3

Sylow's Theorem

Double cosets

Peter Ludwig Mejdell Sylow
1832 – 1918

Definition. Let K, H are subgroups of a group G. Put

$$KgH := \{ kgh \mid k \in K, h \in H \}, \text{ where } g \in G.$$

The subset KgH is called a double coset of a pair $\langle K, H \rangle$ in G. We will use the notation:

$K \backslash G / H$ for the set of double coset of $\langle K, H \rangle$ in G.

Proposition 3.1: Let K, H be subgroups of a group G.

1. Each $g \in G$ belongs to a unique double coset of $\langle K, H \rangle$ in G.
2. The group G is a disjoint union of double cosets of $\langle K, H \rangle$ in G.
3. Every double coset KgH is a union of $|K : (K \cap gHg^{-1})|$ left cosets of H

Proof. 1. Clearly $g \in KgH$. If $g \in KhH$ for some $h \in G$, then $g = u \cdot h \cdot v$ for some $u \in K, v \in H$ and $KgH = KuhvH = KhH$.

2. Follows from 1.

3. Put $A := \{ kgH \mid k \in K \}$. Since $KgH = \bigcup_{k \in K} kgH$, the double coset KgH is a union of $|A|$ left cosets of H. It remains to show that $|A| = |K : (K \cap gHg^{-1})|$.

For $k_1, k_2 \in K$:

- $k_1 gH = k_2 gH$ iff $g^{-1}k_2^{-1}k_1 gH = H$ iff $g^{-1}k_2^{-1}k_1 g \in H$ iff $k_2^{-1}k_1 \in gHg^{-1}$
- $k_1 \cdot (K \cap gHg^{-1}) = k_2 (K \cap gHg^{-1})$ iff $k_2^{-1}k_1 \in K \cap gHg^{-1}$

Since $k_1, k_2 \in K$, the product $k_2^{-1}k_1 \in K \cap gHg^{-1}$ iff $k_2^{-1}k_1 \in gHg^{-1}$. Therefore $k_1 gH = k_2 gH$ iff $k_1 (K \cap gHg^{-1}) = k_2 (K \cap gHg^{-1})$, and so $|A| = |K : K \cap gHg^{-1}|$. $\square$

Corollary 3.2: Let K, H be subgroups of a group G. Let Δ be a complete set of representatives of double cosets of $\langle K, H \rangle$ in G. Then

$$|G : H| = \sum_{g \in \Delta} |K : (K \cap gHg^{-1})| \qquad (*)$$

Proof: ~~Every left coset gH of H in G is a union of |K : (K ∩ gH~~

Every double coset KgH of $\langle K, H \rangle$ in G is a union of $|K : (K \cap gHg^{-1})|$ left cosets of H in G and G is a disjoint union of the double cosets. $\square$

SYLOW'S THEOREM

Definition: Let G be a finite group of order $p^k \cdot m$, where p is a prime, $k \geq 1$ and $p \nmid m$.
A Sylow p-subgroup of G is a subgroup of order p^k.

Recall: Let $\mathbb{F}$ be a finite field of a characteristic p. Then p is a prime and $|\mathbb{F}| = q = p^k$, for some $k \geq 1$.

- $GL_n(q)$ denote the group of all regular $n \times n$-matrices with entries from $\mathbb{F}$.
- $UT_n(q)$ denote the subgroup of $GL_n(q)$ of all upper triangular matrices with 1 on the diagonal.

Lemma 3.3 Let p be a prime, $k \geq 1$, and $q = p^k$. Then

1. $|GL_n(q)| = \prod_{i=0}^{n-1} (q^n - q^i)$
2. $|UT_n(q)| = q^{\frac{n(n-1)}{2}}$

Proof. 1) Let A be a regular $n \times n$ matrix over a q-element field.
- The first row of A can be any non-zero vector. There is $q^n - 1 = q^n - q^0$ of them
- Suppose that we have chosen first i rows. They are linearly independent, and so they span a subspace of dimension i. Its size is q^i. The $(i+1)$st row can be any vector not in this subspace. There are $q^n - q^i$ of them.

Alltogether we have $(q^n - q^0)(q^n - q)\dots(q^n - q^{n-1})$ regular $n \times n$ matrices.

2) Let $B \in UT_n(q)$. There are as many such matrices as ~~elemen~~ possible distributions of elements above ~~over~~ the diagonal. Because there are $\frac{n(n-1)}{2}$ elements ~~over~~ above the diagonal, we have $q^{\frac{n(n-1)}{2}}$ matrices in $UT_n(q)$. $\square$

Proposition 3.4. Let q be a power of a prime p. Then $UT_n(q)$ is a Sylow p-subgroup of $GL_n(q)$.

Proof: By the previous Lemma:

$$|GL_n(q)| = \prod_{i=0}^{n-1}(q^n - q^i) = \prod_{i=0}^{n-1} q^i (q^{n-i} - 1) = \prod_{i=0}^{n-1} q^i \prod_{i=0}^{n-1}(q^{n-i} - 1) = q^{\sum_{i=0}^{n-1} i} \prod_{i=0}^{n-1}(q^{n-i}-1) =$$

$$= q^{\frac{n(n-1)}{2}} \cdot \prod_{i=0}^{n-1}(q^{n-i} - 1) = q^{\frac{n(n-1)}{2}} \prod_{j=1}^{n}(q^j - 1)$$

Observe that $p \nmid \prod_{j=1}^{n}(q^j - 1)$. Since $|UT_n(q)| = q^{\frac{n(n-1)}{2}}$, it is a Sylow p-subgroup of $GL_n(q)$. $\square$

Lemma 3.5: Let H be a Sylow p-subgroup of a finite group G. Let K be a subgroup of G such that $p \mid |K|$. Then there is $x \in G$ such that $K \cap xHx^{-1}$ is a Sylow p-subgroup of K.

Proof. Formula (*) gives

$$|G : H| = \sum_{g \in \Delta} |K : (K \cap gHg^{-1})|,$$

where Δ is a complete set of representatives of double cosets of $\langle K, H \rangle$ in G.

Since H is a p-group, gHg^{-1} is a p-group for every $g \in G$, and $K \cap gHg^{-1}$ is a p-group as well, because it is a subgroup of a p-group.

Since H is a Sylow p-subgroup of G, $p \nmid |G : H|$. It follows that $p \nmid |K : (K \cap xHx^{-1})|$ for some $x \in \Delta$. By the Lagrange theorem:

$$\underbrace{|K|}_{\substack{\text{divisible} \\ \text{by } p}} = \underbrace{|K : (K \cap xHx^{-1})|}_{\text{not divisible by } p} \cdot \underbrace{|K \cap xHx^{-1}|}_{p\text{-group}}.$$

We conclude that $K \cap xHx^{-1}$ is a Sylow p-subgroup of K. $\square$

Theorem (Sylow) 3.6: Let p be a prime number, $k \geq 1$ and m such that $p \nmid m$. Let G be a finite group of order $p^k m$. Then

1. there is a Sylow p-subgroup in G.
2. every p-subgroup of G is contained in a Sylow p-subgroup of G.
3. any two Sylow p-subgroups of G are conjugate.
4. the number of Sylow p-subgroups of G divides m and is congruent to 1 modulo p.

Proof: 1. Recall that a finite group G embeds into the group $GL_n(p)$, where $n = |G|$; this follows from the Cayley's theorem. Apply the previous Lemma with $K := G$, $G := GL_n(p)$ and $H = UT_n(p)$ being a Sylow p-subgroup of G.

2. Observe that a subgroup conjugated to a Sylow p-~~s~~ subgroup of G is again a Sylow p-subgroup of G. Apply the previous Lemma with G as G, K being the given p-group and H a Sylow p-subgroup of G (which exists by 1). We get $x \in G$ such that $K \cap xHx^{-1}$ is a Sylow p-subgroup of K. But K is a p-group, and so $K \leq xHx^{-1}$.

3 Let H, K be Sylow p-subgroups of G. Applying the Lemma again, we get that $K = xHx^{-1}$ for some $x \in G$.

4 In order to prove the last item, we introduce / recall the following concept:

- Let A, B be subsets of a group G. We denote

$$A \cdot B = \{ a \cdot b \mid a \in A, b \in B \}.$$

Lemma 3.7: If A, B are subgroups of a group G, then

$$|A \cdot B| = \frac{|A| \cdot |B|}{|A \cap B|} \qquad (**)$$

Proof. Define an equivalence relation on the set $A \times B$ by $\langle a_1, b_1 \rangle \sim \langle a_2, b_2 \rangle$ iff $a_1 b_1 = a_2 b_2$ and denote by $A\times B/_\sim$ the set of all blocks of $\sim$. Clearly

$$|A \cdot B| = |A \times B/_\sim|.$$

◁ If $a_1 b_1 = a_2 b_2$ for some $a_1, a_2 \in A$, $b_1, b_2 \in B$, then $a_2^{-1} a_1 = b_2 b_1^{-1} = c \in A \cap B$. Then $a_2 = a_1 c^{-1}$ and $b_2 = c b_1$. On the other hand, if $a_2 = a_1 c^{-1}$ and $b_2 = c b_1$ for some $c \in A \cap B$, then $a_2 b_2 = a_1 c^{-1} c b_1 = a_1 b_1$.

It follows that a block $[\langle a, b \rangle]_\sim$ of $\sim$ containing a pair $\langle a, b \rangle \in A \times B$ is

$$[\langle a, b \rangle]_\sim = \{ \langle a c^{-1}, c b \rangle \mid c \in A \cap B \}.$$

The size of the block is $|A \cap B|$. Therefore there are $|A \times B| / |A \cap B| = |A| \cdot |B| / |A \cap B|$ blocks, which proves $(**)$. □

Now we can prove 4. Let H be a Sylow p-subgroup of a group G. By 3 all Sylow p-subgroup of the group G are conjugate, hence the number of them is the size of the set $M := \{ gHg^{-1} \mid g \in G \}$. Recall that $|M| = |G : N_G(H)|$, in particular $|M| \mid |G : H| = m$. Therefore the number of sylow p-subgroups divides m.

Let H act on M by conjugation; i.e., $h \cdot (gHg^{-1}) = hg\,H g^{-1} h^{-1}$. The size of every orbit of this action divides $|H| = p^k$. We conclude the proof by showing that $\{H\}$ is the only singleton orbit. Suppose that $\{gHg^{-1}\}$, for some $g \in G \setminus H$, is another one. Then $H \cdot gHg^{-1} = gHg^{-1} H$ and so $H \cdot gHg^{-1}$ is a subgroup of G. Its size is $\frac{|H| \cdot |gHg^{-1}|}{|H \cap gHg^{-1}|} = p^\ell$ for some $\ell > k$ (indeed, $H \cap gHg^{-1}$ is a proper subgroup of H, and so $|H \cap gHg^{-1}| < p^k$). This is impossible since $p^\ell \nmid |G|$.

Since the size of M is the sum of cardinalities of orbits an all but one are divisible by p and the remaing orbit is a singleton, $|M| \equiv 1 \pmod p$.

□

Remark:

1. Let A, B be subgroups of a (finite) group G. Then AB is a subgroup of G iff $AB = BA$. In particular, AB is a subgroup of G if at least one of the ~~gro~~ subgroups A, B is normal.
(Prove this!)
2. One can derive Cauchy's theorem from Sylow's theorem. Try this!

Lemma 3.8: 1) Let $a, b \in G$ be commuting elements, i.e., $ab = ba$, such that $\gcd(o(a), o(b)) = 1$. Then the group $\langle a, b\rangle$ is cyclic, generated by ab, and $o(ab) = o(a)\cdot o(b)$.

2) Let $a_1, \dots, a_k \in G$ be such that $a_i a_j = a_j a_i$ and $\gcd(o(a_i), o(a_j)) = 1$ for all $1 \le i < j \le k$. Then the group $\langle a_1, \dots, a_k\rangle$ is cyclic, generated by $a_1 a_2 \dots a_k$, and $o(a_1 \dots a_k) = o(a_1)\dots o(a_k)$.

Proof: 1) Put $m = o(a)$, $n = o(b)$.

- Then $(ab)^{mn} = (a^m)^n (b^n)^m = 1$. Therefore $o(ab) \mid mn$
- Suppose that $(ab)^t = 1$ for some $t \in \mathbb{N}$. Then
- $1 = (ab)^{mt} = (a^m)^t b^{mt} = b^{mt}$, hence $n \mid mt$. Since $\gcd(m, n) = 1$, $n \mid t$.
- $1 = (ab)^{nt} = a^{nt} (b^n)^t = a^{nt}$, hence $m \mid nt$. Since $\gcd(m, n) = 1$, $m \mid t$.

Since $\gcd(m, n) = 1$, $mn \mid t$; we conclude that $o(ab) = mn$.

Since m and n are relatively prime, there are k, l such that $mk + nl = 1$.

Then $(ab)^{nl} = a^{nl}\cdot(b^n)^l = a^{nl} = a^{mk+nl} = a$ (we use that $a^m = 1$).

$(ab)^{mk} = (a^m)^k b^{mk} = b^{mk} = b^{mk+nl} = b$ (we make use of $b^n = 1$).

Therefore ab generates $\langle a, b\rangle$. In particular, the group $\langle a, b\rangle$ is cyclic.

2) By induction using 1). ∎

Theorem 3.9: The multiplicative group of a finite field is cyclic.

Proof. Let $\mathbb{F}$ be a finite field, let $\mathbb{F}^*$ denote the multiplicative group of $\mathbb{F}$. Let p be a prime and P a Sylow p-group of $\mathbb{F}^*$. As P is a finite p-group, $|P| = p^k$ for some $k \in \mathbb{N}_0$. The polynomial $x^{p^{k-1}} - 1$ has at most p^{k-1} roots. Therefore there is $a_p \in P$ with $a_p^{p^{k-1}} \neq 1$. Since $o(a_p) \mid |P| = p^k$, $o(a_p) = p^k$.

Let $|\mathbb{F}^*| = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$, where $p_1, \dots, p_n$ are distinct primes and $k_1, k_2, \dots, k_n \in \mathbb{N}$. For every $i \in \{1, \dots, n\}$ there is an element $a_i \in \mathbb{F}^*$ with $o(a_i) = p_i^{k_i}$. By the previous Lemma, $o(a_1 \dots a_n) = o(a_1)\dots o(a_n) = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$, hence $|\mathbb{F}^*| = \langle a_1 \dots a_n\rangle$. □