis of* $\mathbb{F}^4$*. Then* $Wv_1 = v_3, Wv_2 = v_4, Wv_3 = v_1$ *and* $Wv_4 = v_2$*. Thus* W *defines a permutation* ϕ *on* $\{1, 2, 3, 4\}$ *given by* $\phi(i) = j$ *if and only if* $Wv_i = v_j$*.*

Notation 1. *If* W *sends* v_i *to* v_j*, then we write* $w(i) = j$*.*

Propositions 4 (The Weyl Group)**.** *the set* W *consisting of all permutation matrices is a subgroup of* G *called The Weyl Group.*

Proof. The permutation matrices are closed under multiplication and the inverse of W in The Weyl Group is W^T. □

Propositions 5 (Weyl Group and Symmetric Group)**.** *Let* V *be an* n*-vector space over* $\mathbb{F}$ *with standard basis* $\{v_1, v_2, \ldots v_n\}$*. The action of* W*, The Weyl Subgroup in* $GL(n, \mathbb{F})$*, on* $\{v_1, v_2, \ldots, v_n\}$ *is equivalent to the action of* S_n *on* $\{1, 2, \ldots, n\}$

We will now explore the *Bruhat Decomposition* of G

Definition 8 (Transvection)**.** *Let* $1 \leq i, j \leq n$ *be distinct and* α *in* $\mathbb{F}$*.Define* $X_{ij}(\alpha)$ *to be the matrix*

$$\begin{pmatrix} 1 & 0 & \cdots & & & & \\ & 1 & \cdots & & & & \\ \vdots & \cdots & \vdots & & \vdots & \vdots & \vdots \\ & & \cdots & 1 & & \alpha & \\ & & \cdots & & & & \end{pmatrix}.$$