MAS 305 **Algebraic Structures II**

Notes 7 **Autumn 2006**

Sylow's Theorems

Let G be a finite group of order N. Lagrange's Theorem tells us that if $H \leqslant G$ then $|H|$ divides N. The converse is not true: there may be some m dividing N for which G has no subgroup of order m.

Example Take $G = A_4$, with $|G| = 12$. Then $6 \mid 12$ but A_4 has no subgroup of order 6.

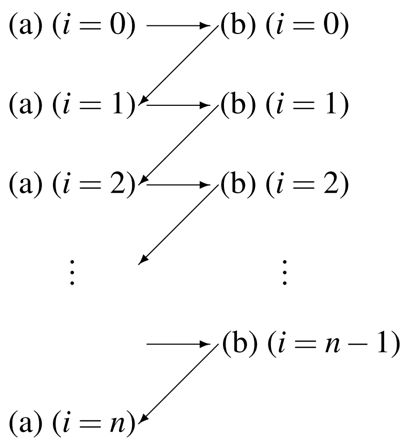
Sylow' Theorems tell us that the converse *is* true when m is a power of a prime number. The following theorem gives the heart of the proof.

Theorem A Let $|G| = p^n s$, where p is a prime, $n \geqslant 1$ and $p \nmid s$. For $i = 1, \ldots, n$,

(a) G contains at least one subgroup of order p^i, and

(b) if $i < n$, every such subgroup is normally contained in a subgroup of order p^{i+1}.

Proof We use a double induction:



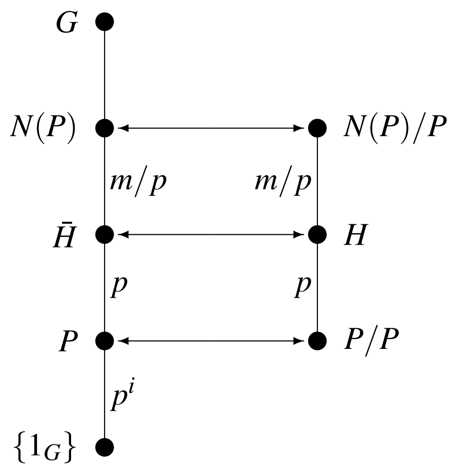
Start Statement (a) is true when $i = 0$: take the subgroup $\{1_G\}$.

One part of inductive step Statement (b) for i clearly implies statement (a) for $i+1$.

Other part of inductive step Assume statement (a) for i, where $i < n$. Then G contains a subgroup P of order p^i.

Consider the action of P by right multiplication on its own right cosets in G. The number of cosets is $|G : P| = p^{n-i}s$, which is divisible by p if $i \leqslant n-1$. The size of each orbit of P divides p^i, so is a power of p, so the number m of orbits of size 1 is divisible by p. Now, $\{Px\}$ is an orbit of size 1 if and only if $x \in N(P)$, so $|N(P)| = mp^i$. But $P \leqslant N(P)$, so $m \neq 0$. Now, $P \trianglelefteq N(P)$, so we can form $N(P)/P$, and $|N(P)/P| = m$, which is divisible by p. By Cauchy's Theorem, $N(P)/P$ has an element of order p and hence a subgroup H of order p. By the Correspondence Theorem, $N(P)$ has a subgroup $\bar{H}$ of order p^{i+1} containing P. So statement (b) is true for i. $\square$

The following picture illustrates the last step in the proof.



Definition Let p be a prime. A *Sylow p-subgroup* of a finite group G is a subgroup H of G such that $|H|$ is the highest power of p dividing $|G|$.

A *Sylow subgroup* of G is a Sylow p-subgroup for some prime p.

Corollary 1 to Theorem A (Sylow's First Theorem) If the prime p divides the order of a finite group G, then G has at least one Sylow p-subgroup.

Corollary 2 to Theorem A If the prime p divides the order of a finite group G and H is a p-subgroup of G then H is contained in at least one Sylow p-subgroup of G.

Corollary 3 to Theorem A If the prime p divides the order of a finite group G and H is a p-subgroup of G and p divides $|G:H|$ (in particular, if G is a p-group and H is any subgroup other than G itself), then p divides $|N(H):H|$; in particular, $H \lneqq N(H)$.

Sylow's Second Theorem For each prime p dividing the order of a finite group G, all Sylow p-subgroups of G are conjugate to each other.

Sylow's Third Theorem For each prime p dividing the order of a finite group G, the number of Sylow p-subgroups of G is congruent to 1 modulo p and divides $|G|$.

Proof of both theorems Let $|G| = p^n s$, where p is prime, $n \geqslant 1$ and $p \nmid s$. Let Ω be the set of Sylow p-subgroups of G. By Sylow's First Theorem, we know that Ω is not empty. Let P and Q be in Ω.

Consider the action of P on Ω by conjugation. If Q is a fixed point of this action then $Q^g = Q$ for all g in P, so $g \in N(Q)$ for all g in P, so $P \leqslant N(Q)$. Consider the group $N(Q)$: we have $P \leqslant N(Q)$ and $Q \trianglelefteq N(Q)$. By the Third Isomorphism Theorem, PQ is a subgroup of $N(Q)$ and $PQ/Q \cong P/P \cap Q$. Therefore PQ is a subgroup of G of order

$$\frac{|P| \times |Q|}{|P \cap Q|} = \frac{p^{2n}}{|P \cap Q|},$$

which is a power of p. Now, $P \leqslant PQ$ and $|P| = p^n$, which is the highest power of p dividing $|G|$, so $|PQ| = p^n$ and $P = PQ$. Similarly, $Q = PQ$. Hence $Q = P$.

Conversely, P itself is certainly a fixed point of this action. So, under the action of P, $\{P\}$ is the only orbit of size 1. All orbits have size dividing p^n, so all the other orbits have size divisible by p. This proves the first part of Sylow's Third Theorem.

Now consider the action of G on Ω by conjugation. The orbits of G are unions of orbits of P, so the orbit of G containing P has size $mp+1$ for some m, while any other orbit of G has size rp for some r. Suppose that Q is in another orbit. Then applying the previous argument with Q in place of P shows that p divides $mp+1$. This contradiction shows that there cannot be another orbit; that is, that G has a single orbit on Sylow p-subgroups, which proves Sylow's Second Theorem.

Now the number of Sylow p-subgroups is equal to the number of conjugates of P in G, which is $|G:N(P)|$, which divides G. This proves the second part of Sylow's Third Theorem. $\square$

Some applications of Sylow's Theorems

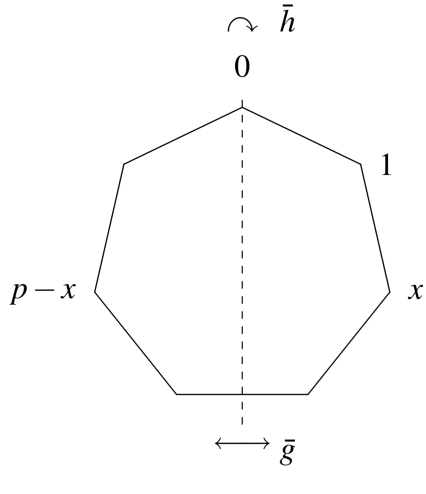
Groups of order $2p$

Suppose that p is an odd prime and $|G| = 2p$. If H is a Sylow p-subgroup of G then $|H| = p$, so H is cyclic. Let $H = \langle h \rangle$. Also, $|G : N(H)|$ divides 2 and is congruent to 1 modulo p, so it must be 1. That is, $N(H) = G$ and $H \lhd G$, and H is the unique Sylow p-subgroup of G.

By Cauchy's Theorem, G has an element g of order 2. Since $H \lhd G$, $g^{-1}hg = h^r$ for some integer r. The map $x \mapsto g^{-1}xg$ is an isomorphism (proof: exercise), so $g^{-1}h^r g = (g^{-1}hg)^r = (h^r)^r = h^{r^2}$. Also, $g^{-1}h^r g = g^{-1}(g^{-1}hg)g = g^{-2}hg^2 = h$ because $g^2 = 1_G$. Therefore $h^{r^2} = h$, so $r^2 = 1$ modulo p. Since p is prime, the integers modulo p form a field, so the only solutions are $r = \pm 1$ modulo p.

If $r = 1$ then $gh = hg$ and so gh has order $2p$ (proof: exercise): therefore $G = \langle gh \rangle$ and G is cyclic. Hence G is Abelian, so $\langle g \rangle \lhd G$, so there is only one Sylow 2-subgroup.

If $r = -1$ then $ghg = h^{-1}$. We shall show that $G \cong D_{2p}$. Label the vertices of the regular p-gon by 0, 1, ..., $p-1$, in the clockwise direction. Let $\bar{h}$ be clockwise rotation through $2\pi/p$, so that $x\bar{h} = x+1$ for every vertex x (using addition modulo p). Let $\bar{g}$ be the reflection through the line of symmetry through the vertex 0, so that $x\bar{g} = p - x$ for every vertex x.



Then

$$x(\bar{g}\bar{h}\bar{g}) = (p-x)(\bar{h}\bar{g}) = (p-x+1)\bar{g} = (x-1) = x\bar{g}^{-1}$$

for every vertex x. Thus the elements of D_{2p} satisfy the correct equations and give a group of the correct order, so $G \cong D_{2p}$.

In D_{2p} there are p Sylow 2-subgroups, one generated by each reflection.

Sylow subgroups of A_4

Temporarily, let us write Q_p for a Sylow p-subgroup, and $N_p = N(Q_p)$.

We have $|A_4| = 12 = 2^2.3$. First consider $p = 3$. Then $|Q_3| = 3$ and so Q_3 is cyclic. There are eight elements of order 3, which come in inverse pairs, so there are four Sylow 3-subgroups, so $|A_4 : N_3| = 4$: therefore $N_3 = Q_3$.

Second, consider $p = 2$. We have $|Q_2| = 4$. There are three elements of order 2, none of order 4, and one of order 1, so these elements whose orders are powers of 2 must all be in a single Sylow 2-subgroup, which is therefore normal in A_4. This subgroup $\{(1),\ (1\,2)(3\,4),\ (1\,3)(2\,4),\ (1\,4)(2\,3)\}$ is sometimes called the *Klein* subgroup of A_4, and written K.

Sylow subgroups of S_4

Now $|S_4| = 24 = 2^3.3$. First consider $p = 3$. Again, Q_3 is cyclic of order 3 and so there are four Sylow 3-subgroups. Now $|N_3| = 24/4 = 6$. Take $Q = \langle(1\,2\,3)\rangle$. In fact, $Q = (A_3 \text{ on } \{1,2,3\})$. Then $Q \trianglelefteq (S_3 \text{ on } \{1,2,3\})$, so $N_3 \cong S_3$.

Second, consider $p = 2$. This time, $|Q_2| = 8$. We know one group of order eight which permutes four objects: the dihedral group D_8. Since D_8 must be contained in S_4, we have $Q_2 \cong D_8$. There are three ways of drawing a square through four points, so there are three Sylow 2-subgroups. (Alternatively, we can argue that D_8 contains exactly two permutations of cycle type 4, and S_4 contains six such permutations, so there must be three Sylow 2-subgroups.) Therefore $|N_2| = 24/3 = 8$ and so $N_2 = Q_2$.

Sylow subgroups of S_5

$|S_5| = 120 = 2^3.3.5$.

First consider $p = 5$. Here Q_5 is cyclic of order 5. There are 24 elements of order 5, with four in each cyclic subgroup of order 5, so there are 6 Sylow 5-subgroups. Therefore $|N_5| = 120/6 = 20$. Can we describe the group N_5 in any other way?

Consider the set of permutations of the integers modulo 5 of the form

$$x \mapsto ax + b,$$

where a and b are integers modulo 5 and $a \neq 0$. There are 20 such permutations, and it is straightforward to check that they form a group, which is called the *affine* group of dimension 1 over $\mathbb{F}_5$, written $\mathrm{Aff}(1,5)$. The only divisor of 4 which is congruent to 1 modulo 5 is 1 itself, so the Sylow 5-subgroup of $\mathrm{Aff}(1,5)$ is normal. Since this group permutes five objects, it must be contained in S_5. Thus we have a group of order 20, contained in S_5 and normalizing a subgroup of order 5, so it must be the one we are looking for: that is, $N_5 \cong \mathrm{Aff}(1,5)$.

Second, consider $p = 3$. Again, Q_3 is cyclic of order 3. There are 20 elements of order 3, and hence 10 Sylow 3-subgroups. Therefore $|N_3| = 120/10 = 12$. If $Q = \langle(123)\rangle$ then $Q = (A_3 \text{ on } \{1,2,3\})$ so it it is clear that Q is a normal subgroup of $(S_3 \text{ on } \{1,2,3\}) \times \langle(45)\rangle$, so $N_3 \cong S_3 \times S_2$.

Finally, consider $p = 2$. $|Q_2| = 8$. The stabilizer of a point in S_5 is S_4, which contains groups isomorphic to D_8, of order 8, so again we must have $Q_2 \cong D_8$. There are 5 ways of choosing a point to miss out of the square, so there are $5 \times 3 = 15$ Sylow 2-subgroups. Therefore $|N_2| = 120/15 = 8 = |Q_2|$ and so $N_2 = Q_2$.

One more theorem about Sylow stuff

Theorem Let p be a prime. If P is a Sylow p-subgroup of a finite group G and $H = N(P)$ then $N(H) = H$. In words: Sylow normalizers are self-normalizing.

Proof If $g \in N(H)$ then $P^g \leqslant H$ so P^g is a Sylow p-subgroup of H. But $P \trianglelefteq H$, so P is the only Sylow p-subgroup of H, so $P^g = P$. Threfore $g \in N(P) = H$. This shows that $N(H) \leqslant H$. However, $H \leqslant N(H)$ for all subgroups H, and therefore $N(H) = H$. $\square$

You might like to verify this on the Sylow normalizers that we have just found.

Groups with orders 20–24

Now we shall use Sylow's Theorems to investigate groups of these orders.

Notation C_n denotes a cyclic group of order n.

If $|G| = 20$ then the Sylow 5-subgroup is normal and is isomorphic to C_5. Possibilities include

C_{20}**,** which has a single Sylow 2-subgroup, isomorphic to C_4;

D_{20}**,** which has five Sylow 2-subgroups, each isomorphic to the Klein group;

$\mathrm{Aff}(1,5)$**,** which has five Sylow 2-subgroups, each isomorphic to C_4.

If $|G| = 21$, then the Sylow-7 subgroup is normal and is isomorphic to C_7. The number of Sylow 3-subgroups is either 1 or 7. If the Sylow 3-subgroup is also normal then the group is isomorphic to C_{21}. In fact, there is another group of order 21 which has seven Sylow 3-subgroups.

If $|G| = 22$ then $G \cong C_{22}$ or $G \cong D_{22}$, because 11 is an odd prime.

If $|G| = 23$ then $G \cong C_{23}$, because 23 is prime.

If $|G| = 24 = 2^3.3$ then one of the following happens.

(i) The Sylow 3-subgroup is normal. Then there are various possiblities, including C_{24} and D_{24}.

(ii) There are four Sylow 3-subgroups and $|G : N_3| = 4$ so $|N_3| = 6$. Then there is a normal subgroup K of G, contained in N_3, such that G/K is isomorphic to a transitive subgroup of S_4. If $K = \{1_G\}$ then $G \cong S_4$. We cannot have K equal to the Sylow 3-subgroup Q_3 in N_3, because that is not normal in G. We cannot have $K = N_3$, because N_3 is not normal in G, by the theorem about Sylow normalizers. The only other possibility is that $|K| = 2$ and $G/K \cong A_4$.