$gH_1 = H_1 g$ for all $g \in G$). Now $|G/H_1| = p^{n-1}$ and by induction hypothesis, there is a normal chain of subgroups

$$\{1\} = K_0 < K_1 < \cdots < K_{n-1} = G/H_1.$$

By the Correspondence Theorem this chain corresponds to a normal chain of intermediate subgroups between H_1 and G

$$H_1 < H_2 < \cdots < H_n = G$$

where $K_{i-1} = H_i/H_1$. Then $|H_i| = |K_{i-1}| \cdot |H_1| = p^{i-1} \cdot p = p^i$ and the chain

$$\{1\} = H_0 < H_1 < \cdots < H_n = G$$

is the chain we want. $\square$.

Remark. In particular this last result tells us that the converse to Lagrange's Theorem holds when G is a p-group. To see the converse of Lagrange's Theorem doesn't hold in general consider the group A_5. This is a simple group with 60 elements that has no subgroup with 30 elements. This is because a subgroup with 30 elements would have index 2 and thus be normal contradicting the simplicity of A_5.

Definition. Let G be a finite group of order $p^n \cdot m$ where p does not divide m. A subgroup of order p^n is called a *Sylow p-subgroup* of G.

Remark. A more elegant way of saying that H is a Sylow p-subgroup of G is to say that H is a p-group such that $[G : H]$ is not divisible by p.

We are now going to prove a number of very nice and useful results about these. In particular we will see that these subgroups always exist and are (for a given group G) all isomorphic. We will also get some information about the number of the Sylow p-subgroups. These results, known collectively as the Sylow theorems, are going to be an important tool to understand the structure of the larger group G.

Theorem 5.4 *(1st Sylow Theorem) Let G be a finite group and p a prime number. There exists a Sylow p-subgroup of G.*

Proof We prove this by induction on $|G|$. If $|G| = 1$ then $\{1\}$ is the Sylow p-subgroup for any prime p and thus the Sylow p-subgroups exist trivially in this case. Suppose now that $|G| \geq 2$, and that the result holds for groups of smaller order. Let p be any prime and suppose that $|G| = p^n m$ where $p \not| m$. If $n = 0$ then the trivial subgroup $\{1\}$ would be a Sylow p-subgroup. We can thus assume that $n \geq 1$. We use the class equation

$$|G| = |Z(G)| + \sum_{i=1}^{r} \underbrace{[G : C_G(a_i)]}_{\text{each } \geq 2}.$$

Suppose first that some of $[G : C_G(a_i)]$ is not divisible by p. Notice that $|G| = [G : C_G(a_i)] \cdot |C_G(a_i)|$ and as p does not divide $[G : C_G(a_i)]$, whereas p^n divides $|G|$, it follows that p^n divides $|C_G(a_i)|$. But $|C_G(a_i)| < |G|$ and thus by induction hypothesis $C_G(a_i)$

contains a Sylow p-subgroup that is of order p^n and thus a Sylow p-subgroup of G as well.

We are then left with the case when all of the indices $[G : C_G(a_i)]$ are divisible by p. Then $|G|$ is divisible by p and from the class equation it then follows that p divides the order of $|Z(G)|$. By Cauchy's Theorem (we only need the abelian version) we know that $Z(G)$ has a subgroup N of order p which has to be normal in G, since $Ng = gN$ for all $g \in G$. By induction hypothesis, G/N contains a Sylow p-subgroup that is a subgroup of order p^{n-1}. By the Correspondence Theorem this subgroup is of the form P/N for some $N \leq P \leq G$. Notice that $|P| = |N| \cdot |P/N| = p \cdot p^{n-1} = p^n$ and thus P is a Sylow p-subgroup of G. □

Corollary 5.5 *Let G be a group of finite order and let p^r be any power of a prime that divides the order of G. Then there exists a subgroup of order p^r.*

Proof Suppose that $|G| = p^n m$ where $p \not| m$. By the first Sylow theorem there is a subgroup P of order p^n and by Theorem 5.3 we know that P has a subgroup of order p^r. □

For the proof of the 1st Sylow Theorems we used arguments that involved counting the elements of G. For our proofs of the other Sylow theorems we will be counting cosets instead.

Counting cosets If $H, K \leq G$ and let X be the set of all right cosets of H in G. Then K acts naturally on X through right multiplication: $Ha * x = Hax$. This turns X into a K-set. The next Lemma gives us a useful formula of counting the number of cosets that belongs to any given K-orbit.

Lemma 5.6 *The number of cosets in the K-orbit containing Ha are*

$$|Ha * K| = [K : K \cap H^a].$$

Proof We apply the Orbit-Stablizer Theorem. We need to determine the stablizer of the coset Ha in K. Now

$$Hak = Ha \;\Leftrightarrow\; Haka^{-1} = H \;\Leftrightarrow\; aka^{-1} \in H \;\Leftrightarrow k \in a^{-1}Ha = H^a$$

As k was in K to start with, this shows that the stablizer of Ha is $K \cap H^a$ and the Orbit-Stabilizer Theorem tells us that $|Ha * K| = [K : K \cap H^a]$. □

A formula for counting cosets. As before we let X be the set of all right H-cosets that we consider as a K-set. Suppose that

$$X = Ha_1 * K \cup Ha_2 * K \cup \cdots \cup Ha_m * K$$

is the partition of X into disjoint K-orbits. Using Lemma 5.6 this implies that

$$\begin{aligned} [G : H] &= |X| \\ &= |Ha_1 * K| + |Ha_2 * K| + \cdots + |Ha_m * K| \\ &= [K : K \cap H^{a_1}] + [K : K \cap H^{a_2}] + \cdots + [K : K \cap H^{a_m}]. \end{aligned}$$

Remark. We know from Theorem 5.3 that any Sylow p-subgroup contains a subgroup of an order that is an arbitrary p-power divisor of $|G|$. Now we show that the converse is true. Every subgroup of p-power order is contained in some Sylow p-subgroup. In fact we prove something much stronger.

Theorem 5.7 *Let $H \leq G$ where H is a subgroup of p-power order. Let P be any Sylow p-subgroup of G. Then*

$$H \leq P^a$$

for some $a \in G$.

Proof Suppose that $|G| = p^n m$ where $p \not| m$. Let X be the collection of all the right P cosets that we consider as a H-set. By the formula for counting cosets, we have

$$m = [G : P] = [H : H \cap P^{a_1}] + [H : H \cap P^{a_2}] + \ldots + [H : H \cap P^{a_m}] \tag{4}$$

for some $a_1, \ldots, a_m \in G$. We claim that $H \cap P^{a_i} = H$ for some $i = 1, \ldots, m$. Otherwise all the indices on the RHS of (4) would be divisible by p and we would get the contradiction that m is divisible by p. Hence $H \cap P^{a_i} = H$ for some $i \in \{1, \ldots, m\}$ or equivalently $H \subseteq P^{a_i}$. $\square$

The 2nd Sylow theorem is a direct consequence of this.

Theorem 5.8 *(2nd Sylow Theorem). Any two Sylow p-subgroup are conjugate. (So they form a single conjugacy class).*

Proof Let P and Q be Sylow subgroups of G. By last theorem we know that

$$Q \subseteq P^a$$

for some $a \in G$. But these two groups have the same order. Hence we have $Q = P^a$. $\square$

Remark. The map $\phi : P \to P^a$, $x \mapsto x^a$ is an isomorphism and thus P and P^a are isomorphic. So all the Sylow p-subgroups are isomorphic and up to isomorphism we can talk about the Sylow p-subgroup.

We now move on to the third and the last of the Sylow theorems. This is going to give us some information on the number of Sylow p-subgroups that is immensely useful as we will see.

Theorem 5.9 *(3rd Sylow Theorem). Let G be a finite group and p a prime. The number $n(p)$ of Sylow p-subgroups of G satisfies:*

(i) $n(p) = 1 + pr$, for some non-negative integer r.
(ii) $n(p)$ divides $|G|$.

Proof (See at the end of this chapter).

Remarks. (1) Suppose that $|G| = p^n m$ whre p does not divide m. Let P be a Sylow p-subgroup of G. As $|G| = p^n m = |P| \cdot [G : P]$ and as $n(p) = 1 + pr$ divides $|G|$ while being coprime to p, we must have that $n(p)$ divides $m = [G : P]$.

(2) Let P be a Sylow p-subgroup of G. The Sylow p-subgroups form a single conjugacy class

$$\{\, a^{-1}Pa : \, a \in G\}$$

The number $n(p)$ of these is one iff all of them are equal to P, i.e. iff $P \trianglelefteq G$.

Example 1. Let G be a group of order $2 \cdot p^r$ where p is an odd prime and $r \geq 1$. By the Sylow theorems there exist a subgroup of order p^r that is then of index 2 and therefore normal. Hence G can't be simple if it is of order $2p^r$.

Example 2. Let G be a group of order pq where p and q are primes and $p > q$. Now the number $n(p)$ of Sylow p-subgroups, satisfies

$$n(p) = 1 + pr \;\text{ and }\; n(p) \text{ divides } |G|/p = q$$

The only possible $n(p)$ satisfying these criteria is $n(p) = 1$. It follows that there is only one subgroup of order p and this must then be normal in G. We have thus shown that there are no simple groups of order pq.

Example 3. To demonstrate the usefulness of the Sylow theorems, let us see how we can use them to see that there is no simple group of order $12 = 3 \cdot 2^2$. Firstly we have by the 1st Sylow theorem (or Cauchy's thm) that there is a subgroup of order 3 and the number $n(3)$ of these satisfies

$$n(3) = 1 + 3r \;\text{ and }\; n(3) \text{ divides } |G|/3 = 4.$$

There are only two possibilities, $n(3) = 1$ or $n(3) = 4$. In the first case there is a normal subgroup of order 3. Let us look at the latter case. We have 4 groups of order 3 and therefore $4 \cdot 2 = 8$ elements of order 3 (in each of the Sylow 3-subgroups there are two elements of order 3 and as the intersection of any two of these is $\{1\}$ we get exactly $4 \cdot 2 = 8$ elements of order 3). There remain 4 elements that must form a unique Sylow 2-subgroup Q (which has order 4). Notice that none of the elements of order 3 can be in Q as 3 does not divide 4. As $n(2) = 1$ we now have that $Q \trianglelefteq G$.

Example 4. Let p, q be distinct primes. We will see that there is no simple group of order p^2q. We consider two cases. If $p > q$ then $n(p) = 1 + pr$ should divide q and as $p > q$ this can only happen if $n(p) = 1$. But in this case we have a normal Sylow p-subgroup. We can thus assume that $p < q$. Now

$$n(q) = 1 + qr \text{ divides } |G|/q = p^2.$$

If $n(q) = 1$ we have a normal Sylow q-subgroup, so we can suppose that $n(q) > 1$. As $q > p$ the only possibility is that $n(q) = p^2$. We then have

$$1 + qr = p^2 \;\Leftrightarrow\; qr = p^2 - 1 = (p-1)(p+1).$$

As the prime q is greater than p, it follows that q divides $p+1$ and again as $q > p$, we must have $q = p+1$. The only two primes that are one apart are 2 and 3. Thus $p = 2$ and $q = 3$ and $|G| = p^2 \cdot q = 12$. But by Example 3, there is no simple group of order 12 and we are done.

Remark. We mentioned before a famous result of Burnside, the Burnside's (p, q)- Theorem. This said that any group G of order $p^n q^m$ is solvable. This means that there are not composition factors that are non-abelian. In particular G can't be non-abelian simple.

Later in the notes and on the exercise sheets we will apply the Sylow theorems to find all groups of order up to and including 15. We will also see that there is no non-abelian simple group of order less than 60 ($|A_5| = 60$). Before leaving this section we add another weapon to our list. This is Poincaré's Lemma that is often of great help.

Definition. Suppose $H \leq G$. The subgroup

$$H_G = \bigcap_{g \in G} H^g$$

is called the *core* of H in G.

Remarks. (1) As $H = H^e$ is one of the conjugates of H it is clear that $H_G \leq H$ and we will see later that $H_G \trianglelefteq G$ as a part of Poincaré's Lemma. This we can also see directly. Let $a \in G$ then

$$H_G^a = \bigcap_{g \in G} H^{ga} = \bigcap_{b \in G} H^b = H_G,$$

where the last identity holds from the fact that $Ga = G$.

(2) If $N \leq H$ and $N \trianglelefteq G$ then for all $g \in G$ we have $N = N^g \leq H^g$. It follows that

$$N \leq \bigcap_{g \in G} H^g = H_G.$$

This shows that H_G is the largest normal subgroup of G that is contained in H.

Theorem 5.10 *Suppose G is a group (possibly infinite) and let $H \leq G$ such that $[G : H] = n < \infty$. Then*

$$G/H_G \cong K$$

for some $K \leq S_n$.

Proof Let $X = \{gH : g \in G\}$. For each $a \in G$, we get a map $L_a : X \to X$, $gH \mapsto agH$. Notice that L_a is bijective with inverse $L_{a^{-1}}$. Also notice that

$$L_a \circ L_b(gH) = L_a(bgH) = abgH = L_{ab}(gH).$$

Now consider the map $\phi : G \to \mathrm{Sym}\,(X),\ a \mapsto L_a$. We have just seen that $L_{ab} = L_a \circ L_b$ and this implies that $\phi(ab) = \phi(a) \circ \phi(b)$. Thus ϕ is a homomorphism. We next identify

the kernel. We have

$$\begin{aligned}\phi(a) = L_a = \mathrm{id} &\Leftrightarrow agH = gH \text{ for all } g \in G \\ &\Leftrightarrow g^{-1}agH = H \text{ for all } g \in G \\ &\Leftrightarrow g^{-1}ag \in H \text{ for all } g \in G \\ &\Leftrightarrow a \in gHg^{-1} \text{ for all } g \in G.\end{aligned}$$

Therefore the kernel is $\bigcap_{g\in G} H^{g^{-1}} = \bigcap_{a\in G} H^a = H_G$. By the 1st Isomorphism Theorem we have that $H_G \trianglelefteq G$ and

$$G/H_G = G/\ker\phi \cong \operatorname{im}\phi$$

where $\operatorname{im}\phi \leq \mathrm{Sym}(X)$. As $|X| = n$ we have that $\mathrm{Sym}(X) \cong S_n$ and thus G/H_G isomorphic to a subgroup of S_n. $\square$.

Corollary 5.11 *(Poincaré's Lemma). Let G be a finite simple group with a subgroup H such that $[G : H] = n > 1$. Then*

$$G \cong K$$

for some $K \leq S_n$. In particular $|G|$ divides $|S_n| = n!$.

Proof H_G is a normal subgroup of G and as H_G is contained in H we can't have $H_G = G$. Now G is simple and we conclude that $H_G = \{1\}$. The result now follows from Theorem 5.11 as $G/\{1\} \cong G$. $\square$

Example 5. Let us give another proof of the fact that there is no simple group of order 12. We argue by contradiction and suppose that G is a simple groups with 12 elements. By the Sylow theorems we have a subgroup of order 4 and thus of index 3. By Corollary 5.12 if follows that $12 = |G|$ divides the $3! = 6$. This is absurd.