4 Applications of the Sylow Theorems

We will look at the structure of groups $G$ of order $pq$ where $p, q$ are prime. There groups will be given by two generators $a, b$ of order $p, q$. [Recall that $G$ is generated by a set $S$ if no proper subgroup of $G$ contains $S$. We write $G = \langle S \rangle$.]

**Lemma 4.1.** Suppose that $G$ is generated by $a, b$ of order $n, m$ satisfying:

\[ bab^{-1} = a^r \]  

Then every element $g$ of $G$ can be written in the form $g = a^i b^j$ and

\[ (a^i b^k)(a^j b^\ell) = a^{i+j} b^{k+\ell} \]  

Furthermore, the expression $g = a^i b^j$ is unique (i.e., $i, j$ are uniquely determined modulo $n, m$ resp.) assuming that $\langle a \rangle$ and $\langle b \rangle$ are disjoint (i.e., no nontrivial power of $a$ is equal to a nontrivial power of $b$).

**Remark 4.2.** I underlined the word “suppose” because there is no guarantee that there exists a group $G$ with elements $a, b$ satisfying (1). For example $r = n$ is not possible since $bab^{-1}$ has the same order as $a$. In order to show that $G$ exists we have to actually construct the group $G$.

**Proof.** Equation (2) implies that the set of all elements of $G$ of the form $a^i b^j$ forms a subgroup. Since $a, b$ generate $G$ this subgroup is all of $G$. But (2) follows from (1):

\[ bab^{-1} = a^r \Rightarrow b^k ab^{-k} = a^r \Rightarrow b^k a^i b^{-k} = a^r b^k \Rightarrow b^k a^j = a^{i+j} b^k \]

The uniqueness follows from the fact that $a^i b^k = a^i b^\ell \Leftrightarrow a^{i-j} = b^{\ell-k}$.

**Definition 4.3.** For $n \geq 3$ the dihedral group $D_{2n}$ is defined to be the group generated by $s, t$ so that $s^n = t^2 = 1$ and $tst = s^{-1}$. Thus by Lemma 4.1

\[ D_{2n} = \{1, s, s^2, \ldots, s^{n-1}, t, st, s^2 t, \ldots, s^{n-1} t\} \]

with multiplication rule given by:

\[ (s^j t^k)(s^j t^\ell) = s^{ij} t^{k+\ell} \]

where the sign of $j$ is $(-1)^k$.

**Theorem 4.4.** Every nonabelian group $G$ of order $2p$ (where $p$ is an odd prime) is dihedral.
Proof. Let $P$ be a $p$-Sylow subgroup of $G$. Then $P \triangleleft G$ since it has index 2. Let $a \in P$ be a generator (so $a$ has order $p$) and let $b \in G$ be an element of order 2. Since $P$ is normal, $bab^{-1} = a^r$ for some $r$ not divisible by $p$. Since $b^2 = 1$ we must have $r^2 \equiv 1 \pmod{p}$ so $r = \pm 1$. Since $G$ is not abelian we must have $r = -1$ and $G \cong D_{2p}$. □

We want to generalize Definition 4.3 and the above theorem to groups of order $pq$ where $p > q$ are prime. We will give a rigorous construction of $G$ in order to avoid the criticism of Remark 4.2.

Assume that $p \equiv 1 \pmod{q}$. Then $q$ divides the order $(p - 1)$ of the multiplicative group of units $F_q^\times$ of the field $F_p = \mathbb{Z}/p$. Consequently, by Cauchy, $F_q^\times$ contains an element of order $q$, i.e., a number $r$ so that

$$r^q \equiv 1, \quad r \not\equiv 1 \pmod{p} \quad (3)$$

Let $\alpha, \beta : F_p \to F_p$ be the set mappings given by $\alpha(x) = x + 1$ and $\beta(x) = rx$. Then $\alpha, \beta$ are permutations of $F$ since $\alpha^p = 1 = \beta^g$ and the following calculation shows that $\beta \alpha \beta^{-1} = \alpha^r$.

$$\beta \alpha \beta^{-1}(x) = \beta \alpha(x/r) = \beta(x/r + 1) = r(x/r + 1) = x + r = \alpha^r(x)$$

Consequently, by Lemma 4.1, the permutations $\alpha, \beta$ generate a subgroup of order $pq$ in the permutation group on $F_p$. Since it depends only on $p, q, r$ we will call this group $G(p, q, r)$. This is a nonabelian group of order $pq$ where $p > q$ are prime and $r$ satisfies (3) above.

**Theorem 4.5.** Let $p > q$ be primes. Then

1. There exists a nonabelian group of order $pq$ iff $p \equiv 1 \pmod{q}$.

2. Any two nonabelian groups of order $pq$ are isomorphic.

Proof. Let $G$ be a group of order $pq$ and let $P$ be the $p$-Sylow subgroup of $G$. Then $P \leq N(P) \leq G$ so $N(P)$ is either equal to $P$ or $G$. But $N(P) = P$ is not possible since the index of $N(P)$ must be congruent to 1 modulo $p$ by the Sylow theorems. Therefore $N(P) = G$ and $P \triangleleft G$. Similarly the $q$-Sylow subgroup $Q$ of $G$ will be normal in $G$ if $q$ does not divide $p - 1$. This will imply that $G = P \times Q$ which is abelian. This proves (1).

To prove the second statement suppose that $G$ is nonabelian. Then $Q \not\triangleleft G$. Let $a, b$ be generators of $P, Q$. Then $bab^{-1} = a^r$ for some $r$ not divisible by $p$. Also since $b^2 = 1$ we must have $r^q \equiv 1 \pmod{p}$ (and $r \not\equiv 1$ since $G$ is nonabelian). Thus $G$ is isomorphic to $G(p, q, r)$ for some $r$ satisfying (3).

---

1. Since $\mathbb{Z}/p$ is a field, the polynomial equation $x^2 = 1$ can have at most two solutions in $\mathbb{Z}/p$. 

---
It remains to show that $G(p, q, r) \cong G(p, q, s)$ if $s$ is another nontrivial solution of the congruence $x^q \equiv 1 \mod p$. However, the solutions of this equation are given by $x = r^i$ for $i = 1, 2, \ldots, q$ so $s = r^i$ for some $1 \leq i \leq q - 1$. But then an isomorphism $\phi : G(p, q, s) \to G(p, q, r)$ is given by $\phi(\alpha) = \alpha$, $\phi(\beta) = \beta^i$. [Then $\phi(\beta \alpha \beta^{-1}) = \beta^i \alpha \beta^{-i} = \alpha^{r^i} = \alpha^s = \phi(\alpha^s)$].

Now we will look at groups $G$ of order $p^2q$.

**Theorem 4.6.** Every group of order $p^2q$ with $p, q$ prime has a normal Sylow subgroup.

**Proof.** Let $P$ (resp. $Q$) be a $p$-Sylow subgroup (resp. $q$-Sylow subgroup) of $G$. Then we want to show that either $P \triangleleft G$ or $Q \triangleleft G$.

Case 1. Suppose that $q \not\equiv 1 \mod p$. Then $P \triangleleft G$ since $|G : N(P)| \equiv 1 \mod p$.

Case 2. Suppose that $p^2 \not\equiv 1 \mod q$. Then $p \not\equiv 1 \mod q$. Consequently, $|G : N(Q)| \neq p, p^2$ so $|G : N(Q)| = 1$ making $Q \triangleleft G$.

Case 3. The remaining case ($q \equiv 1 \mod p$ and $p^2 \equiv 1 \mod q$) is only possible when $p = 2$ and $q = 3$. If $Q$ is not normal in $G$ then $G$ must have four 3-Sylow subgroups giving 8 elements of order 3. The remaining $12 - 8 = 4$ elements must be $P$ forcing $P$ to be normal in $G$. 

Rotman has more to say about groups of order 12.

**Theorem 4.7.** Let $G$ be a group of order 12. Then either

(a) $G$ has a normal 3-Sylow subgroup, in which case $G$ has an element of order 6 or

(b) $G \cong A_4$ which has a normal 2-Sylow subgroup.

**Proof.** Let $Q = \{1, a, a^2\}$ be a 3-Sylow subgroup of $G$.

(a) Suppose first that $Q \triangleleft G$. Then $a, a^2$ are the only elements of $G$ of order 3 so the centralizer $C(a)$ of $a$ has index 1 or 2 so $|C(a)| = 6$ or 12. In either case $C(a)$ contains an element $b$ of order 2. Then $ab$ has order 6 since $a, b$ commute.

(b) If $Q \not\triangleleft G$ then $Q$ must be self-normalizing and the number of 3-Sylow subgroups must be 4. The group $G$ acts on the set of 3-Sylow subgroups by conjugation giving a homomorphism

$$\phi : G \to S_4$$

We know that 3-Sylow subgroup cannot normalize each other. Therefore, $\phi(a)$ fixes $Q$ and cyclically permutes the other three 3-Sylow subgroups of $G$ (making them even permutations). Since the 3-Sylow subgroups generate $G$, the image of $\phi$ lies in $A_4$. Also $\phi$ is a monomorphism since each 3-Sylow subgroup is self-normalizing so there is no nontrivial element of $G$ which normalizes all of them. 

---

2If the four 3-Sylow subgroups of $G$ are all contained in a subgroup $H \leq G$ then $|H : N_H(Q)| = 4$ which implies that $|H|$ is divisible by 4. Since $Q \leq H$, $|H|$ is also divisible by 3 so $|H| = 12$ and $H = G$. 

3