

## 6. SYLOW THEOREMS

This proof is from Alperin and Bell “Groups and representations.”

**Lemma 6.1.** *If  $p \nmid m$  then*

$$\binom{p^k m}{p^k} \equiv m \pmod{p}$$

**Remark 6.2.** *Alperin and Bell do not bother to prove this lemma. Instead they make the following bizarre logical argument. They show that the truth value of Lemma 6.1 is equal to the truth value of the Sylow theorems for any group  $G$  with  $p^k m$  elements. Since the Sylow theorems are true for the cyclic group of order  $p^k m$ , Lemma 6.1 must be true and therefore the Sylow theorems hold for all finite groups!!*

*Proof.* The binomial coefficient theorem says

$$(1+x)^p = 1 + px + \binom{p}{2}x^2 + \binom{p}{3}x^3 + \cdots + px^{p-1} + x^p.$$

Modulo  $p$  this gives the formula  $(1+x)^p \equiv 1^p + x^p = 1 + x^p$ . By induction on  $k$  this gives

$$(1+x)^{p^k} \equiv 1 + x^{p^k}$$

Raising both sides of this equation to the  $m$ th power we get:

$$(1+x)^{p^k m} \equiv (1+x^{p^k})^m = 1 + mx^{p^k} + \binom{m}{2}x^{2p^k} + \cdots$$

The coefficient of  $x^{p^k}$  on the left is  $\binom{p^k m}{p^k}$ . This must be congruent to the corresponding coefficient on the right which is  $m$ .  $\square$

**Lemma 6.3.** *Suppose that  $N$  is a normal subgroup of a finite group  $G$  and  $p \nmid |G:N|$ . Then  $N$  contains every  $p$ -subgroup of  $G$ .*

**Remark 6.4.** *In particular this means that a  $p$ -subgroup  $Q$  of  $G$  can normalize a  $p$ -Sylow subgroup  $P$  only if  $Q \leq P$ . [Since  $P \trianglelefteq N(P)$  and  $p \nmid |N(P):P|$ .]*

*Proof.* Suppose not. Then  $G$  contains a  $p$ -subgroup  $P$  so that  $P \not\leq N \cap P$ . Then

$$\frac{PN}{N} \cong \frac{P}{N \cap P}$$

is a nontrivial  $p$ -subgroup of  $G/N$ . So  $p$  divides  $|G/N|$ .  $\square$

**Lemma 6.5.** *Suppose that  $P$  is a  $p$ -group acting on a finite set  $X$ . Then the number of elements of  $X$  is congruent mod  $p$  to the number of fixed points of the action of  $P$  on  $X$ .*

*Proof.* The size of the orbit  $Px$  of any  $x \in X$  is equal to the index of its stabilizer  $P_x = \{g \in P \mid gx = x\}$  which must be a power of  $p$ :

$$|Px| = |P/P_x| = \frac{|P|}{|P_x|} = \frac{p^k}{p^\ell} = p^{k-\ell}$$

When  $x$  is not a fixed point this number is not 1 so it must be divisible by  $p$ . Thus  $p$  divides the number of non-fixed points in  $X$ . The lemma follows.  $\square$

**Theorem 6.6** (Sylow). *Suppose that  $G$  is a finite group of order  $p^k m$  where  $p \nmid m$ . Then*

- (1)  *$G$  contains a  $p$ -Sylow subgroup (i.e., a subgroup  $P$  of order  $p^k$ ) and every  $p$ -subgroup of  $G$  is contained in some  $p$ -Sylow subgroup of  $G$ .*
- (2) *Any two  $p$ -Sylow subgroups of  $G$  are conjugate.*
- (3) *The set  $\mathcal{P}$  of  $p$ -Sylow subgroups of  $G$  has  $|\mathcal{P}| \equiv 1 \pmod{p}$  elements.*

*Proof.* Let  $\mathcal{X}$  be the set of all subsets  $X \subseteq G$  with  $|X| = p^k$  elements. Then  $\mathcal{X}$  has

$$|\mathcal{X}| = \binom{p^k m}{p^k} \equiv m \pmod{p}$$

number of elements by Lemma 6.1. Note that  $\mathcal{P} \subseteq \mathcal{X}$ , i.e., every Sylow- $p$ -subgroup is an element of  $\mathcal{X}$ .

There is a left action of  $G$  on  $\mathcal{X}$ :

$$\lambda_g(X) = \{gx \mid x \in X\} \in \mathcal{X}$$

The size of the orbit of  $X$  is given by the index of its stabilizer  $H = G_X$ :

$$|\text{orbit}(X)| = |G/H| = |G : H|$$

where

$$H = G_X = \{g \in G \mid gX = X\}$$

But

$$HX = \bigcup_{g \in H} gX = X = \bigcup_{x \in X} Hx$$

is a union of right cosets of  $H$  so  $|X| = p^k$  is a multiple of  $|H|$ . Thus  $|G_X| = |H| = p^\ell$  where  $\ell \leq k$ . Thus every stabilizer is a  $p$ -subgroup of  $G$ .

The number of elements in the orbit of  $X$  is:

$$|\text{orbit}(X)| = \frac{|G|}{|G_X|} = \frac{p^k m}{p^\ell} = mp^{k-\ell} \geq m$$

We will say that the orbit of  $X$  is *small* if it has exactly  $m$  element. Otherwise it is *large*. Large orbits have size divisible by  $p$ .

**Claim** The orbit of  $X$  is small if and only if  $X$  is a right coset of a  $p$ -Sylow subgroup of  $G$ .

*Proof:* For a small orbit, the stabilizer  $H = G_X$  is a  $p$ -Sylow subgroup of  $G$  and  $X$  is a right coset of  $H$ . Conversely, if  $H$  is a  $p$ -Sylow subgroup of  $G$  then  $Hg \in \mathcal{X}$  and  $G$  permutes these  $m$  right cosets of  $H$ . So the orbit of  $H$  is small and  $H$  is contained in the stabilizer. But the stabilizer is a  $p$ -subgroup of  $G$ . So, it must be equal to  $H$ .

Since each  $H \in \mathcal{P}$  gives a small orbit,  $|\mathcal{X}| = \binom{p^k m}{p^k}$  is congruent (mod  $p$ ) to  $m|\mathcal{P}|$ . Since  $m$  is invertible mod  $p$  this shows that  $|\mathcal{P}| \equiv 1 \pmod{p}$ . In particular  $\mathcal{P}$  is nonempty.

Suppose that  $Q$  is a  $p$ -subgroup of  $G$ . Then we want to find a  $P \in \mathcal{P}$  so that  $Q \leq P$ . The group  $Q$  acts on  $\mathcal{P}$  by conjugation. By Lemma 6.5 this action must have at least one fixed point  $P$ . Then  $Q$  normalizes  $P$  so  $Q \leq P$  by Remark 6.4.

It remains to show that the action of  $G$  on  $\mathcal{P}$  (by conjugation) is transitive, i.e., that  $\mathcal{P}$  is a single orbit of the  $G$ -action. If not then for every  $P \in \mathcal{P}$  there is a  $Q \in \mathcal{P}$  which is in a different orbit, i.e., is not conjugate to  $P$ . But the  $G$ -orbit of  $P$  is a disjoint union of  $Q$ -orbits each of which has no fixed points by Remark 6.4. Thus every  $G$  orbit has a multiple of  $p$  elements and  $|\mathcal{P}|$  is a multiple of  $p$  which is a contradiction since it is  $\equiv 1 \pmod{p}$ .  $\square$

Alperin and Bell point out that their proof does not use Cauchy's Theorem which they derive as a corollary.

**Corollary 6.7** (Cauchy's Theorem). *If  $G$  is a finite group whose order  $|G|$  is divisible by a prime  $p$  then  $G$  has an element of order  $p$ .*

*Proof.* We know that  $G$  has at least one  $p$ -Sylow subgroup  $P$ . Take a nontrivial element  $g \in P$ . Since  $o(g)$  divides  $|P|$ ,  $o(g) = p^n$ . So,  $g^{p^{n-1}}$  is an element of  $G$  of order  $p$ .  $\square$

**Homework 3:** Due next Thursday.

(3.1) Show that every subgroup of  $G$  containing  $N(P)$  is self-normalizing.

(3.2) If  $K \trianglelefteq G$  and  $P$  is a Sylow subgroup of  $K$  then  $KN_G(P) = G$ . [This follows from the fact that all conjugates of  $P$  lie in  $K$ .]

(3.3) If each Sylow subgroup of  $G$  is normal then  $G$  is the product of its Sylow subgroups.

(3.4) Show that  $T(n, \mathbb{Z})$  is nilpotent.