Sylow's theorems

GU4041

Columbia University

April 23, 2020

Outline

1. Rough statement of the Sylow theorems
2. Some applications
   - Some examples
3. Proofs of the Sylow Theorems

Statement of the theorems

Let G be a finite group of order n. Let p be a prime that divides n, and suppose $p^r|n$ but p^{r+1} does not divide n; we often write $p^r||n$.

Theorem (Sylow theorems)

(1) *G contains a subgroup $H \subset G$ of order p^r. Any such group is called a* **Sylow p-subgroup**.

(2) *All Sylow p-subgroups of G are conjugate by elements of G. In particular, if G has only one Sylow p-subgroup H, then H is a* **normal** *subgroup of G.*

(3) *The number of distinct Sylow p-subgroups of G is (i) congruent to 1 modulo p and (ii) divides $|G|$.*

Statement of the theorems

Let G be a finite group of order n. Let p be a prime that divides n, and suppose $p^r|n$ but p^{r+1} does not divide n; we often write $p^r||n$.

Theorem (Sylow theorems)

(1) *G contains a subgroup $H \subset G$ of order p^r. Any such group is called a* **Sylow p-subgroup**.

(2) *All Sylow p-subgroups of G are conjugate by elements of G. In particular, if G has only one Sylow p-subgroup H, then H is a* **normal** *subgroup of G.*

(3) *The number of distinct Sylow p-subgroups of G is (i) congruent to 1 modulo p and (ii) divides $|G|$.*

Statement of the theorems

Let G be a finite group of order n. Let p be a prime that divides n, and suppose $p^r | n$ but p^{r+1} does not divide n; we often write $p^r || n$.

Theorem (Sylow theorems)

(1) *G contains a subgroup $H \subset G$ of order p^r. Any such group is called a* **Sylow p-subgroup**.

(2) *All Sylow p-subgroups of G are conjugate by elements of G. In particular, if G has only one Sylow p-subgroup H, then H is a* **normal** *subgroup of G.*

(3) *The number of distinct Sylow p-subgroups of G is (i) congruent to 1 modulo p and (ii) divides $|G|$.*

Statement of the theorems

Let G be a finite group of order n. Let p be a prime that divides n, and suppose $p^r|n$ but p^{r+1} does not divide n; we often write $p^r||n$.

Theorem (Sylow theorems)

(1) *G contains a subgroup $H \subset G$ of order p^r. Any such group is called a* **Sylow p-subgroup**.

(2) *All Sylow p-subgroups of G are conjugate by elements of G. In particular, if G has only one Sylow p-subgroup H, then H is a* **normal** *subgroup of G.*

(3) *The number of distinct Sylow p-subgroups of G is (i) congruent to 1 modulo p and (ii) divides $|G|$.*

Some applications

Example

Let G be a group of order $21 = 3 \cdot 7$ and let a be the number of its distinct Sylow 7-subgroups. By the Third Sylow Theorem $a \equiv 1 \pmod 7$ and a divides 21. The only divisor of 21 congruent to 1 modulo 7 is 1. So $a = 1$ and its unique Sylow 7-subgroup is normal.

More generally,

Proposition

Let G be a group of order pq, where p and q are distinct primes, $q > p$. Then G has a unique Sylow q-subgroup H and H is normal. Moreover H is cyclic and if p does not divide $q - 1$ then G is abelian.

Some applications

Example

Let G be a group of order $21 = 3 \cdot 7$ and let a be the number of its distinct Sylow 7-subgroups. By the Third Sylow Theorem $a \equiv 1 \pmod 7$ and a divides 21. The only divisor of 21 congruent to 1 modulo 7 is 1. So $a = 1$ and its unique Sylow 7-subgroup is normal.

More generally,

Proposition

Let G be a group of order pq, where p and q are distinct primes, $q > p$. Then G has a unique Sylow q-subgroup H and H is normal. Moreover H is cyclic and if p does not divide $q - 1$ then G is abelian.

Some applications

Example

Let G be a group of order $21 = 3 \cdot 7$ and let a be the number of its distinct Sylow 7-subgroups. By the Third Sylow Theorem $a \equiv 1 \pmod 7$ and a divides 21. The only divisor of 21 congruent to 1 modulo 7 is 1. So $a = 1$ and its unique Sylow 7-subgroup is normal.

More generally,

Proposition

Let G be a group of order pq, where p and q are distinct primes, $q > p$. Then G has a unique Sylow q-subgroup H and H is normal. Moreover H is cyclic and if p does not divide $q - 1$ then G is abelian.

Some applications

Example

Let G be a group of order $21 = 3 \cdot 7$ and let a be the number of its distinct Sylow 7-subgroups. By the Third Sylow Theorem $a \equiv 1 \pmod 7$ and a divides 21. The only divisor of 21 congruent to 1 modulo 7 is 1. So $a = 1$ and its unique Sylow 7-subgroup is normal.

More generally,

Proposition

Let G be a group of order pq, where p and q are distinct primes, $q > p$. Then G has a unique Sylow q-subgroup H and H is normal. Moreover H is cyclic and if p does not divide $q - 1$ then G is abelian.

Some applications

Proof.

If a is the number of Sylow q-subgroups of G, then a divides pq and $a \equiv 1 \pmod{q}$. The only divisors of pq are $1, p, q$, and pq, and of those only $1 \equiv 1 \pmod{q}$, because $p < q$.

By the Second Sylow Theorem, the unique Sylow q-subgroup H is normal. Since H is of order q it is abelian. Now consider the conjugation action of G on the normal subgroup H: it defines a homomorphism $c : G \to Aut(H) = \mathbb{Z}_q^{\times}$.

The image J is a divisor of $q-1$, but $J \xrightarrow{\sim} \frac{|G|}{|\ker c|}$ by the First Isomorphism Theorem. So $|J|$ divides $gcd(|G|, q-1) = gcd(pq, q-1) = gcd(p, q-1)$, since q is relatively prime to $q-1$. (Anyway, H is abelian, so its conjugation action on itself is trivial.) . Thus if p does not divide $q-1$, then $|J| = 1$, which means that G is abelian. □

Some applications

Proof.

If a is the number of Sylow q-subgroups of G, then a divides pq and $a \equiv 1 \pmod{q}$. The only divisors of pq are $1, p, q$, and pq, and of those only $1 \equiv 1 \pmod{q}$, because $p < q$.

By the Second Sylow Theorem, the unique Sylow q-subgroup H is normal. Since H is of order q it is abelian. Now consider the conjugation action of G on the normal subgroup H: it defines a homomorphism $c : G \to Aut(H) = \mathbb{Z}_q^{\times}$.

The image J is a divisor of $q - 1$, but $J \xrightarrow{\sim} \frac{|G|}{|\ker c|}$ by the First Isomorphism Theorem. So $|J|$ divides $gcd(|G|, q-1) = gcd(pq, q-1) = gcd(p, q-1)$, since q is relatively prime to $q - 1$. (Anyway, H is abelian, so its conjugation action on itself is trivial.) . Thus if p does not divide $q - 1$, then $|J| = 1$, which means that G is abelian. □

Some applications

Proof.

If a is the number of Sylow q-subgroups of G, then a divides pq and $a \equiv 1 \pmod{q}$. The only divisors of pq are $1, p, q$, and pq, and of those only $1 \equiv 1 \pmod{q}$, because $p < q$.
By the Second Sylow Theorem, the unique Sylow q-subgroup H is normal. Since H is of order q it is abelian. Now consider the conjugation action of G on the normal subgroup H: it defines a homomorphism $c : G \to Aut(H) = \mathbb{Z}_q^\times$.
The image J is a divisor of $q-1$, but $J \xrightarrow{\sim} \frac{|G|}{|\ker c|}$ by the First Isomorphism Theorem. So $|J|$ divides $gcd(|G|, q-1) = gcd(pq, q-1) = gcd(p, q-1)$, since q is relatively prime to $q-1$. (Anyway, H is abelian, so its conjugation action on itself is trivial.) . Thus if p does not divide $q-1$, then $|J| = 1$, which means that G is abelian. □

Some applications

Proof.

If a is the number of Sylow q-subgroups of G, then a divides pq and $a \equiv 1 \pmod{q}$. The only divisors of pq are $1, p, q$, and pq, and of those only $1 \equiv 1 \pmod{q}$, because $p < q$.

By the Second Sylow Theorem, the unique Sylow q-subgroup H is normal. Since H is of order q it is abelian. Now consider the conjugation action of G on the normal subgroup H: it defines a homomorphism $c : G \to Aut(H) = \mathbb{Z}_q^\times$.

The image J is a divisor of $q-1$, but $J \xrightarrow{\sim} \frac{|G|}{|\ker c|}$ by the First Isomorphism Theorem. So $|J|$ divides $gcd(|G|, q-1) = gcd(pq, q-1) = gcd(p, q-1)$, since q is relatively prime to $q-1$. (Anyway, H is abelian, so its conjugation action on itself is trivial.) . Thus if p does not divide $q-1$, then $|J| = 1$, which means that G is abelian. □

Some applications

Proof.

If a is the number of Sylow q-subgroups of G, then a divides pq and $a \equiv 1 \pmod{q}$. The only divisors of pq are $1, p, q$, and pq, and of those only $1 \equiv 1 \pmod{q}$, because $p < q$.

By the Second Sylow Theorem, the unique Sylow q-subgroup H is normal. Since H is of order q it is abelian. Now consider the conjugation action of G on the normal subgroup H: it defines a homomorphism $c : G \to Aut(H) = \mathbb{Z}_q^\times$.

The image J is a divisor of $q-1$, but $J \xrightarrow{\sim} \frac{|G|}{|\ker c|}$ by the First Isomorphism Theorem. So $|J|$ divides $gcd(|G|, q-1) = gcd(pq, q-1) = gcd(p, q-1)$, since q is relatively prime to $q-1$. (Anyway, H is abelian, so its conjugation action on itself is trivial.) . Thus if p does not divide $q-1$, then $|J| = 1$, which means that G is abelian. □

Some applications

Proof.

If a is the number of Sylow q-subgroups of G, then a divides pq and $a \equiv 1 \pmod{q}$. The only divisors of pq are $1, p, q$, and pq, and of those only $1 \equiv 1 \pmod{q}$, because $p < q$.

By the Second Sylow Theorem, the unique Sylow q-subgroup H is normal. Since H is of order q it is abelian. Now consider the conjugation action of G on the normal subgroup H: it defines a homomorphism $c : G \to Aut(H) = \mathbb{Z}_q^\times$.

The image J is a divisor of $q-1$, but $J \xrightarrow{\sim} \frac{|G|}{|\ker c|}$ by the First Isomorphism Theorem. So $|J|$ divides $gcd(|G|, q-1) = gcd(pq, q-1) = gcd(p, q-1)$, since q is relatively prime to $q-1$. (Anyway, H is abelian, so its conjugation action on itself is trivial.) . Thus if p does not divide $q-1$, then $|J| = 1$, which means that G is abelian. □

Some applications

Proof.

If a is the number of Sylow q-subgroups of G, then a divides pq and $a \equiv 1 \pmod{q}$. The only divisors of pq are $1, p, q$, and pq, and of those only $1 \equiv 1 \pmod{q}$, because $p < q$.

By the Second Sylow Theorem, the unique Sylow q-subgroup H is normal. Since H is of order q it is abelian. Now consider the conjugation action of G on the normal subgroup H: it defines a homomorphism $c : G \to Aut(H) = \mathbb{Z}_q^{\times}$.

The image J is a divisor of $q - 1$, but $J \xrightarrow{\sim} \frac{|G|}{|\ker c|}$ by the First Isomorphism Theorem. So $|J|$ divides $gcd(|G|, q - 1) = gcd(pq, q - 1) = gcd(p, q - 1)$, since q is relatively prime to $q - 1$. (Anyway, H is abelian, so its conjugation action on itself is trivial.) . Thus if p does not divide $q - 1$, then $|J| = 1$, which means that G is abelian. □

The case of S_4

If $G = S_4$ then $|G| = 24 = 2^3 \times 3$. We know that any 3 cycle generates a Sylow 3-subgroup. What is the structure of a Sylow 2-subgroup?

A Sylow 2-subgroup of A_4 is isomorphic to the Klein group K_4, and contains all the elements with cycle decomposition $2+2$. This set is invariant under conjugation by S_4, so K_4 is a normal subgroup of S_4. Let $s = (12) \in S_4$ (or any 2 cycle), H the subgroup generated by s. Then $P = H \cdot K_4$ is a Sylow 2-subgroup of order 8 with a normal subgroup of index 2.

The case of S_4

If $G = S_4$ then $|G| = 24 = 2^3 \times 3$. We know that any 3 cycle generates a Sylow 3-subgroup. What is the structure of a Sylow 2-subgroup?
A Sylow 2-subgroup of A_4 is isomorphic to the Klein group K_4, and contains all the elements with cycle decomposition $2 + 2$. This set is invariant under conjugation by S_4, so K_4 is a normal subgroup of S_4.
Let $s = (12) \in S_4$ (or any 2 cycle), H the subgroup generated by s. Then $P = H \cdot K_4$ is a Sylow 2-subgroup of order 8 with a normal subgroup of index 2.

S_4, continued

Note that s commutes with $(12)(34)$ but not with $x = (13)(24)$ or $y = (14)(23)$. In fact, we compute easily:

$$sxs^{-1} = y; sys^{-1} = x.$$

So P is not abelian, and its center is of order 2. Note that

$$s \cdot x = s \cdot (13)(24) = (1324); x \cdot s = (1423) = (1324)^{-1}.$$

So s normalizes the subgroup generated by the 4-cycle (1324) and takes it to its inverse:

$$s \cdot (1324)s^{-1} = s \cdot s \cdot x \cdot s = x \cdot s = (1324)^{-1}.$$

This shows that P is isomorphic to D_8 (and not Q_8).

S_4, continued

Note that s commutes with $(12)(34)$ but not with $x = (13)(24)$ or $y = (14)(23)$. In fact, we compute easily:

$$sxs^{-1} = y; sys^{-1} = x.$$

So P is not abelian, and its center is of order 2. Note that

$$s \cdot x = s \cdot (13)(24) = (1324); x \cdot s = (1423) = (1324)^{-1}.$$

So s normalizes the subgroup generated by the 4-cycle (1324) and takes it to its inverse:

$$s \cdot (1324)s^{-1} = s \cdot s \cdot x \cdot s = x \cdot s = (1324)^{-1}.$$

This shows that P is isomorphic to D_8 (and not Q_8).

S_4, continued

Note that s commutes with $(12)(34)$ but not with $x = (13)(24)$ or $y = (14)(23)$. In fact, we compute easily:

$$sxs^{-1} = y; sys^{-1} = x.$$

So P is not abelian, and its center is of order 2. Note that

$$s \cdot x = s \cdot (13)(24) = (1324); x \cdot s = (1423) = (1324)^{-1}.$$

So s normalizes the subgroup generated by the 4-cycle (1324) and takes it to its inverse:

$$s \cdot (1324)s^{-1} = s \cdot s \cdot x \cdot s = x \cdot s = (1324)^{-1}.$$

This shows that P is isomorphic to D_8 (and not Q_8).

S_4, continued

Note that s commutes with $(12)(34)$ but not with $x = (13)(24)$ or $y = (14)(23)$. In fact, we compute easily:

$$sxs^{-1} = y; sys^{-1} = x.$$

So P is not abelian, and its center is of order 2. Note that

$$s \cdot x = s \cdot (13)(24) = (1324); x \cdot s = (1423) = (1324)^{-1}.$$

So s normalizes the subgroup generated by the 4-cycle (1324) and takes it to its inverse:

$$s \cdot (1324)s^{-1} = s \cdot s \cdot x \cdot s = x \cdot s = (1324)^{-1}.$$

This shows that P is isomorphic to D_8 (and not Q_8).

S_4, continued

Note that s commutes with $(12)(34)$ but not with $x = (13)(24)$ or $y = (14)(23)$. In fact, we compute easily:

$$sxs^{-1} = y; sys^{-1} = x.$$

So P is not abelian, and its center is of order 2. Note that

$$s \cdot x = s \cdot (13)(24) = (1324); x \cdot s = (1423) = (1324)^{-1}.$$

So s normalizes the subgroup generated by the 4-cycle (1324) and takes it to its inverse:

$$s \cdot (1324)s^{-1} = s \cdot s \cdot x \cdot s = x \cdot s = (1324)^{-1}.$$

This shows that P is isomorphic to D_8 (and not Q_8).

Sylow subgroups of A_5

On the other hand, $|A_5| = 60 = 2^2 \cdot 3 \cdot 5$. So a Sylow 2-subgroup is just K_4 again. but it's no longer normal, because there are 15 elements with cycle decomposition $2 + 2$, and they don't form a subgroup; for example, $(13)(25)$, $(15)(24)$, etc. The Sylow 3 and 5-subgroups are generated by a 3-cycle and a 5-cycle, respectively.

There are 24 5-cycles, and each Sylow 5-subgroup has 4 generators, so there are 6 Sylow 5-subgroups. And $6|60$, $6 \equiv 1 \pmod 5$.

Sylow subgroups of A_5

On the other hand, $|A_5| = 60 = 2^2 \cdot 3 \cdot 5$. So a Sylow 2-subgroup is just K_4 again. but it's no longer normal, because there are 15 elements with cycle decomposition $2 + 2$, and they don't form a subgroup; for example, $(13)(25)$, $(15)(24)$, etc. The Sylow 3 and 5-subgroups are generated by a 3-cycle and a 5-cycle, respectively.
There are 24 5-cycles, and each Sylow 5-subgroup has 4 generators, so there are 6 Sylow 5-subgroups. And $6|60$, $6 \equiv 1 \pmod 5$.

A theorem of Cauchy

Theorem

Let G be a finite group of order n and let p be a prime dividing n. Then G has an element of order p.

Proof.

We use the Class Equation, where the x_i are representatives of conjugacy classes not in the center:

$$|G| = |Z(G)| + \sum_i [G : C_{x_i}]$$

Assume the theorem is true for groups of order less than n. If p divides the order of one of the C_{x_i}, then by induction C_{x_i} has an element g of order p, because $|C_{x_i}| < |G| = n$. But $g \in C_{x_i} \subseteq G$, so we are done. □

A theorem of Cauchy

Theorem

Let G be a finite group of order n and let p be a prime dividing n. Then G has an element of order p.

Proof.

We use the Class Equation, where the x_i are representatives of conjugacy classes not in the center:

$$|G| = |Z(G)| + \sum_i [G : C_{x_i}]$$

Assume the theorem is true for groups of order less than n. If p divides the order of one of the C_{x_i}, then by induction C_{x_i} has an element g of order p, because $|C_{x_i}| < |G| = n$. But $g \in C_{x_i} \subseteq G$, so we are done. □

Proof of Cauchy's theorem, continued

Proof.

So we assume p divides no C_{x_i}. Then $p|[G : C_{x_i}] = |G|/|C_{x_i}|$ for all i.

Now p divides

$$|G| - \sum_i [G : C_{x_i}] = |Z(G)|$$

because it divides each term on the left-hand side. Thus p divides $|Z(G)|$. But then $|Z(G)|$ has an element of order p, by the classification of finite abelian groups. □

Proof of Cauchy's theorem, continued

Proof.

So we assume p divides no C_{x_i}. Then $p|[G : C_{x_i}] = |G|/|C_{x_i}|$ for all i. Now p divides

$$|G| - \sum_i [G : C_{x_i}] = |Z(G)|$$

because it divides each term on the left-hand side. Thus p divides $|Z(G)|$. But then $|Z(G)|$ has an element of order p, by the classification of finite abelian groups.

Proof of Cauchy's theorem, continued

Proof.

So we assume p divides no C_{x_i}. Then $p|[G:C_{x_i}] = |G|/|C_{x_i}|$ for all i. Now p divides

$$|G| - \sum_i [G:C_{x_i}] = |Z(G)|$$

because it divides each term on the left-hand side. Thus p divides $|Z(G)|$. But then $|Z(G)|$ has an element of order p, by the classification of finite abelian groups.

□

Proof of the First Sylow Theorem

Of courser the proof is by induction on $|G|$. Say $n = |G| = p^r m$ with $p \nmid m$. We use the Class Equation in the opposite way.

$$|G| = |Z(G)| + \sum_i [G : C_{x_i}]$$

If G is abelian then we know the result by the classification of finite abelian groups. So we assume G is not abelian. . Then the set of x_i is not empty, and for each i $|C_{x_i}| < n$.

Proof of the First Sylow Theorem

Of courser the proof is by induction on $|G|$. Say $n = |G| = p^r m$ with $p \nmid m$. We use the Class Equation in the opposite way.

$$|G| = |Z(G)| + \sum_i [G : C_{x_i}]$$

If G is abelian then we know the result by the classification of finite abelian groups. So we assume G is not abelian. . Then the set of x_i is not empty, and for each i $|C_{x_i}| < n$.

Proof of the First Sylow Theorem

Of courser the proof is by induction on $|G|$. Say $n = |G| = p^r m$ with $p \nmid m$. We use the Class Equation in the opposite way.

$$|G| = |Z(G)| + \sum_i [G : C_{x_i}]$$

If G is abelian then we know the result by the classification of finite abelian groups. So we assume G is not abelian. . Then the set of x_i is not empty, and for each i $|C_{x_i}| < n$.

Proof of the First Sylow Theorem, continued

First suppose p does not divide $[G : C_{x_i}]$ for at least one i, hence p^r divides C_{x_i}, which is of smaller order than G. By induction C_{x_i} has a subgroup of order p^r.

So we may suppose p divides every $[G : C_{x_i}]$, hence p divides $|Z(G)|$. Then $Z(G)$ contains a subgroup N of order p (by classification, or by Cauchy's theorem). But any subgroup of $Z(G)|$ is normal in G (exercise). So G/N is of order less than n and by induction contains a subgroup $\bar{K}$ of order p^{r-1}. Let $K \subset G$ be the corresponding subgroup containing N (the preimage of $\bar{K}$ under the quotient map). Then

$$|K| = |N|\bar{K} = p \cdot p^{r-1} = p^r.$$

and we are done.

Proof of the First Sylow Theorem, continued

First suppose p does not divide $[G : C_{x_i}]$ for at least one i, hence p^r divides C_{x_i}, which is of smaller order than G. By induction C_{x_i} has a subgroup of order p^r.

So we may suppose p divides every $[G : C_{x_i}]$, hence p divides $|Z(G)|$. Then $Z(G)$ contains a subgroup N of order p (by classification, or by Cauchy's theorem). But any subgroup of $Z(G)|$ is normal in G (exercise). So G/N is of order less than n and by induction contains a subgroup $\bar{K}$ of order p^{r-1}. Let $K \subset G$ be the corresponding subgroup containing N (the preimage of $\bar{K}$ under the quotient map). Then

$$|K| = |N|\bar{K} = p \cdot p^{r-1} = p^r.$$

and we are done.

Proof of the First Sylow Theorem, continued

First suppose p does not divide $[G : C_{x_i}]$ for at least one i, hence p^r divides C_{x_i}, which is of smaller order than G. By induction C_{x_i} has a subgroup of order p^r.

So we may suppose p divides every $[G : C_{x_i}]$, hence p divides $|Z(G)|$. Then $Z(G)$ contains a subgroup N of order p (by classification, or by Cauchy's theorem). But any subgroup of $Z(G)|$ is normal in G (exercise). So G/N is of order less than n and by induction contains a subgroup $\bar{K}$ of order p^{r-1}. Let $K \subset G$ be the corresponding subgroup containing N (the preimage of $\bar{K}$ under the quotient map). Then

$$|K| = |N|\bar{K} = p \cdot p^{r-1} = p^r.$$

and we are done.

Proof of the First Sylow Theorem, continued

First suppose p does not divide $[G : C_{x_i}]$ for at least one i, hence p^r divides C_{x_i}, which is of smaller order than G. By induction C_{x_i} has a subgroup of order p^r.
So we may suppose p divides every $[G : C_{x_i}]$, hence p divides $|Z(G)|$. Then $Z(G)$ contains a subgroup N of order p (by classification, or by Cauchy's theorem). But any subgroup of $Z(G)|$ is normal in G (exercise). So G/N is of order less than n and by induction contains a subgroup $\bar{K}$ of order p^{r-1}. Let $K \subset G$ be the corresponding subgroup containing N (the preimage of $\bar{K}$ under the quotient map). Then

$$|K| = |N|\bar{K} = p \cdot p^{r-1} = p^r.$$

and we are done.

Normalizers

Definition

Let $H \subseteq G$ be a subgroup. The **normalizer** $N_G(H)$ of H in G is the set of $g \in G$ such that
$$gHg^{-1} \subseteq H.$$

Lemma

If G is finite then $|gHg^{-1}| = |H|$ for any $g \in G$. So $gHg^{-1} \subseteq H$ implies $gHg^{-1} = H$.

Proof.

Conjugation by g is a bijection between gHg^{-1} and H, so it preserves the cardinality. □

Normalizers

Definition

Let $H \subseteq G$ be a subgroup. The **normalizer** $N_G(H)$ of H in G is the set of $g \in G$ such that

$$gHg^{-1} \subseteq H.$$

Lemma

If G is finite then $|gHg^{-1}| = |H|$ for any $g \in G$. So $gHg^{-1} \subseteq H$ implies $gHg^{-1} = H$.

Proof.

Conjugation by g is a bijection between gHg^{-1} and H, so it preserves the cardinality. □

Normalizers

Definition

Let $H \subseteq G$ be a subgroup. The **normalizer** $N_G(H)$ of H in G is the set of $g \in G$ such that

$$gHg^{-1} \subseteq H.$$

Lemma

If G is finite then $|gHg^{-1}| = |H|$ for any $g \in G$. So $gHg^{-1} \subseteq H$ implies $gHg^{-1} = H$.

Proof.

Conjugation by g is a bijection between gHg^{-1} and H, so it preserves the cardinality. □

A lemma

Lemma

Let $H \subseteq G$ be a subgroup. Then $N_G(H)$ is a subgroup of G.

Proof.

Obvious: if $g_1, g_2 \in N_G(H)$, then

$$g_1 g_2 (H) g_2^{-1} g_1^{-1} \subset g_1 H g_1^{-1} \subset H.$$

□

Of course $H \subset N_G(H)$ (and is even a normal subgroup).

A lemma

Lemma

Let $H \subseteq G$ be a subgroup. Then $N_G(H)$ is a subgroup of G.

Proof.

Obvious: if $g_1, g_2 \in N_G(H)$, then

$$g_1 g_2 (H) g_2^{-1} g_1^{-1} \subset g_1 H g_1^{-1} \subset H.$$

□

Of course $H \subset N_G(H)$ (and is even a normal subgroup).

A lemma

Lemma

Let $H \subseteq G$ be a subgroup. Then $N_G(H)$ is a subgroup of G.

Proof.

Obvious: if $g_1, g_2 \in N_G(H)$, then

$$g_1 g_2 (H) g_2^{-1} g_1^{-1} \subset g_1 H g_1^{-1} \subset H.$$

□

Of course $H \subset N_G(H)$ (and is even a normal subgroup).

Another lemma

Lemma

Suppose $P \subseteq G$ is a p-Sylow subgroup. Let $g \in N_G(P)$ and assume g has order p^r for some $r \geq 1$. Then $g \in P$.

Proof.

Consider the subgroup $\langle gP \rangle \subset N_G(P)/P$. If $g \notin P$ then $\langle gP \rangle$ has order p. Let $J \subset N_G(P)$ be the subgroup generated by g and P; so that

$$J/P = \langle gP \rangle.$$

On the other hand, the coset gP is the image of g under the map $J \mapsto J/P$, and is thus of order p^a for some $a \leq r$. If $g \notin P$ it follows that $|J| = p \cdot |P| > |P|$. But $|P|$ is the largest power of p dividing $|G|$. Thus we must have $J = P$. □

Another lemma

Lemma

Suppose $P \subseteq G$ is a p-Sylow subgroup. Let $g \in N_G(P)$ and assume g has order p^r for some $r \geq 1$. Then $g \in P$.

Proof.

Consider the subgroup $\langle gP \rangle \subset N_G(P)/P$. If $g \notin P$ then $\langle gP \rangle$ has order p. Let $J \subset N_G(P)$ be the subgroup generated by g and P; so that

$$J/P = \langle gP \rangle.$$

On the other hand, the coset gP is the image of g under the map $J \mapsto J/P$, and is thus of order p^a for some $a \leq r$. If $g \notin P$ it follows that $|J| = p \cdot |P| > |P|$. But $|P|$ is the largest power of p dividing $|G|$. Thus we must have $J = P$. □

Another lemma

Lemma

Suppose $P \subseteq G$ is a p-Sylow subgroup. Let $g \in N_G(P)$ and assume g has order p^r for some $r \geq 1$. Then $g \in P$.

Proof.

Consider the subgroup $\langle gP \rangle \subset N_G(P)/P$. If $g \notin P$ then $\langle gP \rangle$ has order p. Let $J \subset N_G(P)$ be the subgroup generated by g and P; so that

$$J/P = \langle gP \rangle.$$

On the other hand, the coset gP is the image of g under the map $J \mapsto J/P$, and is thus of order p^a for some $a \leq r$. If $g \notin P$ it follows that $|J| = p \cdot |P| > |P|$. But $|P|$ is the largest power of p dividing $|G|$. Thus we must have $J = P$. □

Another lemma

Lemma

Suppose $P \subseteq G$ is a p-Sylow subgroup. Let $g \in N_G(P)$ and assume g has order p^r for some $r \geq 1$. Then $g \in P$.

Proof.

Consider the subgroup $\langle gP \rangle \subset N_G(P)/P$. If $g \notin P$ then $\langle gP \rangle$ has order p. Let $J \subset N_G(P)$ be the subgroup generated by g and P; so that

$$J/P = \langle gP \rangle.$$

On the other hand, the coset gP is the image of g under the map $J \mapsto J/P$, and is thus of order p^a for some $a \leq r$. If $g \notin P$ it follows that $|J| = p \cdot |P| > |P|$. But $|P|$ is the largest power of p dividing $|G|$. Thus we must have $J = P$. □

One more lemma

Lemma

Suppose $H, K \subseteq G$ are subgroups. The number of distinct subgroups hKh^{-1}, with $h \in H$, is $[H : N_G(K) \cap H]$.

Proof.

Omitted: see Judson book, p. 191, Lemma 15.6. □

This is easy but it is another one of those proofs that is best read rather than seen on the (virtual) blackboard. The idea is clear:

$$h_1 K h_1^{-1} = h_2 K h_2^{-1} \Leftrightarrow (h_2 h_1^{-1}) K (h_2 h_1^{-1})^{-1} = K \Leftrightarrow h_2 \in h_1 N_G(K).$$

So the set of H-conjugates of K is in bijection with $H/(N_G(K) \cap H)$.

One more lemma

Lemma

Suppose $H, K \subseteq G$ are subgroups. The number of distinct subgroups hKh^{-1}, with $h \in H$, is $[H : N_G(K) \cap H]$.

Proof.

Omitted: see Judson book, p. 191, Lemma 15.6. □

This is easy but it is another one of those proofs that is best read rather than seen on the (virtual) blackboard. The idea is clear:

$$h_1Kh_1^{-1} = h_2Kh_2^{-1} \Leftrightarrow (h_2h_1^{-1})K(h_2h_1^{-1})^{-1} = K \Leftrightarrow h_2 \in h_1N_G(K).$$

So the set of H-conjugates of K is in bijection with $H/(N_G(K) \cap H)$.

One more lemma

Lemma

Suppose $H, K \subseteq G$ are subgroups. The number of distinct subgroups hKh^{-1}, with $h \in H$, is $[H : N_G(K) \cap H]$.

Proof.

Omitted: see Judson book, p. 191, Lemma 15.6. □

This is easy but it is another one of those proofs that is best read rather than seen on the (virtual) blackboard. The idea is clear:

$$h_1 K h_1^{-1} = h_2 K h_2^{-1} \Leftrightarrow (h_2 h_1^{-1}) K (h_2 h_1^{-1})^{-1} = K \Leftrightarrow h_2 \in h_1 N_G(K).$$

So the set of H-conjugates of K is in bijection with $H/(N_G(K) \cap H)$.

Proof of the Second Sylow Theorem

Here is the statement again:

Theorem

All Sylow p-subgroups of G are conjugate by elements of G.

Proof.

Let $|G| = n = p^r m$ as before, and let $\mathcal{S} = \{P = P_1, \ldots, P_k\}$ be the set of distinct conjugates of P. By the last Lemma, $k = [G : N_G(P)]$. Since $P \subseteq N_G(P)$, k divides m and thus is not divisible by p. Let $Q \neq P$ be a p-Sylow subgroup. We need to show that $Q = P_i$ for some $i \neq 1$. We consider the set of Q-conjugates of $P_i \in \mathcal{S}$, which is a partition of $\mathcal{S}$. Then

$$k = \sum_i [Q : Q \cap N_G(P_i)] = \sum_i |Q|/|Q \cap N_G(P_i)|.$$

Proof of the Second Sylow Theorem

Here is the statement again:

Theorem

All Sylow p-subgroups of G are conjugate by elements of G.

Proof.

Let $|G| = n = p^r m$ as before, and let $\mathcal{S} = \{P = P_1, \ldots, P_k\}$ be the set of distinct conjugates of P. By the last Lemma, $k = [G : N_G(P)]$. Since $P \subseteq N_G(P)$, k divides m and thus is not divisible by p.
Let $Q \neq P$ be a p-Sylow subgroup. We need to show that $Q = P_i$ for some $i \neq 1$. We consider the set of Q-conjugates of $P_i \in \mathcal{S}$, which is a partition of $\mathcal{S}$. Then

$$k = \sum_i [Q : Q \cap N_G(P_i)] = \sum_i |Q|/|Q \cap N_G(P_i)|.$$

Proof of the Second Sylow Theorem

Proof.

$$k = \sum_i [Q : Q \cap N_G(P_i)] = \sum_i |Q|/|Q \cap N_G(P_i)|.$$

Since p does not divide k it cannot divide $|Q|/|Q \cap N_G(P_i)|$ for some i. But the quotient $|Q|/|Q \cap N_G(P_i)|$ is a power of p, because $|Q|$ is, so $Q \cap N_G(P_j) = Q$ for some j. In other words, $Q \subset N_G(P_j)$, which by the previous lemma implies that $Q \subset P_j$. Since $|Q| = |P_j|$, we are done. □

Proof of the Third Sylow Theorem

Here is the statement again:

Theorem

The number k of distinct Sylow p-subgroups of G is (i) congruent to 1 modulo p and (ii) divides the order of G.

Proof.

We know that $k = [G : N_G(P)]$ if $P = P_1$ is a Sylow p-subgroup. This implies (ii). □

Proof of the Third Sylow Theorem

Proof.

On the other hand, we partition the set $\mathcal{S}$ of Sylow p-subgroups into P-conjugacy classes, as before:

$$k = \sum_i [P : P \cap N_G(P_i)] = 1 + \sum_{i>1} |P|/|P \cap N_G(P_i)|.$$

If $P \cap N_G(P_i) = P$ then $P \subset N_G(P_i)$, and thus $P = P_i$. So for $i > 1$, $|P \cap N_G(P_i)|$ is a proper subgroup of $|P|$, so $|P|/|P \cap N_G(P_i)| \equiv 0 \pmod{p}$. Thus $k \equiv 1 \pmod{p}$, which completes the proof of (i).

Proof of the Third Sylow Theorem

Proof.

On the other hand, we partition the set $\mathcal{S}$ of Sylow p-subgroups into P-conjugacy classes, as before:

$$k = \sum_i [P : P \cap N_G(P_i)] = 1 + \sum_{i>1} |P|/|P \cap N_G(P_i)|.$$

If $P \cap N_G(P_i) = P$ then $P \subset N_G(P_i)$, and thus $P = P_i$. So for $i > 1$, $|P \cap N_G(P_i)|$ is a proper subgroup of $|P|$, so $|P|/|P \cap N_G(P_i)| \equiv 0 \pmod p$. Thus $k \equiv 1 \pmod p$, which completes the proof of (i). □

Groups of order 20

Theorem

There are no simple groups of order 20, 72, 48.

Proof.

If $|G| = 20$, then G has a Sylow 2-subgroup P of order 5. Since 1 is the only divisor of 20 that is congruent to 1 mod 5, P is normal, so G is not simple.

□

Groups of order 72

If $|G| = 72$, we consider a 3-Sylow subgroup P of order 9. The number k of conjugates of H is congruent to 1 mod 3 and divides 72. The divisors of 72 are $1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72$. The only ones congruent to 1 mod 3 are 1 and 4. We have to eliminate $k = 4$. If $k = [G : N_G(P)] = 4$ then by an in-class "challenge" G contains a normal subgroup N, contained in $N_G(P)$, of index $\leq 4! = 24$. Since $24 < 72$ and $N \subseteq N_G(P)$, which is not equal to G (since we are assuming P is not normal), $|N| > 1$ and $N \neq G$. Thus N is a proper normal subgroup of G.

Groups of order 72

If $|G| = 72$, we consider a 3-Sylow subgroup P of order 9. The number k of conjugates of H is congruent to 1 mod 3 and divides 72. The divisors of 72 are $1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72$. The only ones congruent to 1 mod 3 are 1 and 4. We have to eliminate $k = 4$. If $k = [G : N_G(P)] = 4$ then by an in-class "challenge" G contains a normal subgroup N, contained in $N_G(P)$, of index $\leq 4! = 24$. Since $24 < 72$ and $N \subseteq N_G(P)$, which is not equal to G (since we are assuming P is not normal), $|N| > 1$ and $N \neq G$. Thus N is a proper normal subgroup of G.

Groups of order 72

If $|G| = 72$, we consider a 3-Sylow subgroup P of order 9. The number k of conjugates of H is congruent to 1 mod 3 and divides 72. The divisors of 72 are $1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72$. The only ones congruent to 1 mod 3 are 1 and 4. We have to eliminate $k = 4$. If $k = [G : N_G(P)] = 4$ then by an in-class "challenge" G contains a normal subgroup N, contained in $N_G(P)$, of index $\leq 4! = 24$. Since $24 < 72$ and $N \subseteq N_G(P)$, which is not equal to G (since we are assuming P is not normal), $|N| > 1$ and $N \neq G$. Thus N is a proper normal subgroup of G.

Groups of order 48

Finally, if $|G| = 48$, let P be a 2-Sylow subgroup, of order 16, thus of index 3. Again, G contains a normal subgroup of index $\leq 3! = 6$, which is less than 48.

Groups of order 48

Finally, if $|G| = 48$, let P be a 2-Sylow subgroup, of order 16, thus of index 3. Again, G contains a normal subgroup of index $\leq 3! = 6$, which is less than 48.

Proof of the “challenge”

Challenge

If G contains a subgroup H of index n then G contains a **proper normal** subgroup N of index at most $n!$; in fact, $N \subseteq H$, so in particular $N \neq G$.

Proof.

Consider the set X of left cosets G/H. Multiplication on the left by G defines a permutation of the n elements of X (in fact, a transitive action). Thus there is a homomorphism $s : G \to S_n$, and

$$G/\ker(s) \xrightarrow{\sim} Image(s) \subseteq S_n.$$

It follows that $\ker(s)$ is of index $|Image(s)| \leq |S_n| = n!$. And $\ker(s)$ is a normal subgroup.

Proof of the "challenge"

Challenge

If G contains a subgroup H of index n then G contains a **proper normal** subgroup N of index at most $n!$; in fact, $N \subseteq H$, so in particular $N \neq G$.

Proof.

Consider the set X of left cosets G/H. Multiplication on the left by G defines a permutation of the n elements of X (in fact, a transitive action). Thus there is a homomorphism $s : G \to S_n$, and

$$G/\ker(s) \xrightarrow{\sim} Image(s) \subseteq S_n.$$

It follows that $\ker(s)$ is of index $|Image(s)| \leq |S_n| = n!$. And $\ker(s)$ is a normal subgroup.

□