

## A DIFFERENT PROOF OF SYLOW'S THEOREMS

### THE FIRST THEOREM OF SYLOW

The following slight variation of the proof of Theorem 5.1 in the Notes allows to refine the argument and obtain additional information.

**First theorem of Sylow.** *Let  $|G| = p^m r$ , where  $p$  is a prime and  $p \nmid r$ . Then  $G$  has a subgroup of order  $p^m$ .*

*Proof.* (Same proof as in Section 5 of the Notes, except for the last two sentences, to be replaced by the following.)

Since  $H$  is the stabilizer of  $H$  we have  $VH = V$ , that is,  $\bigcup_{v \in V} vH = V$ . Thus,  $V$  is a union of left cosets of  $H$  in  $G$ , and hence  $|V| = p^m$  is a multiple of  $|H|$ . However, since it was shown earlier that  $p^m$  divides  $|H|$  we conclude that  $|H| = p^m$  as desired.  $\square$

By continuing the argument we obtain the following strengthening of the above theorem (because  $n_p \equiv 1 \pmod{p}$  implies that  $n_p > 0$ ). In the treatment given in the Notes this comes later as part (5) of Theorem 5.7. We will also prove it again in the next section.

**Theorem.** *Let  $|G| = p^m r$ , where  $p$  is a prime and  $p \nmid r$ . Let  $n_p$  be the number of subgroups of  $G$  of order  $p^m$ . Then  $n_p \equiv 1 \pmod{p}$ .*

*Proof.* In the above proof we have shown that if  $V \in \mathbf{S}$  belongs to a  $G$ -orbit of length not divisible by  $p$  then  $V$  is a left coset of a subgroup of  $G$  of order  $p^m$ . Conversely, if  $P$  is a subgroup of  $G$  of order  $p^m$  then all left cosets of  $P$  in  $G$  are clearly stabilized by  $P$  in the action (actually, the stabilizer of any such coset *equals*  $P$ ), and so belong to  $G$ -orbits of length prime to  $p$ , because of the orbit-stabilizer theorem and because  $p \nmid |G : P| = r$  (actually each such orbit will have length *exactly*  $r$ ). Hence the set  $\mathbf{S}'$  of elements of  $\mathbf{S}$  whose orbit has length not a multiple of  $p$  coincides with the set of left cosets of subgroups of  $G$  of order  $p^m$ . Since the latter has cardinality  $r n_p$  we have  $r n_p = |\mathbf{S}'| \equiv |\mathbf{S}| \pmod{p}$ . If are willing to use the information that  $|\mathbf{S}| = \binom{p^m r}{p^m} \equiv r \pmod{p}$  (see the Lemma below) we obtain the desired conclusion that  $n_p \equiv 1 \pmod{p}$ . But we can also avoid that and proceed as follows.

We have shown that  $r n_p \equiv |\mathbf{S}| \pmod{p}$ . However,  $|\mathbf{S}|$  does not depend on the particular group of order  $p^m r$  under consideration (in fact, it equals  $\binom{|G|}{p^m}$ , which depends only on the order of  $G$ ). Hence the value of  $r n_p$  modulo  $p$  does not depend on the particular group  $G$  but only on its order  $p^m r$ , and we may as well compute that for our favorite group of that order. Taking as  $G$  the cyclic group of order  $p^m r$  we find that  $r n_p \equiv r \pmod{p}$ , because  $n_p = 1$  for that group. Therefore, it must be  $r n_p \equiv r \pmod{p}$  for any group  $G$  of order  $p^m r$ , and we conclude that  $n_p \equiv 1 \pmod{p}$ .  $\square$

In the above proof we have used (but then also shown how to avoid using) the following Lemma.

**Lemma.** *If  $p$  is a prime we have  $\binom{p^m r}{p^m} \equiv r \pmod{p}$  (whether  $p$  divides  $r$  or not).*

*Proof.* Recall that  $(a+b)^p = a^p + b^p$  in any commutative ring of characteristic  $p$ , because the binomial coefficients  $\binom{p}{i}$  are divisible by  $p$  for  $0 < i < p$ . More generally,  $(a+b)^{p^m} = a^{p^m} + b^{p^m}$  follows inductively. In particular, this holds in  $\mathbb{F}_p[x]$ , the polynomial ring over the field  $\mathbb{F}_p$  of  $p$  elements (thus,  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ). Consequently, we have

$$\sum_{i=0}^{p^m r} \binom{p^m r}{i} x^i = (1+x)^{p^m r} = (1+x^{p^m})^r = \sum_{j=0}^r \binom{r}{j} x^{p^m j}$$

in  $\mathbb{F}_p[x]$  (or in  $\mathbb{Z}[x]$  provided we replace the middle equality with a congruence modulo  $p$ ). We conclude that  $\binom{p^m r}{i} \equiv 0 \pmod{p}$  if  $p^m \nmid i$ , and that  $\binom{p^m r}{p^m j} \equiv \binom{r}{j} \pmod{p}$ , of which the desired conclusion is a special case.  $\square$

As in the Notes, one obtains Corollary 5.2 as a consequence, and then one proves Theorem 5.3 and Corollary 5.5. Theorem 5.6 and 5.7, however, may be replaced by the next section.

*Remark.* Note that the case  $p = 2$  of Cauchy's Lemma admits a much easier proof: in a group of even order, pair together each element with its inverse and conclude that there is at least one element  $g$ , besides the identity element  $e$ , such that  $g^{-1} = g$ , that is,  $g^2 = e$ .

*Remark.* Some proofs of the first theorem of Sylow (the older ones) start with proving Cauchy's Lemma and then use that to prove Sylow's Theorem working by induction on  $G$ . That kind of proof produces Corollary 5.5 directly (of which Theorem 5.1 is a special case).

## THE SECOND THEOREM OF SYLOW

The main difference in the following proof of the second theorem of Sylow (which is adapted from the book of N. Jacobson, Basic Algebra I, 1974) from that given in the Notes of the module is that here we focus on the subgroups of  $G$  of order  $p^m$  while the Notes focus on the  $p$ -subgroups of  $G$  (which by now we know to have order a power of  $p$ ) which are not contained in any larger one. (Following this approach we would like to take the former as the definition *Sylow  $p$ -subgroups* of  $G$ , as some textbooks do, but we will not do that to avoid confusion with the Notes, which take the latter.) Clearly a subgroup of  $G$  of order  $p^m$  has the property of not being contained in a larger  $p$ -subgroup, because of Lagrange's theorem. The two properties will eventually be seen to be equivalent, but the difference in focus affects the order in which the various facts are proved, although the arguments are similar. Both proofs are based on the action of  $G$  by conjugation on the set of subgroups of order  $p^m$  (rather than by right multiplication on the set of subsets of cardinality  $p^m$  as in the previous section).

We start with a Lemma concerning the normalizer of a subgroup of order  $p^m$ . Recall that the normalizer  $N_G(H)$  of a subgroup  $H$  of  $G$  is defined as

$N_G(H) := \{g \in G : H^g = H\}$ . This is the stabilizer of the subgroup  $H$  in the action of  $G$  by conjugation on the set of its subsets (that is, on  $\mathcal{P}(G)$ ). Note that this is different from the *centralizer* of  $H$  in  $G$ , which is defined as  $C_G(H) := \{g \in G : h^g = h \text{ for all } h \in H\} = \bigcap_{h \in H} C_G(h)$ . Certainly  $C_G(H) \leq N_G(H)$ , but  $N_G(H)$  always contains  $H$  while  $C_G(H)$  does exactly when  $H$  is abelian. Also note that  $H \trianglelefteq N_G(H)$ , in fact  $N_G(H)$  is the largest subgroup of  $G$  of which  $H$  is a normal subgroup.

**Lemma.** *Let  $|G| = p^m r$ , where  $p$  is a prime and  $p \nmid r$ . Let  $P$  be a subgroup of  $G$  of order  $p^m$  and let  $H$  be any  $p$ -subgroup of  $G$  contained in  $N_G(P)$ . Then  $H \leq P$ .*

*Proof.* (Recall from the previous section that  $H$ , as any finite  $p$ -group, has order a power of  $p$ .) Since  $H$  is a subgroup of  $N_G(P)$  and  $P$  is a normal subgroup of  $N_G(P)$  it follows that  $HP$  is also a subgroup, and  $HP/P \cong H/(H \cap P)$  by the second isomorphism theorem. Hence  $HP$  is isomorphic to a quotient group of  $H$ , and so has order a power of  $p$ . However,  $|HP| = |HP : P| \cdot |P|$  and  $|P| = p^m$  is the largest power of  $p$  which divides  $|G|$ . Hence  $|HP : P| = 1$  and so  $H \leq P$ .  $\square$

**Second theorem of Sylow.** *Let  $|G| = p^m r$ , where  $p$  is a prime and  $p \nmid r$ .*

- (1) *Any two subgroups of  $G$  of order  $p^m$  are conjugate.*
- (2) *The number of subgroups of  $G$  of order  $p^m$  is a divisor of the index in  $G$  of any of them (that is, of  $r$ ) and is congruent to 1 modulo  $p$ .*
- (3) *Any  $p$ -subgroup of  $G$  is contained in one of order  $p^m$ .*

*Proof.* Let  $\Pi$  be the set of subgroups of  $G$  of order  $p^m$ . According to the first theorem of Sylow  $\Pi$  is not empty. Let  $G$  act on  $\Pi$  by conjugation and let  $\Sigma$  be one of the orbits of this action. (We want to show that  $\Sigma = \Pi$ .) If  $P \in \Pi$  we can restrict the action of  $G$  on  $\Sigma$  to  $P$  and decompose  $\Sigma$  into  $P$ -orbits. Each one of these has cardinality length (cardinality) a power of  $p$  because it divides  $|P| = p^m$ .

Suppose that  $\Sigma$  contains a  $P$ -orbit  $\{P'\}$  of length one. Then  $P \leq N_G(P')$  and so  $P \leq P'$  by the Lemma. But then  $P' = P$  because they have the same order. Hence if  $P \in \Sigma$  then  $\{P\}$ , which is a  $P$ -orbit of length one, is the only one with this property. Since all other  $P$ -orbits in  $\Sigma$  have length multiple of  $p$  we have  $|\Sigma| \equiv 1 \pmod{p}$ . Similarly, if  $P \notin \Sigma$  then all  $P$ -orbits in  $\Sigma$  have length multiple of  $p$ , and so  $|\Sigma| \equiv 0 \pmod{p}$ . Since  $P \in \Pi$  was arbitrary  $|\Sigma|$  should satisfy both conclusion, which is a contradiction unless there is only one orbit and  $\Sigma = \Pi$ . This proves (1), and also that  $|\Pi| \equiv 1 \pmod{p}$ , which is part of (2). The other part of (2), that  $|\Pi|$  divides  $|G : P|$ , also follows because  $|\Pi| = |G : N_G(P)|$  and  $P \leq N_G(P)$ .

Now let  $H$  be a  $p$ -subgroup of  $G$ , hence of order a power of  $p$ , and restrict the action of  $G$  on  $\Pi$  to  $H$ . Since each  $H$ -orbit has length a power of  $p$  and  $|\Pi| \equiv 1 \pmod{p}$ , there exists at least one orbit  $\{P\}$  of length one. Then  $H \leq N_G(P)$ , and so  $H \leq P$ , again by the Lemma.  $\square$

*Remark.* One can also generalize statement (2) of the Theorem and prove (but we will not) that the number of subgroups of  $G$  order  $p^k$  is congruent to 1 modulo  $p$ , for any  $0 \leq k \leq m$ . Note that, unlike Sylow's theorems, this statement is nontrivial even for  $G$  a  $p$ -group.