Sylow's Theorem

The term "modern algebra" principally refers to abstract theories in which the objects of study are assumed to satisfy certain basic rules, or axioms, but are otherwise undefined. Its prominence stems from the discovery of many examples of mathematical objects of different kinds that obey the same abstract rules, leading to the development of axiomatic theories with many different applications. This style of algebra has been pre-eminent since the 1920's; so, roughly speaking, "modern algebra" means 20th century algebra.

While group theory is the primary example of an abstract algebraic theory, it arose somewhat earlier than other parts of abstract algebra, being an invention of 19th century mathematics. In this week's lectures we shall look at one of the most famous theorems of finite group theory, discovered in 1872 by the Norwegian mathematician Ludwig Sylow.

Theorem. *Let G be a finite group and p a prime number. Let $\#G = p^k m$ where m is not divisible by p (so that p^k is the highest power of p that is a factor of $\#G$). Then G has a subgroup of order p^k. Moreover, if we define d to be the number of subgroups of G of order p^k then d is a divisor of m and $d \equiv 1$ (mod p).*

Recall that $d \equiv 1 \pmod{p}$ means that d is 1 more than a multiple of p; that is, $d = 1 + Np$ for some integer N.

To illustrate what Sylow's Theorem says, let us suppose that G is a finite group of order 56, and let $p = 7$ (a prime number). We have $56 = 7 \times 8$, and 8 is not divisible by 7. So G has at least one subgroup with 7 elements. Furthermore, if d is the number of such subgroups then d must be a divisor of 8 and must also be congruent to 1 modulo 7. The divisors of 8 are 1, 2, 4 and 8, and of these numbers only 1 and 8 are congruent to 1 modulo 7. So a group of order 56 must have a unique subgroup of order 7 or eight subgroups of order 7.

Since 2 is also a prime number we can equally well apply Sylow's Theorem with $\#G = 56$ and $p = 2$. This time we write $56 = 2^3 \times 7$, observing that 7 is not divisible by 2, and conclude that G has at least one subgroup of order 8. Moreover, the number of subgroups of order 8 must be a divisor of 7 and must be congruent to 1 modulo 2. The divisors of 7 are 1 and 7, both of which are congruent to 1 modulo 2. So a group of order 56 must either have exactly one subgroup of order 8 or exactly seven subgroups of order 8.

For another example, suppose that $\#G = 24 = 3 \times 8$. Applying Sylow's Theorem with $p = 3$ we see that G must have at least one subgroup of order 3; moreover, if d is the number of subgroups of order 3 then d is a divisor of 8 and $d \equiv 1 \pmod{3}$. The divisors of 8 are 1, 2, 4 and 8; of these, only 1 and 4 are congruent to 1 modulo 3. So G either has 1 subgroup of order 3 or four subgroups of order 3. Similarly, if we apply Sylow's Theorem with $p = 2$ then, since $24 = 2^3 \times 3$, the conclusion is that G has d subgroups of order 8, where $d = 1$ or $d = 3$.

We remark that when Sylow's Theorem is applied with $p = 2$ the condition that $d \equiv 1 \pmod{p}$ never gives us any new information. We have $\#G = 2^k m$, where m is an odd number, and we know that d has to be a divisor of m. Since all divisors of an odd number are odd, all the divisors of m will necessarily satisfy the requirement of being congruent to 1 modulo 2. However, when $p > 2$, and particularly when p is large, the fact that $d \equiv 1 \pmod{p}$ is often very useful.

For a final example, suppose that $\#G = 720$. Observe that $720 = 3^2 \cdot 80$, and 80 is not divisible by 3. By Sylow's Theorem, applied with $p = 3$, it follows that G has a subgroup of order 9. The divisors of 80 that are congruent to 1 modulo 3 are 1, 4, 10, 16 and 40. So the number of subgroups of order 9 must be one of these numbers. Similarly, since $720 = 2^4 \cdot 45$, Sylow's Theorem applied with $p = 2$ says that G has a subgroup of order 16, the number of such subgroups being a divisor of 45. And an application of Sylow's Theorem with $p = 5$ guarantees that G has 1, 6, 16 or 36 subgroups of order 5.

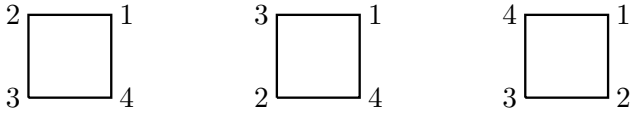
One can also apply Sylow's Theorem with p a prime number that is not a divisor of $\#G$, but doing so nevers tells us anything that was not already obvious. If p does not divide $\#G$ then p^0 is the highest power of p that is a divisor of $\#G$; so Sylow's Theorem tells us that G has a subgroup of order p^0. But $p^0 = 1$, and we know that every group G has exactly one subgroup of order 1. Indeed, since a subgroup of G must always contain e, the identity element of G, a subgroup of order 1 must consist of e and nothing else. It is easily checked that the subset $\{e\}$ satisfies SG1, SG2 and SG3, and is therefore, in all cases, the unique subgroup of G of order 1. (The condition that $d \equiv 1 \pmod{p}$ is satisfied, of course, since $d = 1$.)

Let us now consider the specific group $G = \mathrm{Sym}(4)$, the group of all permutations of 1, 2, 3, 4. Since we have already done some investigations of subgroups of this group, we should be able to verify that Sylow's theorem is consistent with what we know, and perhaps also gain some more information.

The group Sym(4) has 24 elements. We have seen that the set

$$\{\mathrm{id}, (1\,2\,3\,4), (1\,4\,3\,2), (1\,3)(2\,4), (1\,3), (2\,4), (1\,2)(3\,4), (1\,4)(2\,3)\}$$

a subgroup of Sym(4) of order 8; this confirms one of the conclusions of Sylow's Theorem. Recall that we obtained the subgroup above by considering the symmetries of a square with vertices numbered 1, 2, 3 and 4. But we can choose the numbering of the vertices in more than one way, and different choices may in fact give us different groups. Indeed, consider the following three alternative numberings.



For the first of these choices, the group of symmetries is that given above. The second numbering gives

$$\{\mathrm{id}, (1\,3\,2\,4), (1\,4\,2\,3), (1\,2)(3\,4), (1\,2), (3\,4), (1\,3)(2\,4), (1\,4)(3\,2)\}$$

as the group of symmetries, while the third numbering gives

$$\{\mathrm{id}, (1\,3\,4\,2), (1\,2\,4\,3), (1\,4)(3\,2), (1\,4), (3\,2), (1\,3)(2\,4), (1\,2)(3\,4)\}.$$

So Sym(4) has at least three distinct subgroups of order 8. But we saw above that, by Sylow's Theorem, a group of order 24 either has exactly one subgroup of order 8 or exactly three subgroups of order 8. So for Sym(4) we must have the latter alternative: Sylow's Theorem tells us that the above three subgroups of order 8 are the only subgroups of Sym(4) of order 8.

Now consider $p = 3$. In Sym(4) there are several 3-cycles, such as $(1\,2\,3)$; these are elements of order 3. Now if g is any element of any group then the set of all powers of g is a subgroup, usually denoted by $\langle g \rangle$. (Recall that this subgroup is known as the *cyclic subgroup generated by* g.) It is easily checked that

$$\langle (1\,2\,3) \rangle = \{\mathrm{id}, (1\,2\,3), (1\,3\,2)\},$$

a subgroup of order 3. Other 3-cycles will similarly generate subgroups of order 3. Now there are eight 3-cycles altogether: there are 4 ways to choose the numbers to go in the cycle (since one of 1, 2, 3 or 4 is to be left out) and then two possible cyclic orderings for the numbers that are chosen. The eight 3-cycles are, in fact, $(1\,2\,3)$, $(1\,3\,2)$, $(1\,2\,4)$, $(1\,4\,2)$, $(1\,3\,4)$, $(1\,4\,3)$, $(2\,3\,4)$ and $(2\,4\,3)$, and we see that

$$\begin{aligned}
\langle (1\,2\,3) \rangle &= \langle (1\,3\,2) \rangle = \{\mathrm{id}, (1\,2\,3), (1\,3\,2)\}, \\
\langle (1\,2\,4) \rangle &= \langle (1\,4\,2) \rangle = \{\mathrm{id}, (1\,2\,4), (1\,4\,2)\}, \\
\langle (2\,3\,4) \rangle &= \langle (2\,4\,3) \rangle = \{\mathrm{id}, (2\,3\,4), (2\,4\,3)\},
\end{aligned}$$

Thus Sym(4) has at least four subgroups of order 3. But we saw above that, by Sylow's Theorem, the number of subgroups of order 3 in a group of order 24 must be either 1 or 4. Thus Sym(4) must have exactly four subgroups of order 3: they are the ones listed above.

Rather than prove Sylow's Theorem in its full generality, we shall only prove it in some special cases. Specifically, we shall prove that any group of order 36 must have a subgroup of order 9. However, we shall use a method of proof that applies in general; essentially, the general proof just has variables where we shall have specific numbers.

The proof makes use of the following result, whose proof appears in the notes for Week 8.

Proposition. *Suppose that S is a nonempty subset of a group G, and suppose that no two distinct right translates of S have any elements in common. Then there exists a subgroup H of G and an element $g \in G$ such that $S = Hg$.*

Recall that a right translate of S is by definition a set of the form $Sg = \{\, xg \mid x \in S \,\}$, where g is in G. In the case that S is a subgroup the right translates of S are also called the right cosets of S. We have seen that the right cosets of a subgroup of G partition G, in the sense that distinct right cosets have no elements in common, and every element of G lies in some right coset. The above proposition is a converse to this.

Assume now that G is a group with $\#G = 36$. We need to prove that at least one of the $\binom{36}{9}$ subsets of G with nine elements is a subgroup of G. In fact, the number of these subsets that are subgroups is congruent to 1 modulo 3. The first thing to observe is that the number $\binom{36}{9}$ is not divisible by 3. Indeed,

$$\binom{36}{9} = \frac{36 \cdot 35 \cdot 34 \cdot 33 \cdot 32 \cdot 31 \cdot 30 \cdot 29 \cdot 28}{9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}$$

and the powers of 3 occurring as factors of numbers in the numerator of this expression are matched exactly by those occurring as factors of numbers in the denominator. For each i from 0 to 8, the highest power of 3 that is a factor of $36 - i$ is the same as the highest power of 3 that is a factor of $9 - i$. Cancelling all these 3's leaves

$$\binom{36}{9} = \frac{4 \cdot 35 \cdot 34 \cdot 11 \cdot 32 \cdot 31 \cdot 10 \cdot 29 \cdot 28}{1 \cdot 8 \cdot 7 \cdot 2 \cdot 5 \cdot 4 \cdot 1 \cdot 2 \cdot 1}$$

and given that this is an integer it is undoubtedly not divisible by 3, since the top line is not divisible by 3. The actual value is $94143280 = 3 \times 31381093 + 1$; so it is in fact congruent to 1 modulo 3.

Let $\mathscr{S}$ be the set of all 9-element subsets of G. We have just shown that $\#\mathscr{S}$ not divisible by 3. Now let us define a relation $\sim$ on $\mathscr{S}$ as follows: if $X, Y \in \mathscr{S}$ then $X \sim Y$ if and only if $X = Yg$ for some $g \in G$. That is, $X \sim Y$ if and only if X is a right translate of Y.

Lemma. *The relation $\sim$ is an equivalence relation on $\mathscr{S}$.*

Proof. Let e be the identity element of G. For all $X \in \mathscr{S}$ we have $X = Xe$, showing that X is a right translate of itself. So $X \sim X$ holds for all $X \in \mathscr{S}$; that is, $\sim$ is reflexive.

Let $X, Y \in \mathscr{S}$ with $X \sim Y$. Then $X = Yg$ for some $g \in G$, and it follows that $Xg^{-1} = Ygg^{-1} = Ye = Y$. Thus Y is a right translate of X whenever X is a right translate of Y; that is, $\sim$ is symmetric.

Let $X, Y, Z \in \mathscr{S}$ with $X \sim Y$ and $Y \sim Z$. Then $X = Yg$ and $Y = Zg'$ for some $g, g' \in G$, and it follows that $X = (Zg')g = Z(gg')$, whence $X \sim Z$. So $\sim$ is also transitive. □

So the 94143280 elements of $\mathscr{S}$ are divided into equivalence classes, two elements being in the same class if and only if they are right translates of each other. For each $X \in \mathscr{S}$, the equivalence class containing X consists of all subsets of G that are right translates of X.

Lemma. *Let X be a 9-element subset of G.*
(1) *Every element of G lies in some right translate of X.*
(2) *The number of right translates of X is at least four.*
(3) *If the number of right translates of X is exactly four then these translates are disjoint from each other.*

Proof. Let g be an arbitrary element of G, and choose an element $x_0 \in X$. Then $g = x_0 x_0^{-1} g \in X x_0^{-1} g$ (since $x_0 \in X$). So g is in the right translate $X x_0^{-1} g$ of X, and since g was arbitrary this shows that every element of G lies in some right translate of X.

Suppose that X has k right translates. Since they all have nine elements, the total number of elements in their union is at most $9k$, and it is exactly $9k$ if and only if the k right translates are disjoint from one another. But from the first part we know that the union of the translates is G, which has 36 elements. So $36 \leq 9k$, and $36 = 9k$ if and only if the translates are disjoint. That is, $k \geq 4$, and $k = 4$ if and only if the translates of X are disjoint, as claimed. □

Lemma. *If X is a 9-element subset of G then the number of right translates of X is 36, 18, 12, 9, 6 or 4, and if the number is 4 then X is a right coset of some subgroup.*

Proof. We showed in an earlier lecture that the number of right translates of any subset W of G is $\#G/\#\mathrm{Stab}(W)$, where $\mathrm{Stab}(W) = \{ g \in G \mid Wg = W \}$. So the number of right translates of X is $36/\#\mathrm{Stab}(X)$. The answer must be a whole number; so $\#\mathrm{Stab}(X)$ must be a divisor of 36, whence $36/\#\mathrm{Stab}(X)$ is also a divisor of 36. But we saw in the previous lemma that the number of right translates of X is at least 4, and since the divisors of 36 that are greater than or equal to 4 are precisely 36, 18, 12, 9, 6, and 4, we conclude that these are the only possibilities for the number of right translates of X. Furthermore, if the number of right translates is 4 then, as we proved in the previous

lemma, the translates are pairwise disjoint. And by the proposition we stated above, any nonempty subset whose translate are pairwise disjoint must be a coset of a subgroup of G; so the result is proved. □

Each equivalence class for the relation $\sim$ on $\mathscr{S}$ consists of the right translates of an 9-element subset, and so the number of elements in the equivalence class must be 36, 18, 12, 9, 6, or 4. The total number of elements in $\mathscr{S}$ is the sum of the numbers of elements in the various equivalence classes; so

$$\#\mathscr{S} = 36n_1 + 18n_2 + 12n_3 + 9n_4 + 6n_5 + 4n_6$$

for some nonnegative integers n_1, n_2, n_3, n_4, n_5 and n_6. But the right hand side above can be written as

$$3(12n_1 + 6n_2 + 4n_3 + 3n_4 + 2n_5 + n_6) + n_6,$$

which differs from n_6 by a multiple of 3. So $\#\mathscr{S} \equiv n_6 \pmod 3$. But we have seen that $\#\mathscr{S} = 94143280 \equiv 1 \pmod 3$; so we conclude that $n_6 \equiv 1 \pmod 3$. In particular, $n_6 \neq 0$; that is, there is at least one equivalence class with four elements. But as we have observed, the sets in such an equivalence class must be cosets of a subgroup. Each equivalence class with four elements consists of the four right cosets of a subgroup of order nine. So we conclude that there is at least one subgroup of order nine.

In fact, by applying the above steps a little more carefully we can show that the number of subgroups of order nine is congruent to 1 modulo 3. It is certainly true that the right cosets of any subgroup of order nine constitute an equivalence class with four elements, and every equivalence class with four elements consists of the cosets of a subgroup of order 9. So the number of subgroups of order 9 is precisely the number of equivalence classes with four elements. This is the number that was called n_6 above, and we showed that $n_6 \equiv 1 \pmod 3$.

Let us now repeat the argument in greater generality, and show that if m is not a multiple of 3 then any group of order 9m must have a subgroup of order 9. It will be convenient to first prove an important but elementary fact about congruence modulo n. Recall first the definition:

$$a \equiv b \pmod n$$

if and only if

$$a - b = qn \quad \text{for some integer } q.$$

Here is the fact we wish to prove.

Lemma. *Let a, b, c and d be integers such that $a \equiv b \pmod n$ and $c \equiv d \pmod n$. Then $a + c \equiv b + d \pmod n$ and $ac \equiv bd \pmod n$.*

Proof. Since $a - b$ is a multiple of n there exists an integer q such that $a = b + qn$. Similarly, since $c - d$ is a multiple of n there exists an integer q' such that $c = d + q'n$. Now

$$a + c = (b + qn) + (d + q'n) = (b + d) + (q + q')n,$$

whence $(a + c) - (b + d)$ is a multiple of n, and similarly

$$ac = (b + qn)(d + q'n) = bd + qnd + bq'n + qnq'n = bd + (qd + bq' + qq'n)n,$$

whence $ac - bd$ is also a multiple of n. So $a + c \equiv b + d \pmod{n}$ and $ac \equiv bd \pmod{n}$, as required. □

The so-called *Fundamental Theorem of Arithmetic* states that every positive integer can be uniquely factorized as a product of prime numbers. We shall not prove this, as it would take us too far afield. Closely allied to the Fundamental Theorem of Arithmetic is the following result: if a and b are integers and p is a prime number that is a factor of the product ab then p is a factor of a or b (or both).

Lemma. *Suppose that p is a prime and a, b, c, d integers such that $ac \equiv bd \pmod{p}$ and $a \equiv b \not\equiv 0 \pmod{p}$. Then $c \equiv d \pmod{p}$.*

Proof. Since $a \equiv b \pmod{p}$ it follows that $ac \equiv bc \pmod{p}$. Since also $ac \equiv bd$, we have $bc \equiv bd \pmod{p}$. Thus $b(c - d) = bc - bd$ is a multiple of p. But p is prime, and b is not a factor of b (by the hypothesis that $b \not\equiv 0 \pmod{p}$); so b must be a factor of $c - d$. Thus $c \equiv d \pmod{p}$, as claimed. □

The next result is the first ingredient we require for the proof of Sylow's Theorem in the case we are concerned with.

Lemma. *Suppose that m is not a multiple of 3. Then $\binom{9m}{9} \equiv m \pmod{3}$.*

Proof. The formula for the binomial coefficients (which should be familiar from secondary school and junior level mathematics) gives $\binom{9m}{9} = \frac{(9m)!}{9!(9m-9)!}$. Cancelling $(9m - 9)!$ gives

$$\binom{9m}{9} = \frac{9m(9m-1)(9m-2)(9m-3)(9m-4)(9m-5)(9m-6)(9m-7)(9m-8)}{9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1},$$

and then cancelling factors of 3 gives

$$\binom{9m}{9} = \frac{m(9m-1)(9m-2)(3m-1)(9m-4)(9m-5)(3m-2)(9m-7)(9m-8)}{1 \cdot 8 \cdot 7 \cdot 2 \cdot 5 \cdot 4 \cdot 1 \cdot 2 \cdot 1}.$$

Write $A = (9m - 1)(9m - 2)(3m - 1)(9m - 4)(9m - 5)(3m - 2)(9m - 7)(9m - 8)$ and $B = 8 \cdot 7 \cdot 2 \cdot 5 \cdot 4 \cdot 1 \cdot 2 \cdot 1$, and observe that corresponding factors in these two products are congruent modulo 3. Thus $9m - 1 \equiv 8 \pmod{3}$, $9m - 2 \equiv 7 \pmod{3}$, $3m - 1 \equiv 2 \pmod{3}$, and so on. So $A \equiv B \pmod{3}$. None of factors of B are multiples of 3; so $B \not\equiv 0 \pmod{3}$. Now since

$$B\binom{9m}{9} = mA \pmod{3}$$

it follows from the last lemma above that we can cancel A and B from this expression, leaving $\binom{9m}{9} \equiv m$, as claimed. □

Now suppose that G is a finite group with $\#G = 9m$, where $m \not\equiv 0 \pmod{3}$. Let $\mathscr{S}$ be the set of all 9-element subsets of G, and for $X, Y \in \mathscr{S}$ define $X \sim Y$ if and only if X is a right translate of Y. Then $\sim$ is an equivalence relation on $\mathscr{S}$, and so $\mathscr{S}$ is the disjoint of $\sim$-equivalence classes:

$$\mathscr{S} = \mathscr{T}_1 \cup \mathscr{T}_2 \cup \cdots \cup \mathscr{T}_l \tag{1}$$

for some l, where each $\mathscr{T}_i$ consists of elements of $\mathscr{S}$ that are all right translates of one another.

If X is any element of $\mathscr{S}$ then all the right translates of X have 9 elements, and their union is the whole of G. Since $\#G = 9m$ it follows that the number of right translates of X must be at least m, and it is exactly m if and only if the translates are pairwise disjoint. We know that if the translates are pairwise disjoint then they are the cosets of a subgroup. Furthermore, the number of right translates of X is $\#G/\#\mathrm{Stab(X)}$, a divisor of $\#G$. So for each $\sim$-equivalence class $\mathscr{T}_i$ in Eq. (1) above, $\#\mathscr{T}_i$ is a divisor of $9m$ that is at least m, and equals m only if $\mathscr{T}_i$ consists of the right cosets of a subgroup of G of order 9.

We have assumed that m is not divisible by 3; so any divisor of $9m$ that is not divisible by 3 must be a divisor of m, and hence no bigger than m. So every divisor of $9m$ that exceeds m must be congruent to 0 modulo 3. By Eq. (1),

$$\#\mathscr{S} = \#\mathscr{T}_1 + \#\mathscr{T}_2 + \cdots + \#\mathscr{T}_l,$$

and each number $\#\mathscr{T}_i$ on the right hand side of this equation either equals m or is divisible by 3. So

$$\#\mathscr{S} \equiv Km \pmod 3, \tag{2}.$$

where K is the number of equivalence classes $\mathscr{T}_i$ that consist of right cosets of subgroups of G. That is, K is the number of subgroups of G of order 9. Now $\#\mathscr{S}$ is the number of 9-element subsets of a set with $9m$ elements, and this equals $\binom{9m}{9}$. So by Eq. (2) and the lemma,

$$Km \equiv \binom{9m}{m} \equiv m \pmod 3,$$

and since $m \not\equiv 0 \pmod 3$ we can cancel the m and conclude that $K \equiv 1 \pmod 3$. In particular, $K \neq 0$: a group of order $9m$ must have a nonzero number of subgroups of order 9.