10. SYLOW SUBGROUPS

§10.1. Sylow Subgroups

Let G be an abelian group written additively. If p is a prime then the Sylow p-subgroup is defined to be: $\mathbf{Syl_p(G)} = \{g \in G \mid p^n g = 0 \text{ for some } n\}$. It is easy to show that this is a subgroup.

Written multiplicatively it becomes

$$\{g \in G \mid g^{p^n} = 1 \text{ for some } n\}.$$

This is the set of all elements whose order is a power of p but if G is non-abelian this set is usually not a subgroup and has no significance.

Example 1: If $G = \mathbf{S}_3$ then $\{g \in G \mid g^{2^n} = 1 \text{ for some } n\} = \{I, (12), (13), (23)\}$, which is certainly not a subgroup.

If p is prime, a ***p*-group** is a group where the order of every element is a power of p. If G is a finite p-group then its order is a power of p. This is because, if |G| was divisible by any other prime, there would have to be an element of that order.

If G is a finite group and p^n is the largest power of p that divides |G| then, by Lagrange's Theorem, the largest possible order for a p-subgroup will be p^n. But Lagrange's Theorem does not guarantee that this maximum will be attained. However, it is indeed true, as I will show. If p^n is the largest power of p that divides |G|

then G has a subgroup (possibly many) of order p^n. They are called the **Sylow *p*-subgroups** of G, named after the Norwegian mathematician Ludwig Sylow [1832 – 1918].

The three Sylow theorems not only assert the existence of Sylow subgroups for all primes but also give information about the numbers of Sylow subgroups. We will not follow Sylow's original proofs, but instead use a proof due to Wielandt that uses the concept of groups acting on sets.

§10.2. Actions of Groups on Sets

If G is a group, a **G-set** is a set, X, together with a function $*: X \times G \to X$ such that:

(1) $x * 1 = x$ for all $x \in X$ and

(2) $(x * g) * h = x * (gh)$ for all $x \in X$ and $g, h \in G$.

If X is a G-set we say that G **acts** on the set X.

A G-set is a sort of primitive vector space. The underlying set is just a set, not an abelian group, and the scalars come from a group, not a field. Instead of writing $\lambda\mathbf{v}$ we write multiplication by a scalar as $\lambda * \mathbf{v}$. The fact that we have not so many axioms for a G-set as we do for a vector space reflects the fact that the set X has no

structure itself and the system of scalars here is a group, which has less structure than a field.

Another similar situation is where we have a representation of a group. Here the underlying structure is a vector space, while the scalars are the elements of a group.

The **stabiliser** of a subset Y of a G-set X is defined to be

$$\sigma(Y) = \{g \in G \mid y * g = x \text{ for all } y \in Y\}.$$

In the case where $Y = \{x\}$ we write $\sigma(x)$ instead of $\sigma(\{x\})$.

Example 2: Let $X = \{1, 2, 3, 4, 5, 6\}$ and $G = \mathbf{D}_8$.
Define $x * g$ as follows:

*	**1**	**A**	**A^2**	**A^3**	**B**	**AB**	**A^2B**	**A^3B**
1	1	2	1	2	6	3	6	3
2	2	1	2	1	3	6	3	6
3	3	6	3	6	2	1	2	1
4	4	4	4	4	5	5	5	5
5	5	5	5	5	4	4	4	4
6	6	3	6	3	1	2	1	2

$\sigma(1) = \{1, A^2\}$;
$\sigma(2) = \{1, A^2\}$;
$\sigma(3) = \{1, A^2\}$;
$\sigma(4) = \{1, A, A^2, A^3\}$;
$\sigma(5) = \{1, A, A^2, A^3\}$;
$\sigma(6) = \{1, A^2\}$;
$\sigma(X) = \{1, A^2\}$.

Theorem 1: (1) If X is a G-set and $Y \subseteq X$ then $\sigma(Y)$ is a subgroup of G.

(2) $\sigma(X) \trianglelefteq G$ and $G/\sigma(X)$ is isomorphic to a group of permutations on X.

Proof: The fact that $\sigma(Y)$ is a subgroup of G is easily checked.

If S(X) denotes the symmetric group (the group of all permutations) on X the function $\theta: G \to S(X)$ defined by $\theta(g)(x) = x * g$ is a group homomorphism whose kernel is $\sigma(X)$. The image is a subgroup of S(X). ☟☺

A G-set X is defined to be **faithful** if $\sigma(X)$ is trivial. Example 2 is an example of a **non faithful** (we never say 'unfaithful') G-set.

If X is a faithful G-set the group G is actually isomorphic to a group of permutations because $\sigma(X)$ is trivial. Think of the group of permutations as a 'faithful copy' of the group G, being isomorphic to it. If a G-set isn't faithful the group of permutations is a scaled down version of G, being isomorphic to $G/\sigma(X)$.

At the other extreme, a G-set X is defined to be **trivial** if $\sigma(X) = G$. Here $g * x = x$ for all $g \in G$ and all $x \in X$.

(This is similar to the trivial representation of a group.)

Theorem 2 (CAYLEY): Every finite group G is isomorphic to a group of permutations on G.

Proof: G acts on itself by defining $g * h = gh$ and the resulting G-set is faithful. (In other words, right multiplication by an element of G permutes the elements of G.) ✋☺

This action is called the **regular action** of G on G. It is similar to the regular representation.

Examples 3:

(1) The **conjugation action** of G on G defined by

$$x * g = x^g = g^{-1}xg.$$

(2) An **isometry** $f:\mathbb{R}^3 \to \mathbb{R}^3$ is a distance preserving transformation. They are maps of the form $f(\mathbf{x}) = A\mathbf{x} + \mathbf{b}$ where A is an orthogonal 3×3 matrix and $\mathbf{b} \in \mathbb{R}^3$. The set of all isometries of $\mathbb{R}^3$ form a group G under composition and we can think of $\mathbb{R}^3$ as a G-set with $f * \mathbf{v}$ defined as $f(\mathbf{v})$.

§10.3. Orbits

Suppose X is a G-set and let $x \in X$. The set of all those elements of X that can be reached from x by multiplying by some element of G is called the **orbit** containing x. In fact the relation ~ defined on X by $x \sim y$ if $x * g = y$ for some $g \in G$, is an equivalence relation and the equivalence classes are the orbits. We denote the orbit containing x by $\boldsymbol{x}^{\mathbf{G}}$. The set of orbits is denoted by **X/G**. A G-set is defined to be **transitive** if it has only one orbit.

Examples 4:

(1) If G is viewed as a G-set under the action of conjugation then the orbits are the conjugacy classes and the stabiliser of g is the centraliser $C_G(g)$.

(2) If $H \leq G$ then G can be viewed as an H-set under the action $g * h = gh$. The orbits are the right cosets of H and the stabiliser of g is the trivial subgroup.

Theorem 3: If G is finite and X is a G-set

$$\#x^G = |G : \sigma(x)|.$$

Proof: $x * g = x * h \leftrightarrow x * (gh^{-1}) = x$

$$\leftrightarrow gh^{-1} \in \sigma(x)$$

$$\leftrightarrow g\sigma(x) = h\sigma(x).$$

So $f(x * g) = g\sigma(x)$ is a well-defined 1-1 and onto map between the orbit of x and the set of right cosets of the stabiliser $\sigma(x)$. ✋☺

This generalises the result that says that the number of conjugates is the index of the centraliser.

Example 2 (continued):

The orbits are {1, 2, 3, 6} and {4, 5}.

So 2^G = {1, 2, 3, 6} and $\#2^G = 4$, $|\sigma(2)| = 2$, and $|G:\sigma(2)| = 4$. $\#4^G = 2 = |G : \sigma(2)|$.

§10.4. Cauchy's Theorem

Let X be a G-set. Then $\mathbf{X_G}$ is defined to be
$\{x \in X \mid x * g = x \text{ for all } g \in G\}$.

Example 5: Let $G = \mathbf{S}_3$ and $X = \{1, 2, 3, 4, 5\}$ where G acts on X in the natural way. Then since the symbols 4, 5 are always fixed by the elements of G and the others are not, $X_G = \{4, 5\}$.

Theorem 4: If G is a finite p-group and X is a finite G-set then $|X| \equiv |X_G| \pmod{p}$.
Proof: Suppose $|G| = p^n$ and let $x \in X$ and let x^G denote the orbit of x.
Then $p^n = |G| = |G:\sigma(x)|.|\sigma(x)| = |x^G|.|\sigma(x)|$.
Either $|x^G| = 1$ or $|x^G| \equiv 0 \pmod{p}$.
But $|x^G| = 1$ means that $x \in X_G$. Since X is the disjoint union of orbits the result follows. ✋☺

Corollary: If G is a finite p-group and X is a finite G-set whose size is not divisible by p then there exists an element $x \in X$ such that $x * g = x$ for all $g \in G$.

This gives another way of expressing the proof of Cauchy's theorem.

Theorem 5 (CAUCHY): If p is a prime divisor of |H| there exists an element of H of order p.
Proof: Apply the corollary to $G = \langle A \mid A^p \rangle$ and

X = {(g_1, ... , g_p) | each $g_i \in$ H with not all g_i = 1,
but the product $g_1 ... g_p = 1$}.
Then |X| = $|H|^{p-1} - 1$, which is not divisible by p.

The action of G on X is given by:

(g_1, ... , g_p) ∗ A = (g_2, ... , g_p, g_1).

By the corollary there exists (g_1, ... , g_p) with

(g_1, ... , g_p) ∗ A = (g_1, ... , g_p).

So $g_1 = g_2 = ... = g_p$. Call this g. Then $g^p = 1$. ✋☺

Example 6: If |G| = 105 = 3 × 5 × 7 there must be elements of orders 3, 5 and 7. And of course there's the identity with order 1. The other possible orders, by Lagrange's Theorem, are 15, 21, 35 and (only if G is cyclic) 105. But unlike 3, 5 and 7 there are no guarantees.

By Lagrange's Theorem, if |G| = p^n, where p is prime, the orders of the elements must be powers of p. The converse also holds. If, in a finite group, the orders of all the elements are powers of p then the order of the group must be a power of p. For if not, and q is a different prime divisor of the group order, there would have to be an element of order q.

Example 7: $\mathbf{A}_5$ has order 60 but has no subgroup of order 30, even though 30 divides 60 (but of course it isn't prime power). The reason why no such subgroup exists is because such a subgroup would have to be a normal

subgroup (subgroups of index 2 are normal) and $\mathbf{A}_5$ is simple.

§10.5. Normalisers

If $H \leq G$ and $g \in G$ we define

$$\mathbf{H^g} = g^{-1}Hg = \{g^{-1}hg \mid h \in H\}.$$

It is called the **conjugate of H by *g***. The **normaliser** of a subgroup $H \leq G$ is defined by

$$N_G(H) = \{g \mid H^g = H\}.$$

It is easily checked that $H \leq N_G(H) \leq G$, and in fact $N_G(H)$ is the largest subgroup in which H is normal. It is also obvious that $N_H(G)$ always contains Z(G).

Theorem 6: The number of conjugates of H in G is

$$|G : N_G(H)|.$$

Proof: Let $N = N_G(H)$, let X be the set of conjugates of H in G and let R be the set of left cosets N*g* in G. We define a function $f: R \to X$ by $f(Ng) = H^g$.

If $Ng_1 = Ng_2$ then $g_2 = bg_1$ for some $b \in N$.

Then $H^{g_2} = H^{bg_1} = H^{g_1}$. Hence *f* is well-defined.

If $H^{g_2} = H^{g_1}$ then $H^{g_2 g_1^{-1}} = H$ and so $g_2 g_1^{-1} \in N$.

Hence $Ng_1 = Ng_2$.

We have thus shown that *f* is 1-1.

Clearly *f* is onto. Hence $|X| = |R| = |G : N|$. ✋☺

A **maximal** subgroup of G is a subgroup H < G where there is no subgroup K for which H < K < G. **Minimal** subgroups are defined similarly. By Lagrange's Theorem subgroups of prime order are minimal. By Cauchy's Theorem the converse is true: minimal subgroups have prime order.

Also, by Lagrange's Theorem, subgroups of index p are maximal. Here the converse is not always true. A maximal subgroup may not have prime index. However, we'll show that it's true for finite p-groups.

For p-groups the converse of Lagrange's Theorem holds. If $|G| = p^n$ then G has subgroups of order p^r for all r with $0 \leq r \leq n$.

Example 8: If G = $\mathbf{S}_4$ and H = $\mathbf{S}_3$, fixing the symbol 4, then H has index 4 in G. However it is maximal. The reason is as follows. If K was a subgroup between H and G then |G:K| =2. So |K| = 12 and, having index 2 it would have to be normal in G. But the only normal subgroup of order 12 in $\mathbf{S}_4$ is $\mathbf{A}_4$ (example 17 of chapter 6), so K = $\mathbf{A}_4$. But H contains (123) and so isn't a subgroup of $\mathbf{A}_4$. So we get a contradiction.

The next theorem states that in a finite p-group the normaliser of a proper subgroup is always bigger than the subgroup itself. It gives us information about maximal subgroups of p-groups.

Theorem 7: If G is a finite p-group and $H < G$ then
$$H < N_G(H).$$
Proof: It is easily checked that $N_{G/K}(H/K) = N_G(H)/K$.
Let G be a minimal counter-example and let H be a subgroup of G where $N_G(H) = H$.
By the minimality, H contains no non-trivial normal subgroup of G. Since $N_G(H)$ contains Z(G) we get a contradiction. ✋☺

Corollary: In a *p*-group, subgroups of index *p* are normal.
Proof: By Lagrange's Theorem, a subgroup of index *p* must be maximal – that is, there is no subgroup strictly between it and the whole group. So if |G:H| is prime, $N_G(H) = G$, which is just another way of saying that H is normal. ✋☺

Theorem 8: If G is a finite *p*-group of order p^r then it has at least one subgroup of order p^s for every $s \leq r$.
Proof: Prove this by induction on *r*.
Suppose $|G| = p^{r+1}$ and $1 \leq s \leq r + 1$.
Since Z(G) is non-trivial it has a subgroup K of order *p*. (Abelian groups have subgroups of every possible order.)
Now subgroups of the centre are normal and so $|G/K| = p^r$. By induction G/K has a subgroup H/K of order p^{s-1} whence $|H| = p^s$. ✋☺

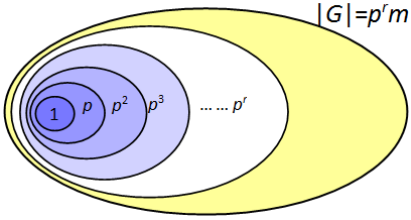
Corollary to Theorem 7: Maximal subgroups of *p*-groups are normal. ☺

§10.6. The Sylow Theorems

The following is one of a very famous trilogy of theorems first proved by the Norwegian mathematical Ludwig Sylow.

If $|G| = p^n m$ where p is prime and $(p, m) = 1$ a Sylow p-subgroup is one of order p^n. The following proof of their existence is due to Helmut Wielandt.

Theorem 8 (SYLOW'S FIRST THEOREM):
If $|G| = p^r m$, where p, m are coprime, then G has at least one subgroup of order p^s for all $s \leq r$.



Proof: Suppose $|G| = p^r m$ where p is prime.
Suppose that p is coprime to m and let X be the set of all subsets of size p^r. Then G acts on X by the action

$$S * g = Sg = \{sg \mid s \in S\}.$$

Now $\#X = \binom{p^r m}{p^r}$ which is coprime to p.
Hence for some $S \in X$, $\#S^G$ is coprime to p.

Let $P = \sigma(S)$ be the stabiliser of S. Then $|G:P|$ is coprime to p and hence p^r divides $|P|$.

Now if $s \in S$, $sP \subseteq S$ and so $|P| \leq p^r$. Hence $|P| = p^r$. Finally, since a p-group of order p^r contains at least one

subgroup of order p^s for all $s \leq r$, the same is true for G. ✋☺

Theorem 9 (SYLOW'S SECOND THEOREM):
The Sylow p-subgroups of a finite group G are conjugate to one another.

Proof: Let $|G| = p^n m$ where p does not divide m and where $n > 0$.

Let P be a Sylow p-subgroup of G.

So $|P| = p^n$ and $|G:P| = m$.

Let $P, Pg_2, \ldots, Pg_m$ be the left cosets of P.

Make $X = \{P, Pg_2, \ldots, Pg_m\}$ into a G-set by defining

$$(Pg_i) * g = P(g_i g).$$

There is just one orbit, the whole of X, and the stabilisers therefore have size p^n. In fact they are all conjugate, because if $g \in Pg_i$ then $g^{-1}Pg = \sigma(Pg_i)$ (the LHS is a subset of the RHS and they have the same size).

Let Q be another Sylow p-subgroup of G. Then X, the set of left cosets of P, can be regarded as a Q-set in the same way as above.

The size of at least one orbit of X under this action, say the one containing Pg_r, is not divisible by p.

Let $R = Q \cap \sigma(Pg_r)$.

This is the stabilizer of Pg_r under the Q-action.

Hence the size of the orbit divides p^n and so is 1.

It follows that R = Q and so $Q = \sigma(Pg_r) = g_r^{-1}Pg_r$. ✋☺

Theorem 10 (SYLOW'S THIRD THEOREM):
The number of Sylow p-subgroups of G is congruent to 1, modulo p, and divides m.
Proof: Let $|G| = p^n m$ where p does not divide m and where $n > 0$.
Let P be a Sylow p-subgroup of G.
So $|P| = p^n$ and $|G:P| = m$.
Let $N = N_G(P)$ and let Y be the set of left cosets of N in G. The number of Sylow p-subgroups is the number of conjugates of P, which is $|G:N|$.
Since $P \leq N$, $|G:N|$ divides m.
Let P act on Y as above. The sizes of the orbits are powers of p and, unless they are 1, they are multiples of p. So it remains to show that there is only one orbit of size 1.

Suppose $Ngx = Ng$ for all $x \in P$.

Then $gxg^{-1} \in N$ for all $x \in P$ and so $P^{g^{-1}} \leq N$.

Let $Q = P^{g^{-1}}$. Since $Q \leq N_G(P)$, $PQ \leq N_G(P)$.
Hence $PQ/P \cong Q/(P \cap Q)$.
It follows that $|PQ|$ is a power of p.
But, since P is a maximal p-subgroup of G, it follows that PQ = P, or in other words, P = Q.

Hence $P^{g^{-1}} = P$ and so $g \in N$.
So {N} is the only orbit of size 1. ✋☺

§10.7. Applications of Sylow's Theorems

Theorem 11: Suppose $|G| = p^a q^b$ where p, q are distinct primes with $p < q$ and $a \leq 2$. Then G has a normal Sylow q-subgroup.

Proof: Suppose Q is a Sylow q-subgroup and let n be the number of Sylow q-subgroups of G.

Then $n \mid p^2$ and $n \equiv 1 (\text{mod } q)$.

If $n = p^2$ then $p^2 \equiv 1 (\text{mod } q)$ and hence q divides either $p - 1$ or $p + 1$. Both are impossible since $p < q$. We get a similar contradiction if $n = p$. Hence $n = 1$ and so Q is normal in G. ✋☺

Corollary: If $|G| = pq$, where p, q are primes and $p < q$, then G is either cyclic or it is

$\langle A, B \mid A^q, B^p, B^{-1}AB = A^r \rangle$ where $r \equiv 1 (\text{mod } q)$. ☺

EXERCISES FOR CHAPTER 10

EXERCISE 1: Consider the G-set X where
G = {1, 2, 3, ... , 12} and X = {*a*, *b*, *c*, .. , *g*} and where the action is given by the table:

	a	***b***	***c***	***d***	***e***	***f***	***g***
1	*a*	*b*	*c*	*d*	*e*	*f*	*g*
2	*c*	*g*	*f*	*b*	*e*	*a*	*d*
3	*f*	*d*	*a*	*g*	*e*	*c*	*b*
4	*f*	*d*	*a*	*g*	*e*	*c*	*b*
5	*a*	*b*	*c*	*d*	*e*	*f*	*g*
6	*c*	*g*	*f*	*b*	*e*	*a*	*d*
7	*a*	*b*	*c*	*d*	*e*	*f*	*g*
8	*c*	*g*	*f*	*b*	*e*	*a*	*d*
9	*f*	*d*	*a*	*g*	*e*	*c*	*b*
10	*c*	*g*	*f*	*b*	*e*	*a*	*d*
11	*f*	*d*	*a*	*g*	*e*	*c*	*b*
12	*a*	*b*	*c*	*d*	*e*	*f*	*g*

(a) Find the orbits;
(b) Find the stabilisers of *c* and of *e*;
(c) Find a normal subgroup, H, of G such that G/H is isomorphic to a subgroup of the group of permutations on X.

EXERCISE 2: Consider the group
G = {I, (12)(34), (13)(24), (14)(23), (12), (34), (1324), (1423)} acting in the natural way on X = {1, 2, 3, 4}.
(a) Find the orbits;
(b) Find the stabiliser of 3.

EXERCISE 3: Let G = $\mathbf{A}_4$ and let
X = {(123), (132), (124), (142), (134), (143), (234), (243)},
the set of all 3-cycles in $\mathbf{A}_4$. Let the action be given by $x * g = g^{-1}xg$.

(a) Find the orbits;

(b) Find the stabiliser of (123).

EXERCISE 4: G is a non-abelian group of order 8 with exactly one element, z, of order 2.
Let X = $\{\{x, x^{-1}\} \mid x \in G \text{ and } x \neq x^{-1}\}$ and make X into a G-set by defining:

$$\{x, x^{-1}\} * y = \{ y^{-1}xy, y^{-1}x^{-1}y\} \text{ for } x, y \in G.$$

(a) Prove that |Z(G)| = 2.

(b) Prove that Z(G) = {1, z}.

(c) Prove that, except for 1 and z, the elements have order 4.

(d) Find the number of elements in X.

(e) Prove that X has at least one orbit of size 1.

(f) Prove that there exist $a, b \in G$ such that

(i) $b^{-1}ab = a^{-1}$ and

(ii) $b^2 = a^2 = z$.

(g) Prove that $a^{-1}ba = b^{-1}$.

(h) Find the number of orbits of X.

SOLUTIONS FOR CHAPTER 10

EXERCISE 1: (a) $\{a, c, f\}$, $\{b, d, g\}$, $\{e\}$;
(b) {1, 5, 7, 12}, G; (c) H = {1, 5, 7, 12}.

EXERCISE 2: (a) there is just one orbit (the action is transitive); (b) {I, (12)}.

EXERCISE 3: (a) {(123), (142), (134), (243)}, {(132), (124), (143), (234)}; (b) {I, (123), (132)}.

EXERCISE 4:
(a) Since G is non abelian $|Z| < 8$. Since G is a p-group, $|G| > 1$. Since G/Z(G) is not cyclic, $|Z(G)| \neq 4$. Hence $|Z(G)| = 2$.

(b) Let Z(G) = $\{1, a\}$. Since a has order 2 we must have $a = z$.

(c) The other 6 elements of G must have orders dividing 8 but bigger than 2. They can't be of order 8 because then G would be cyclic. Hence they must have order 4.

(d) The only elements which are equal to their inverses are 1 and z so X must consist of the remaining 6 elements grouped in pairs. Hence X has 3 elements.

(e) The size of the orbit of $\alpha \in X$ is $|G:\sigma(\alpha)|$ and so must divide 8. Hence the orbits of X must have size 1 or 2 and so one of them, at least, must have size 1.

(f) Let $\{a, a^{-1}\}$ be an orbit of size 1 and let $\{b, b^{-1}\}$ and $\{c, c^{-1}\}$ be the other two elements of X.
Hence the elements of G are $1, z, a, a^{-1}, b, b^{-1}, c, c^{-1}$. Since $\{a, a^{-1}\} * b = \{a, a^{-1}\}$ we must have $b^{-1}ab = a$ or a^{-1}. If $b^{-1}ab = a$ then $C_G(a)$ must contain at least the 5 elements $1, z, a, a^{-1}, b$ and so must be the whole of G.

But this would mean that $a \in Z(G)$, a contradiction. Hence $b^{-1}ab = a^{-1}$. Since a and b have order, both a^2 and b^2 must have order 2 and so must both equal z.

(g) From the equation $b^{-1}ab = a^{-1}$ and $b^2 = a^2$ we deduce that $a^{-1}ba = (b^{-1}ab)ba = b^{-1}(ab^2a) = b^{-1}a^4 = b^{-1}$.

(h) The stabiliser of $\{b, b^{-1}\}$ contains at least the 5 elements $1, z, a, b, b^{-1}$ and so must be the whole of G. Hence $\{b, b^{-1}\}$ forms an orbit of size 1. (This set contains 2 elements of G but, since the elements of X are unordered pairs $\{g, g^{-1}\}$, it is only one element of X.)

This just leaves $\{c, c^{-1}\}$ which must therefore form an orbit of size 1. Hence X has 3 orbits, all of size 1.