13. SYLOW SUBGROUPS

§13.1. Syllow Subgroups

Let G be an abelian group written additively. If p is a prime then the Sylow p-subgroup is defined to be:

\[ \text{Syl}_p(G) = \{ g \in G \mid p^n g = 0 \text{ for some } n \} \]

It is easy to show that this is a subgroup.

Written multiplicatively it becomes \( \{ g \in G \mid g^p = 1 \text{ for some } n \} \). This is the set of all elements whose order is a power of p but if G is non-abelian this is usually not a subgroup.

**Example 1:** If G = S_3 then \( \{ g \in G \mid g^2 = 1 \text{ for some } n \} = \{ I, (12), (13), (23) \} \), 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 finite then the order of a p-group is a power of p.

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 we will show. If \( p^n \) divides \(|G|\) then G has a subgroup (possibly more than one) of order \( p^n \). They are called **Sylow p-subgroups**, named after the mathematician.

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.

§13.2. 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. We have here a primitive analogue of the vector space from linear algebra. We can think of the elements of X as being like vectors, the elements of G as our scalars and the operation * as a scalar multiplication. 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.

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

\[ \sigma(S) = \{ g \in G \mid x * g = x \text{ for all } x \in S \} \]

In the case where \( S = \{ x \} \) we write \( \sigma(x) \) instead of \( \sigma(\{ x \}) \).
Example 2: Let \( X = \{1, 2, 3, 4, 5, 6\} \) and \( G = D_8 \).

Define \( x \ast g \) as follows:

\[
\begin{array}{cccccccc}
1 & 1 & 2 & 1 & 2 & 6 & 3 & 6 & 3 \\
2 & 2 & 1 & 2 & 1 & 3 & 6 & 3 & 6 \\
3 & 3 & 6 & 3 & 6 & 2 & 1 & 2 & 1 \\
4 & 4 & 4 & 4 & 4 & 5 & 5 & 5 & 5 \\
5 & 5 & 5 & 5 & 5 & 4 & 4 & 4 & 4 \\
6 & 6 & 3 & 6 & 3 & 1 & 2 & 1 & 2 \\
\end{array}
\]

\( \sigma(1) = \{1, A^2\} \);
\( \sigma(2) = \{1, A^2\} \);
\( \sigma(3) = \{1, A^2\} \);
\( \sigma(4) = \{1, A, A^2, A^3\} \);
\( \sigma(5) = \{1, A, A^2, A^3\} \);
\( \sigma(6) = \{1, A^2\} \);
\( \sigma(X) = \{1, A^2\} \), so \( X \) is not a faithful \( G \)-set.

Theorem 1: If \( X \) is a \( G \)-set and \( S \subseteq X \) then \( \sigma(S) \leq G \).

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

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

If \( S(X) \) denotes the symmetric group (the group of permutations) on \( X \) the function

\( \theta: G \rightarrow S(X) \) defined by \( \theta(g)(x) = x \ast g \) 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. 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 (for some reason we never say “unfaithful”) 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 \( \sigma(X) = G \).

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

**Proof:** \( G \) acts on itself by \( g \ast h = gh \) 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 \( G \).

Examples 3:

1. The **conjugation action** of \( G \) on \( G \) defined by \( x \ast g = x^g = g^{-1}xg \).
2. For any set \( X \) there is the **trivial action** defined by \( x \ast g = x \).
3. If \( G \) is the group \( O(n, \mathbb{R}) \) of orthogonal \( n \times n \) real matrices then we can define an action of \( G \) on the set of real \( n \)-dimensional row vectors, \( \mathbb{R}^n \) by \( x \ast A = xA \).
(4) An isometry $f: \mathbb{R}^3 \to \mathbb{R}^3$ is a distance preserving transformation. They are maps of the form $f(x) = xA + b$ where $A$ is an orthogonal $3 \times 3$ matrix and $b \in \mathbb{R}^3$.

$\text{IS}(3, \mathbb{R})$ is defined to be the group of congruence transformations under the usual multiplication of functions: $(fg)(x) = g(f(x))$, that is, first $f$ then $g$.

$\text{IS}(3, \mathbb{R})$ acts on $\mathbb{R}^3$ by defining $v * f$ to be $f(v)$.

**Klein’s definition of geometry**: Euclidean Geometry is the study of those properties of subsets of $\mathbb{R}^3$ that are invariant under the above action of $\text{IS}(3, \mathbb{R})$ on $\mathbb{R}^3$.

(5) The symmetry group of a subset $X$ of $\mathbb{R}^3$ is $\text{Sym}(X)$, the set of all congruence transformations, that fix the set $X$.

§13.3. 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 $\sim$ 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 $x^G$. 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:** $x^g = x^h \iff x^g (gh^{-1}) = x \iff gh^{-1} \in \sigma(x) \iff g \sigma(x) = h \sigma(x)$. 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 the number of conjugates is the index of the centraliser.

**Example 2 (continued):**

The orbits are $\{1, 2, 3, 6\}$ and $\{4, 5\}$. So $\#^G = \{1, 2, 3, 6\}$ and $\#^2 = 4$, $\#(2) = 2$, and $|G : (2)| = 4$. $\#^4 = 2 = |G : (2)|$.

§13.4. Cauchy’s Theorem

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

**Example 5:** Let $G = S_3$ 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, $X_G = \{4, 5\}$. 

217
Theorem 4: If $G$ is a finite $p$-group and $X$ is a finite $G$-set then $|X| \equiv |X_G|$ (mod $p$).

Proof: Suppose $|G| = p^n$ and let $x \in X$ and $O(x)$ be the orbit of $x$. Then $p^n = |G| = |G: \sigma(x)| \cdot |\sigma(x)| = |O(x)| \cdot |\sigma(x)|$. Either $|O(x)| = 1$ or $|O(x)| \equiv 0$ (mod $p$). But $|O(x)| = 1$ means $x \in X_G$. 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 $x \ast g = x$ 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 $X = \{(g_1, ..., g_p) \mid$ 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 $(g_1, ..., g_p) \ast A = (g_2, ..., g_p, g_1)$. By the corollary there exists $(g_1, ..., g_p)$ with $(g_1, ..., g_p) \ast A = (g_1, ..., g_p)$. So $g_1 = g_2 = ... = g_p = g$ say and hence $g^p = 1$.

Example 6: If $|G| = 105 = 3 \times 5 \times 7$ 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.

Corollary: Suppose $G$ is a finite group and $p$ is prime. Then $G$ is a $p$-group if and only if the order of each element of $G$ is a power of $p$.

Example 7: $A_5$ has order 60 but has no subgroup of order 30, even though 30 divides 60 (but of course it isn’t prime). 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, as we shall show later, $A_5$ has no normal subgroups other than itself and 1.

§13.5. Normalizers

If $H \leq G$ and $g \in G$ we define $H^g = g^{-1}Hg = \{g^{-1}hg \mid h \in H\}$. 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 $G = |G : N_G(H)|$.

Proof: Let $N = N_G(H)$, let $X$ be the set of conjugates of $H$ in $G$ and let $R$ be the set of right cosets $Ng$ in $G$.

We define a function $f: R \rightarrow X$ 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 $H^{g_2g_1^{-1}} = H$ and so $g_2g_1^{-1} \in N$. Hence $Ng_1 = Ng_2$. We have thus shown that $f$ is 1-1.

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

218
Theorem 7: If $G$ is a finite $p$-group and $H \triangleleft G$ then $H \triangleleft N_G(H)$.

**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.

A **maximal** subgroup of $G$ is a subgroup $H \triangleleft G$ where there is no subgroup $K$ for which $H \triangleleft K \triangleleft G$. **Minimal** subgroups are defined similarly.

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

§13.6. The Sylow Theorems

The following is one of a very famous trilogy of theorems first proved by the Norwegian mathematical Ludwig Sylow who died in 1918. 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):** Finite groups have Sylow $p$-subgroups for all primes $p$ dividing their order.

**Proof:** Suppose $|G| = p^n m$ where $p$ is prime and $(p, m) = 1$ and let $X$ be the set of all subsets of size $p^n$. Then $G$ acts on $X$ by the action $S \trianglerighteq g = Sg = \{sg \mid s \in S\}$. Now $|X| = \binom{p^n m}{p^n}$ which is coprime to $p$. Hence for some $S \in X$, $|\text{orb}(S)|$ is coprime to $p$. Let $P = \text{stab}(S)$. Then $|G : P|$ is coprime to $p$ and hence $p^n$ divides $|P|$. Now if $s \in S$, $sP \subseteq S$ and so $|P| \leq p^n$. Hence $|P| = p^n$.

**Theorem 9 (Sylow’s Second and Third Theorems):**

1. The Sylow $p$-subgroups of a finite group $G$ are conjugate.
2. The number of Sylow $p$-subgroups of $G$ is congruent to 1, modulo $p$, and divides $m$.

**Proof:**

1. 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 $P, P_{g_2}, \ldots, P_{g_m}$ be the right cosets of $P$. Make $X = \{P, P_{g_2}, \ldots, P_{g_m}\}$ into a $G$-set by defining $(P_{g_i}) * g = P(g_{g_i})$.

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 $g \in P_{g_i}$ then $g^{-1}P_{g_i} = \sigma(P_{g_i})$ (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 right 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 $P_{g_i}$, is not divisible by $p$. Let $R = Q \cap \sigma(P_{g_i})$. This is the stabilizer of $P_{g_i}$ under the $Q$-action. Hence the size of the orbit divides $p^n$ and so is 1. It follows that $R = Q$ and so $Q = \sigma(P_{g_i}) = g_{g_i}^{-1}P_{g_i}$.
(2) Now let \( N = N_G(P) \) and let \( Y \) be the set of right cosets of \( N \) in \( G \). The number of Sylow \( p \)-subgroups is the number of conjugates of \( P \), which \( |G:N| \). 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 \( P \leq N \).

Let \( Q = P^g \). 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 \( P^g = P \) and so \( g \in N \). So \{N\} is the only orbit of size 1.

§13.7. Applications of the Sylow Theorems

**Theorem 10:** Suppose \( |G| = p^aq^b \) where \( p, q \) are 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 \( n \equiv 1 \pmod{q} \).

If \( n = p^2 \) then \( p^2 \equiv 1 \pmod{q} \) 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 \( G \cong C_{pq} \) or \( G = \langle A, B \mid A^q, B^p, B^{-1}AB = A^r \rangle \) where

\( q^{-1} \) \( (1 2 3) \) \( (2 5 8) \) \( (3 6 9) \) \( \langle 1 \ 2 \ 3 \rangle \) \( \langle 4 \ 5 \ 6 \rangle \) \( \langle 7 \ 8 \ 9 \rangle \) \( x = (1 4 7)(2 5 8)(3 6 9) \). Then \( x^{-1}(1 2 3)x = (2 5 8) \),

\( x^{-1}(2 5 8)x = (3 6 9) \) and

\( x^{-1}(3 6 9)x = (1 2 3) \)

The group generated by \( H \) and \( x \) consists of all elements of \( S_{11} \) of the form \( hx^r \) where \( h \in H \) and \( r \in \{0, 1, 2\} \). Clearly it has order \( 3^4 \) and so is the Sylow 3-subgroup.

§13.8. Sylow Subgroups of Symmetric Groups

**Example 8:** Find the Sylow subgroups of \( S_{11} \).

**Solution:** The set of prime divisors of \( 11! \) is \( \Omega = \{2, 3, 5, 7, 11\} \).

\( p = 11: \langle (1 2 3 4 5 6 7 8 9 10 11) \rangle \) has order 11 and so is a Sylow 11-subgroup of \( S_{11} \).

\( p = 7: \langle (1 2 3 4 5 6 7 8 9) \rangle \) has order 7 and so is a Sylow 7-subgroup of \( S_{11} \).

\( p = 5: \langle (1 2 3 4 5) \rangle \) and \( B = \langle (6 7 8 9 10) \rangle \) then \( A \times B \) has order \( 5^2 \), which is the largest power of 5 dividing \( 11! \). It is therefore a Sylow 5-subgroup of \( S_{11} \).

We can summarise the results so far by saying that the Sylow \( p \)-subgroups of \( S_{11} \) are isomorphic to \( C_{11} \), \( C_7 \) and \( C_5 \times C_5 \) respectively.

\( p = 3: \) Clearly \( S_{11} \) has a subgroup of order \( 3^3 \) that is isomorphic to \( C_3 \times C_3 \times C_3 \). But the largest power of 3 that divides \( 11! \) is \( 3^4 \). So this is not a Sylow 3-subgroup.

Let \( H = \langle (1 2 3) \rangle \times \langle (4 5 6) \rangle \times \langle (7 8 9) \rangle \). We can extend \( H \) by an element of order 3 that takes each block of three to the next, with the last going to the first. More specifically, let \( x = (1 4 7)(2 5 8)(3 6 9) \).

Then \( x^{-1}(1 2 3)x = (2 5 8) \),

\( x^{-1}(2 5 8)x = (3 6 9) \) and

\( x^{-1}(3 6 9)x = (1 2 3) \)

The group generated by \( H \) and \( x \) consists of all elements of \( S_{11} \) of the form \( hx^r \) where \( h \in H \) and \( r \in \{0, 1, 2\} \). Clearly it has order \( 3^4 \) and so is the Sylow 3-subgroup.
p = 2: The largest power of 2 that divides 11! is $2^8$.
We can easily find a subgroup of $S_{11}$ isomorphic to $C_2 \times C_2 \times C_2 \times C_2 \times C_2$ such as
$$H = \langle (1 \ 2) \rangle \times \langle (3 \ 4) \rangle \times \langle (5 \ 6) \rangle \times \langle (7 \ 8) \rangle \times \langle (9 \ 10) \rangle.$$ This has order $2^5$. We could extend $\langle (1 \ 2) \rangle \times \langle (3 \ 4) \rangle \times \langle (5 \ 6) \rangle \times \langle (7 \ 8) \rangle$ by $x = (1 \ 3 \ 5 \ 7 \ 2 \ 4 \ 6 \ 8)$ and this would give a subgroup of order $2^6$. Even tacking on $\langle (9 \ 10) \rangle$ as an extra direct factor only takes it to $2^7$ which is not quite big enough. We will return to this problem later.

The technique for constructing the Sylow subgroups for $p = 2$ and 3 is called the **wreath product**. The wreath product is very difficult to describe formally, but is quite intuitive when you see it in practice. Here is an a formal definition, but don’t expect to understand it until you have seen some examples.

Suppose $G, H$ are permutation groups, and if $G \in S_m$ and $H \in S_n$. Suppose $G_1, G_2, \ldots, G_n$ are isomorphic copies of $G$, with $\phi_i : G \to G_i$ being an isomorphism for each $i$.

Then $G \wr H = (G_1 \times G_2 \times \ldots \times G_n)H$ where each $G_i$ is isomorphic to $G$ and where, if $g \in G_i$ and $h \in H$, $g h^{-1}$ is the corresponding element in $G_{\phi_i(h)}$. More precisely, if $\phi_i : G \to G_i$ is an isomorphism $g h^{-1} = \phi_i^{-1}(\phi_i(g))$. The elements have the form $g_1 g_2 \ldots g_n h$, where each $g_i \in G_i$ and $h \in H$. The $g_i$ commute with one another, the elements of $H$ multiply as in that permutation group and if $g \in G_i$ then $h g = \phi_i h^{-1} \phi_i(g) h$. A typical element of $G \wr H$ is a sequence $(g_1, g_2, \ldots, g_n, h)$ with each $g_i \in G_i$ and $h \in H$ but, for clarity, we will write this as $[g_1, g_2, \ldots, g_n, h]$.

**Example 9:** Let $G = S_3$ and $H = \langle (12345) \rangle$.
If $a = [(12), (23), (132), (12)] (12345)$ and $b = [(123), (12), (12), (I)] (12524)$, find $ab$.

**Solution:**
$$ab = [(12), (23), (132), (12)] (12345) (12345).$$
The first step is to move the $(12345)$ down to the end. As $(12345)$ passes over the second square bracket it merely permutes the components cyclically, according to that permutation.
So $ab = [(12), (23), (132), (12)] (12345) (12345).$

Now we simply multiply elements within each of the groups $G$ and $H$.
$$ab = [(12), (23), (132), (12)] (12345) (12345).$$
$$= [(12), (12), (12), (I)] (14253).$$

**Example 10:** Find the orders of the wreath products $S_3 \wr S_4$ and $S_4 \wr S_3$.

**Solution:** $S_3 \wr S_4$ consists of a direct product of 4 copies of $S_3$ extended by $S_4$. Its order is therefore $(3!)^4 . 4! = 6^4 . 24 = 31104$.

$S_4 \wr S_3$ consists of a direct product of 3 copies of $S_4$ extended by $S_3$.
Its order is therefore $(4!)^3 . 3! = 24^3 . 6 = 82944$.

**Example 11:** Find the largest order of any element of $S_3 \wr S_3$.

**Solution:** The largest order of any element of $S_3 \times S_3 \times S_3$ is the same as the largest order of any element of $S_3$, namely 3.
If $x = [a, b, c]$ then $x$ has order 3 at most.
If $x = [a, b, c](\times \times)$, where $(\times \times)$ is any 2-cycle, then $x^2 \in S_3 \times S_3 \times S_3$ and so $x$ has order 6 at most. If $x = [a, b, c](123)$ then
\[ x^2 = [a, b, c](123), \quad [a, b, c](123) \\
= [a, b, c][c, a, b](132) \\
= [ac, ab, bc](132). \]

\[ x^3 = [a, b, c](123) [ac, ab, bc](132) \\
= [a, b, c][bc, ac, ab] \\
= [abc, abc, abc]. \]

So \( x \) has order at most 9 and if \( a = b = 1 \) and \( c = (123) \) then \( x \) has order 9.

Hence the maximum order of any element of \( S_3 \) is 9.

**Example 8 (revisited):** Find, up to isomorphism, the Sylow subgroups of \( S_{11} \)

**Solution:** We found them all, except for \( p = 2 \), and they can be written as follows.

<table>
<thead>
<tr>
<th>( p )</th>
<th>Sylow ( p )-subgroup</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>( C_{11} )</td>
</tr>
<tr>
<td>7</td>
<td>( C_7 )</td>
</tr>
<tr>
<td>5</td>
<td>( C_5 \times C_5 )</td>
</tr>
<tr>
<td>3</td>
<td>( C_3 \rtimes C_3 )</td>
</tr>
</tbody>
</table>

**\( p = 2 \):** Partition \( \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\} \) into pairs, as far as we can. We get \( \{1, 2\}, \{3, 4\}, \{5, 6\}, \{9, 8\}, \{9, 10\}, \{11\} \), with \( \{11\} \) left over.

We can take a \( C_2 \) for each of these to get \( C_2 \times C_2 \times C_2 \times C_2 \times C_2 \), which has order \( 2^5 \).

Now partition these pairs into pairs of pairs, as far as we can.

We get \( \{\{1, 2\}, \{3, 4\}\}, \{\{5, 6\}, \{7, 8\}\}, \{9, 10\} \), with \( \{9, 10\} \) left over.

Now on each of these pairs of pairs we can construct a group isomorphic to \( C_2 \rtimes C_2 \). Each has order \( 2^3 \). If we now take \( (C_2 \rtimes C_2) \rtimes C_2 \) we get a group of order \( (2^3)^2 \times 2 = 2^7 \).

But we had \( \{9, 10\} \) left over, on which we can form another \( C_2 \). The Sylow 2-subgroup is thus \( ((C_2 \rtimes C_2) \rtimes C_2) \times C_2 \), which has order \( 2^8 \).

We adopt the convention that wreath products are bracketed from the left, so that

\( A \rtimes B \rtimes C \) will be assumed to mean \( (A \rtimes B) \rtimes C \). We also assume that wreath products take precedence over direct products, so that \( A \times B \rtimes C \) will be assumed to mean \( A \times (B \rtimes C) \). We can therefore write the Sylow 2-subgroups of \( S_{11} \), up to isomorphism, as \( C_2 \rtimes C_2 \rtimes C_2 \times C_2 \).

The Sylow subgroups of \( S_{11} \) are therefore:

<table>
<thead>
<tr>
<th>( p )</th>
<th>Sylow ( p )-subgroup</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>( C_{11} )</td>
</tr>
<tr>
<td>7</td>
<td>( C_7 )</td>
</tr>
<tr>
<td>5</td>
<td>( C_5 \times C_5 )</td>
</tr>
<tr>
<td>3</td>
<td>( C_3 \rtimes C_3 )</td>
</tr>
</tbody>
</table>

**Example 12:** Find the Sylow 5-subgroups of \( S_{57} \).

**Solution:** Writing 57 as a sum of powers of 5 we get \( 57 = 5^2 \times 2 + 5 + 2 \).

We can therefore partition \( \{1, 2, ..., 58\} \) as

\( \{1, 2, ..., 25\}, \{26, 27, ..., 50\}, \{51, 52, 53, 54, 55\}, \{56\}, \{57\}, \{58\} \).

On each block of 25 symbols we can construct \( C_5 \rtimes C_5 \) and on the block of 5 we can construct \( C_5 \).
So the Sylow 5-subgroups of $S_{57}$ are therefore isomorphic to $C_5 \times C_5 \times C_5 \times C_5$.

To describe Sylow subgroups of symmetric groups compactly we define $G^n$ to mean the direct product of $n$ copies of $G$ and we define $G^{(n)}$ to denote the wreath product of $n$ copies of $G$.

**Example 13:** $S_4^3 = S_4 \times S_4 \times S_4$ and $S_4^{(3)} = S_4[S_4]S_4$.

**Theorem 11:** If $p$ is prime and $n = a_rp^r + a_{r-1}p^{r-1} + \ldots + a_1p + a_0$, where for each $i$, $0 \leq a_i < p$, the Sylow $p$-subgroups of $S_n$ are isomorphic to $C_p^{(r)a_r} \times C_p^{(r-1)a_{r-1}} \times \ldots \times C_p^{(2)a_2} \times C_p^{a_1}$.

**Proof:** The existence of a subgroup of $S_n$ the above form should be now obvious. We omit the proof that its order is the highest power of $p$ that divides $n!$.

**Example 14:** Find the Sylow $p$-subgroups of $S_{30}$ for $p \leq 7$ and their orders.

**Solution:**

<table>
<thead>
<tr>
<th>$p$</th>
<th>Sylow $p$-subgroup</th>
<th>order</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>$C_7 \times C_7 \times C_7 \times C_7$</td>
<td>$7^4$</td>
</tr>
<tr>
<td>5</td>
<td>$C_5 \times C_5 \times C_5$</td>
<td>$5^7$</td>
</tr>
<tr>
<td>3</td>
<td>$C_3 \times C_3 \times C_3 \times C_3$</td>
<td>$3^{14}$</td>
</tr>
<tr>
<td>2</td>
<td>$C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2$</td>
<td>$2^{26}$</td>
</tr>
</tbody>
</table>

**EXERCISES FOR CHAPTER 13**

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

<table>
<thead>
<tr>
<th></th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
<th>f</th>
<th>g</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
<td>e</td>
<td>f</td>
<td>g</td>
</tr>
<tr>
<td>2</td>
<td>c</td>
<td>g</td>
<td>f</td>
<td>b</td>
<td>e</td>
<td>a</td>
<td>d</td>
</tr>
<tr>
<td>3</td>
<td>f</td>
<td>d</td>
<td>a</td>
<td>g</td>
<td>e</td>
<td>c</td>
<td>b</td>
</tr>
<tr>
<td>4</td>
<td>f</td>
<td>d</td>
<td>a</td>
<td>g</td>
<td>e</td>
<td>c</td>
<td>b</td>
</tr>
<tr>
<td>5</td>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
<td>e</td>
<td>f</td>
<td>g</td>
</tr>
<tr>
<td>6</td>
<td>c</td>
<td>g</td>
<td>f</td>
<td>b</td>
<td>e</td>
<td>a</td>
<td>d</td>
</tr>
<tr>
<td>7</td>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
<td>e</td>
<td>f</td>
<td>g</td>
</tr>
<tr>
<td>8</td>
<td>c</td>
<td>g</td>
<td>f</td>
<td>b</td>
<td>e</td>
<td>a</td>
<td>d</td>
</tr>
<tr>
<td>9</td>
<td>f</td>
<td>d</td>
<td>a</td>
<td>g</td>
<td>e</td>
<td>c</td>
<td>b</td>
</tr>
<tr>
<td>10</td>
<td>c</td>
<td>g</td>
<td>f</td>
<td>b</td>
<td>e</td>
<td>a</td>
<td>d</td>
</tr>
<tr>
<td>11</td>
<td>f</td>
<td>d</td>
<td>a</td>
<td>g</td>
<td>e</td>
<td>c</td>
<td>b</td>
</tr>
<tr>
<td>12</td>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
<td>e</td>
<td>f</td>
<td>g</td>
</tr>
</tbody>
</table>

(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 $G = A_4$ and let $X = \{(123), (132), (124), (142), (134), (143), (234), (243)\}$, the set of all 3-cycles in $A_4$. Let the action be given by $x * g = g^{-1} x g$.
(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 $X = \{\{x, x^{-1}\} \mid x \in G$ and $x \neq x^{-1}\}$ and make $X$ into a $G$-set by defining:
\[\{x, x^{-1}\} * y = \{y^{-1} xy, y^{-1} x^{-1} y\}\]
for $x, y \in G$.
(a) Prove that $|Z(G)| = 2$.
(b) Prove that $Z(G) = \{1, z\}$.
(c) Prove that the elements other than 1 and $z$ 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 $\exists a, b \in G$ 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 13**

**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) $\{1, (12)\}$.

**EXERCISE 3:** (a) $\{(123), (124), (134), (243)\}$, $\{(132), (124), (143), (234)\}$;
(b) $\{1, (123), (132)\}$.

**EXERCISE 4:**
(a) Since $G$ is non abelian $|Z| < 8$. Since $G$ is a p-group ($p = 2$) $|G| > 1$. 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, 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 1 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.