

1. Lecture 4

By Lagrange's theorem, we know that if H is a subgroup of a finite group G , then $|H|$ divides $|G|$. We will investigate the extent to which the converse holds: if d divides $|G|$, must G contain a subgroup of order d ? Sylow's first theorem gives an affirmative answer when d is a power of a prime. Sylow's theorems are proved based on the generalized class formula for groups whose order is power of a prime.

THEOREM 1. *Suppose p is a prime, P is a non-trivial group of order p^n , X is a finite set, and $P \curvearrowright X$. Then*

$$|X| \equiv |X^P| \pmod{p}.$$

PROOF. By the generalized class equation,

$$(1) \quad |X| = |X^P| + \sum_{P \cdot x \in X \setminus X^P} [P : P_x].$$

For $x \in X \setminus X^P$, P_x is a proper subgroup of P . Hence, $[P : P_x]$ is a divisor of p^n larger than 1. Thus, $[P : P_x] \stackrel{p}{\equiv} 0$ for all $x \in X \setminus X^P$. Therefore, by (1), it follows that

$$|X| \stackrel{p}{\equiv} |X^P|.$$

This completes the proof. □

Sometimes the above congruence is used to show the existence of a P -fixed point. An interesting example is Zagier's proof of Fermat's theorem.

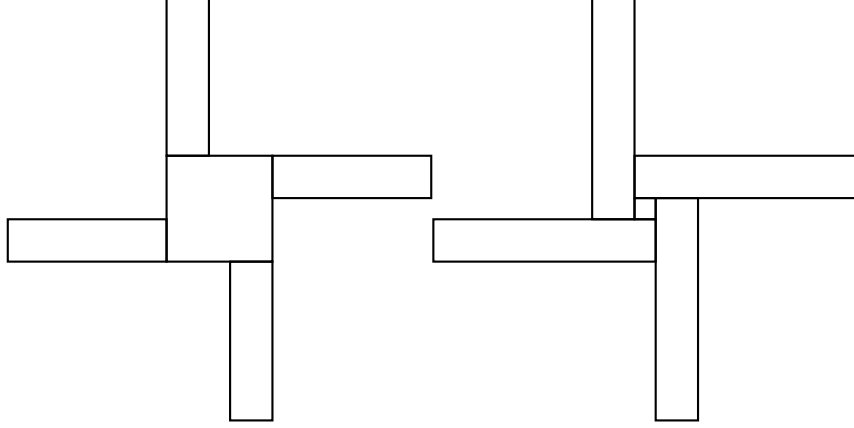
Recall that Fermat's theorem states that if p is a prime of the form $4k + 1$, then there exist $a, b \in \mathbb{Z}$ such that $p = a^2 + b^2$. A common technique in algebra and number theory is to transform a polynomial into a multilinear function by introducing new variables. Zagier begins with a partial application of this idea and considers the equation $p = x^2 + 4yz$:

$$X := \{(x, y, z) \in \mathbb{Z}^3 \mid p = x^2 + 4yz\}.$$

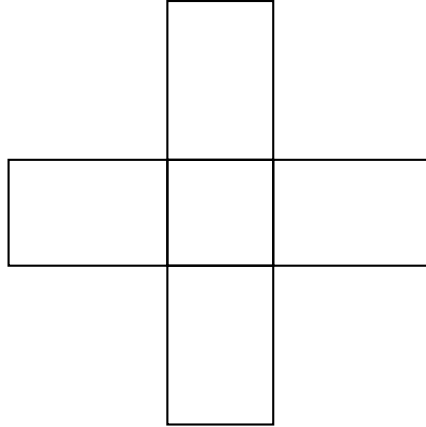
Note that $(1, k, 1) \in X$. Another observation is that

$$\tau : X \rightarrow X, \tau(x, y, z) := (x, z, y)$$

is a well-defined bijection of order 2. If we can show that $|X|$ is odd, then $X^{(\tau)}$ is not empty, which implies that there exist $(x, y, y) \in X$. It follows that $p = x^2 + 4y^2$ for some $x, y \in \mathbb{Z}$, which implies Fermat's theorem.



To show $|X|$ is odd, we consider another order 2 symmetry of X that can be visualized using “windmills”: an x -by- x square core, and four blades that are y -by- z . The only “windmills” that do not admit two different partitioning as above are of the form:



This means either $x = y$ or $x = z$. Since p is prime and $p = x^2 + 4xz$, we deduce that $x = 1$. Hence, the second symmetry has only one fixed point, which implies that $|X|$ is odd. This completes the proof.

THEOREM 2 (Cauchy's theorem). *Suppose G is a finite group and p is a prime factor of the order of G . Let*

$$f_p(G) := |\{g \in G \mid \text{ord}(g) = p\}|.$$

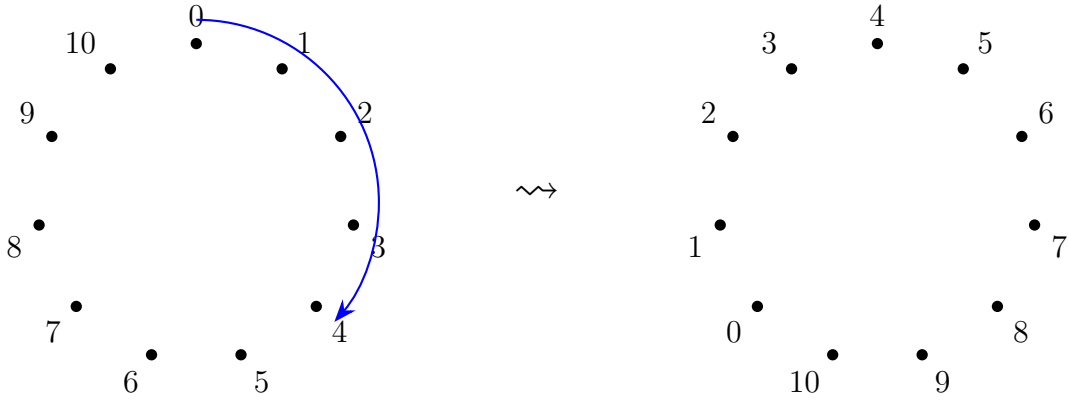
Then $f_p(G) \stackrel{p}{\equiv} -1$. In particular, $f_p(G) \neq 0$, which means G has an element of order p .

PROOF. Since p is prime, $\text{ord}(g) = p$ if and only if $g \neq 1$ and $g^p = 1$. A common trick for investigating solutions to a higher degree equation is to study a multilinear version of the equation instead (similar to Zagier's trick!). Thus, rather than the equation $g^p = 1$, we study the equation $g_0 \cdots g_{p-1} = 1$. Let

$$X := \{(g_0, \dots, g_{p-1}) \in G^p \mid g_0 \cdots g_{p-1} = 1\}.$$

Note that $\mathbb{Z}/p\mathbb{Z} \curvearrowright G^p$ via

$$n \cdot (g_0, \dots, g_{p-1}) := (g_n, \dots, g_{p-1}, g_0, \dots, g_{n-1}).$$



Next, we observe that X is G -invariant. If $\mathbf{g} := (g_0, \dots, g_{p-1}) \in X$, then for every $n \in \mathbb{Z}/p\mathbb{Z}$,

$$(g_0 \cdots g_{n-1})(g_n \cdots g_{p-1}) = 1.$$

This implies

$$(g_n \cdots g_{p-1})(g_0 \cdots g_{n-1}) = 1,$$

which means

$$n \cdot \mathbf{g} \in X.$$

Altogether, we deduce that $\mathbb{Z}/p\mathbb{Z} \curvearrowright X$. Hence, by Theorem 1,

$$(2) \quad |X| \stackrel{p}{\equiv} |X^{\mathbb{Z}/p\mathbb{Z}}|.$$

Note that

$$(3) \quad X^{\mathbb{Z}/p\mathbb{Z}} = \{(g, \dots, g) \in G^p \mid g^p = 1\}.$$

By (3), it follows that

$$(4) \quad |X^{\mathbb{Z}/p\mathbb{Z}}| = f_p(G) + 1$$

as $(1, \dots, 1) \in X^{\mathbb{Z}/p\mathbb{Z}}$ and other elements of $X^{\mathbb{Z}/p\mathbb{Z}}$ are in bijection with elements of order p in G .

We also observe that

$$(g_0, \dots, g_{p-1}) \in X \quad \text{if and only if} \quad g_{p-1} = (g_0 \cdots g_{p-2})^{-1}.$$

Therefore, $|X| = |G|^{p-1}$. As $p \mid |G|$, we deduce that $p \mid |X|$. Thus, by (2) and (4), we deduce

$$f_p(G) + 1 \stackrel{p}{\equiv} 0,$$

which completes the proof. $\square$

For a prime p , a group G is called a p -group if the order of every element of G is a power of p .

COROLLARY 3. *Suppose p is prime. Then a finite group G is a p -group if and only if $|G| = p^n$ for some non-negative integer n .*

PROOF. ($\Leftarrow$) Follows from Lagrange's theorem.

($\Rightarrow$) Suppose to the contrary that the order of G has a prime factor q distinct from p . Then by Cauchy's theorem, G has an element of order q , which is a contradiction. $\square$

The following theorem plays an important role in investigating finite groups.

THEOREM 4. *Suppose p is prime, G is a finite group, and P is a p -subgroup of G . Then*

$$[G : P] \stackrel{p}{\equiv} [N_G(P) : P].$$

In particular, the following statements hold.

- (1) *If $p \mid [G : P]$, then $p \mid [N_G(P) : P]$.*
- (2) *If $p \nmid [G : P]$, then $[G : N_G(P)] \stackrel{p}{\equiv} 1$.*

PROOF. Consider the left-translation action $P \curvearrowright G/P$. By Theorem 1,

$$|G/P| \stackrel{p}{\equiv} |(G/P)^P|.$$

What can we say about $(G/P)^P$?

$$\begin{aligned}
 xP \in (G/P)^P &\iff \forall g \in P, gxP = xP \\
 &\iff \forall g \in P, x^{-1}gx \in P \\
 &\iff xPx^{-1} \subseteq P \quad (\text{since } |xPx^{-1}| = |P|) \\
 &\iff xPx^{-1} = P \iff x \in N_G(P).
 \end{aligned}$$

Hence,

$$(G/P)^P = N_G(P)/P.$$

Therefore,

$$(5) \quad |N_G(P)/P| \stackrel{p}{\equiv} |G/P|.$$

If $p \nmid [G : P]$, then by (5), $p \nmid [N_G(P) : P]$.

Suppose $p \nmid [G : P]$. Since $[G : P] = [G : N_G(P)][N_G(P) : P]$, we deduce that $\gcd(p, [N_G(P) : P]) = 1$. Thus,

$$[G : N_G(P)][N_G(P) : P] \stackrel{p}{\equiv} [N_G(P) : P] \quad \text{implies} \quad [G : N_G(P)] \stackrel{p}{\equiv} 1.$$

This completes the proof. $\square$

THEOREM 5 (Sylow's first theorem). *Suppose $p^n \mid |G|$. Then there exist*

$$P_1 \subseteq P_2 \subseteq \cdots \subseteq P_n$$

such that P_i is a subgroup of G and $|P_i| = p^i$ for all i . Moreover, P_i is normal in P_{i+1} .

PROOF. We proceed by induction on n .

Base case. By Cauchy's theorem, G has an element g of order p . This means $P_1 := \langle g \rangle$ is a subgroup of order p .

Induction step. Suppose $p^{n+1} \mid |G|$. By the induction hypothesis, there exist

$$P_1 \subseteq P_2 \subseteq \cdots \subseteq P_n$$

that are subgroups of G and $|P_i| = p^i$ for $i = 1..n$. Since $p^{n+1} \mid |G|$ and $|P_n| = p^n$, we have $p \mid [G : P_n]$. By Theorem 4, $p \mid [N_G(P_n) : P_n]$. Note that P_n is a normal subgroup of $N_G(P_n)$. Hence, $N_G(P_n)/P_n$ is a group and its order is divisible by p . Thus, by Cauchy's theorem (or the base case), $N_G(P_n)/P_n$ has a subgroup

$\overline{P}_{n+1}$ of order p . By the correspondence theorem, there exists a subgroup P_{n+1} of $N_G(P_n)$ such that

$$P_n \subseteq P_{n+1} \quad \text{and} \quad P_{n+1}/P_n = \overline{P}_{n+1}.$$

Hence, $|P_{n+1}| = |P_n||\overline{P}_{n+1}| = p^{n+1}$. Note that $P_{n+1} \subseteq N_G(P_n)$ and $P_n \subseteq P_{n+1}$ implies that P_n is a normal subgroup of P_{n+1} . This completes the proof. $\square$

(Let us recall the **correspondence theorem**. Suppose N is a normal subgroup of G . Then the following maps are mutual inverse of each other:

$$\begin{aligned} \text{Sub}(G/N) &\rightarrow \{H \in \text{Sub}(G) \mid N \subseteq H\}, \quad \overline{H} \mapsto \pi^{-1}(\overline{H}) \\ \{H \in \text{Sub}(G) \mid N \subseteq H\} &\rightarrow \text{Sub}(G/N), \quad H \mapsto H/N, \end{aligned}$$

where $\pi : G \rightarrow G/N$ is the natural quotient map.)

DEFINITION 6. A subgroup P of a finite group G is called a Sylow p -subgroup if P is a p -group and $p \nmid [G : P]$. The set of all Sylow p -subgroups of G is denoted by $\text{Syl}_p(G)$. The cardinality of $\text{Syl}_p(G)$ is denoted by $s_p(G)$, or simply s_p .

Note that if $\theta \in \text{Aut}(G)$ and $P \in \text{Syl}_p(G)$, then $|\theta(P)| = |P|$, which implies that $\theta(P)$ is a p -group and $p \nmid [G : \theta(P)]$. Hence, $\theta(P)$ is a Sylow p -subgroup of G . Therefore, $\text{Aut}(G) \curvearrowright \text{Syl}_p(G)$ via $\theta \cdot P := \theta(P)$. In particular, $G \curvearrowright \text{Syl}_p(G)$ via conjugation.

DEFINITION 7. An action $G \curvearrowright X$ is called transitive if $|G \backslash X| = 1$. This means X is a single G -orbit.

THEOREM 8 (Sylow's second theorem). Suppose $P_0 \in \text{Syl}_p(G)$.

- (1) For every p -subgroup P of G , there exists $x \in G$ such that $P \subseteq xP_0x^{-1}$.
- (2) All Sylow p -subgroups of G are conjugate of P_0 . Equivalently, the action $G \curvearrowright \text{Syl}_p(G)$ is transitive.

PROOF. (1) Consider the left-translation action $P \curvearrowright G/P_0$. Since P is a finite p -group, by Theorem 1,

$$(6) \quad |G/P_0| \stackrel{p}{\equiv} |(G/P_0)^P|.$$

Since $P_0 \in \text{Syl}_p(G)$, $p \nmid |G/P_0|$. Thus, by (6), $|(G/P_0)^P| \neq 0$. Suppose x is in $(G/P_0)^P$. Therefore,

$$\begin{aligned} \forall g \in P, gxP_0 = xP_0 &\iff \forall g \in P, x^{-1}gx \in P_0 \\ &\iff x^{-1}Px \subseteq P_0 \\ &\iff P \subseteq xP_0x^{-1}. \end{aligned}$$

(2) Suppose $P_1 \in \text{Syl}_p(G)$. Then, by Part (1), there exists $x \in G$ such that

$$(7) \quad P_1 \subseteq xP_0x^{-1}.$$

Since $P_0, P_1 \in \text{Syl}_p(G)$, it follows that $|P_1| = |P_0| = |xP_0x^{-1}|$. Thus, by (7), we deduce $P_1 = xP_0x^{-1}$. This completes the proof. $\square$

THEOREM 9 (Sylow's third theorem). $s_p(G) \stackrel{p}{\equiv} 1$.

PROOF. Suppose $P_0 \in \text{Syl}_p(G)$. By Sylow's second theorem, $\text{Syl}_p(G)$ consists of all the conjugates of P_0 . By the orbit-stabilizer theorem, the number of conjugates of P_0 is $[G : N_G(P_0)]$. Hence,

$$s_p(G) = [G : N_G(P_0)].$$

Since $P_0 \in \text{Syl}_p(G)$, P_0 is a p -subgroup and $p \nmid [G : P_0]$. Therefore, by Theorem 4,

$$[G : N_G(P_0)] \stackrel{p}{\equiv} 1.$$

Altogether, we deduce $s_p(G) \stackrel{p}{\equiv} 1$. This completes the proof. $\square$