If $|G|=n$, and $k|n$, then in general there is no reason for G to contain an element of order k, or even a subgroup of order k. – the "converse to Lagrange's thm" fails.

Ex: A_4 (resp. A_5) has no subgroup of order 6 (resp. 30) – such a subgroup would be normal.

Fix a prime p (which divides $|G|$) and write $|G| = p^e m$, $p \nmid m$.

Def. A subgroup $H \subset G$ of order $|H| = p^e$ is called a Sylow p-subgroup of G.

Theorems (Sylow, 1872)

1) For every prime p, a Sylow p-subgroup of G exists.
2) All Sylow p-subgroups are conjugates of each other:
   $H, H' \subset G$ p-Sylow $\Rightarrow \exists\, g \in G$ st. $H' = gHg^{-1}$
   Moreover, any subgroup $K \subset G$ with $|K|$ a power of p is contained in a Sylow p-subgroup.
3) Let s_p be the number of Sylow p-subgroups of G.
   Then $s_p \equiv 1 \mod p$, and $s_p \mid |G|$. (or equivalently, $s \mid m = \frac{|G|}{p^e}$)

Example: classify groups of order 15.

If $|G| = 15$ then there exist Sylow subgroups $H, K \subset G$ with $|H|=3$, $|K|=5$.

The numbers of such Sylow subgroups: $\begin{cases} s_3 \mid 5 \text{ and } s_3 \equiv 1 \mod 3 \Rightarrow s_3 = 1. \\ s_5 \mid 3 \text{ and } s_5 \equiv 1 \mod 5 \Rightarrow s_5 = 1 \end{cases}$

This implies H and K are normal! (since their conjugates gHg^{-1}, gKg^{-1} are also Sylow subgroups, but H and K are the unique such).

Using criterion coming up next for direct products, this implies
$G \simeq H \times K \simeq \mathbb{Z}/3 \times \mathbb{Z}/5 \simeq \mathbb{Z}/15$. Every group of order 15 is cyclic! □

Digression: normal subgroups, semidirect products and direct products.

- Let's say $N \subset G$ is a normal subgroup, then we have an exact sequence
  $$1 \to N \to G \xrightarrow{p} H \to 1 \quad \text{where } H \simeq G/N.$$
  This does not imply that $G \simeq H \times N$, or in fact even that G contains a subgroup isomorphic to H!
  Ex: $\mathbb{Z}\cdot p \subset \mathbb{Z}$ subgroup, $0 \to \mathbb{Z}p \to \mathbb{Z} \to \mathbb{Z}/p \to 0$, but $\mathbb{Z}$ has no subgroup $\simeq \mathbb{Z}/p$.
- On the other hand, assume H can in fact be identified with a subgroup of G, via an injective homomorphism $i: H \hookrightarrow G$ s.t. $p \circ i = id_H$.

This means: N and H are subgroups of G, N is normal, and every coset of N contains a unique element of H.

so $H \simeq G/N$ is a group isomorphism, and the above set up arises as
$h \mapsto hN = Nh$
$\uparrow$ N normal

$$\begin{tikzcd} 1 \arrow[r] & N \arrow[r, hook, "\text{inclusion}"] & G \arrow[r, two heads] \arrow[rr, bend left, two heads, "p"] & G/N \arrow[r, "\sim"] & H \arrow[ll, bend left, hook, "\text{inclusion}"] \end{tikzcd}$$

Thus, every element of G can be uniquely expressed as $g = nh$, $n \in N, h \in H$
So we have a bijection of sets
$$N \times H \longrightarrow G$$
$$(n,h) \longmapsto n.h$$

This need not be a group isomorphism! (in particular because H need not be a normal subgroup of G). However, since N is normal, we do know that
$$(n_1h_1)\cdot(n_2h_2) \in (Nh_1)(Nh_2) = Nh_1h_2, \text{ in fact: } (n_1h_1)(n_2h_2) = \underbrace{(n_1h_1n_2h_1^{-1})}_{(\text{using: } N \text{ normal}) \in N}\underbrace{(h_1h_2)}_{\in H}$$

This can be interpreted as a semi-direct product of N and H:

Def: given groups N and H, and an action of H on N by automorphisms, ie. a homomorphism $\varphi: H \to \mathrm{Aut}(N)$, we define the semidirect product $N \rtimes_\varphi H$ =
- as a set: $N \times H$
- group law: $(n_1, h_1) \cdot (n_2, h_2) = (n_1\varphi(h_1)(n_2), h_1h_2)$

(check: this satisfies group axioms, in particular it's associative).

In the above setting, $H \subset G$ acts on the normal subgroup $N \subset G$ by conjugation: $\varphi(h)(n) = hnh^{-1}$ and then we find that $G \simeq N \rtimes_\varphi H$. To summarize:

Prop: If N and H are subgroups of G, N normal, st. every coset of N contains a unique element of H ($\Leftrightarrow$ every element of G is uniquely $g = n.h$), then G is isomorphic to a semidirect product $N \rtimes_\varphi H$.

Ex: $1 \to A_3 \to S_3 \xrightarrow{\text{sgn}} \mathbb{Z}/2 \to 1$, $A_3 = \{1, \sigma, \sigma^2\} \simeq \mathbb{Z}/3$ (σ 3-cycle) alternating subgp (normal)
can realize $\mathbb{Z}/2$ as subgroup $\{id, \tau\} \subset S_3$ τ transposition (not normal)
so $S_3 \simeq \mathbb{Z}/3 \rtimes \mathbb{Z}/2$ where $\mathbb{Z}/2$-action on A_3 by conjugation: $\tau\sigma\tau^{-1} = \sigma^{-1}$.

Similarly $1 \to \underset{\text{rotations}}{\mathbb{Z}/n} \to D_n \to \mathbb{Z}/2 \to 1$, $\mathbb{Z}/2 \simeq \{id, \text{reflection}\} \subset D_n$,
so $D_n \simeq \mathbb{Z}/n \rtimes \mathbb{Z}/2$. These are not $\simeq$ direct products.

Remark: if G is finite, $|G| = |H|\cdot|N|$, and $H \cap N = \{e\}$, then every coset of N contains a unique element of H; so assuming N normal we have a semidirect product, by the proposition.

Indeed: the homomorphism $\begin{array}{l} H \to G/N \\ h \mapsto hN \end{array}$ $(H \hookrightarrow G \twoheadrightarrow G/N)$ has $\ker = H \cap N = \{e\}$, so it is injective, and $|H| = |G/N|$, so it is bijective.

Alternatively: if $n_1h_1 = n_2h_2$ then $n_2^{-1}n_1 = h_2h_1^{-1} \in H \cap N = \{e\}$, so $n_1 = n_2$ and $h_1 = h_2$. Thus the products $n\cdot h$, $n \in N$, $h \in H$ are all distinct, every element of G has at most one such expression, so exactly one since $|G| = |N||H|$.

★ Finally: if both N and H are normal subgroups of G, and every element of G can be uniquely expressed as $g = n.h$, $n \in N$, $h \in H$ ($\Leftrightarrow$ every coset of one subgroup contains a unique element of the other subgroup), then $G \simeq N \times H$.

(i.e. the semidirect product is actually a direct product).

This is because cosets intersect in a single element: $nH \cap Nh = \{nh\}$ and, since H & N are normal, $(n_1h_1)(n_2h_2) \in Nh_1 \cdot Nh_2 = Nh_1h_2$

and $(n_1h_1)(n_2h_2) \in n_1H \cdot n_2H = n_1n_2H$

so $(n_1h_1)(n_2h_2) \in n_1n_2H \cap Nh_1h_2$, hence $(n_1h_1)(n_2h_2) = (n_1n_2)(h_1h_2)$

showing that $\begin{array}{l} N \times H \to G \\ (n,h) \mapsto nh \end{array}$ is now a group isomorphism.

Corollary: If G is finite, $N, H \subset G$ normal subgroups, $N \cap H = \{e\}$ and $|G| = |H|\cdot|N|$, then $G \simeq N \times H$.

Rmk: The condition $N \cap H = \{e\}$ is eg automatic if $\gcd(|N|,|H|) = 1$ (since $N \cap H$ is a subgroup of N & H so its order divides $|N|$ and $|H|$).

★ So: returning to a group G of order 15, Sylow thms $\Rightarrow$ G has unique subgroups H and K of orders 3 and 5, which are normal (uniqueness $\Rightarrow$ $gHg^{-1} = H$, $gKg^{-1} = K$)

Since $3\cdot 5 = 15$ and $\gcd(3,5) = 1$, the criterion holds and so

$G \simeq H \times K \simeq \mathbb{Z}/3 \times \mathbb{Z}/5 \simeq \mathbb{Z}/15$.

★ Another example: groups of order 21. Sylow gives the existence of subgroups H of order 3, K of order 7. Also, the number of conjugate subgroups of each of these: $s_7 \equiv 1 \bmod 7$ and $s_7 | 3$, so $s_7 = 1$; $s_3 \equiv 1 \bmod 3$ and $s_3 | 7$, so

s_3 could be either 1 or 7. If $s_3 = s_7 = 1$ then H and K are normal (since equal to their conjugates), and the above criterion implies that $G \simeq H \times K \simeq \mathbb{Z}/3 \times \mathbb{Z}/7 \simeq \mathbb{Z}/21$.

Otherwise, if $s_3 = 7$ then K is normal but H isn't: we have a semidirect product $K \rtimes H$. Let x be a generator of $K \simeq \mathbb{Z}/7$ and y a generator of $H \simeq \mathbb{Z}/3$: then $x^7 = y^3 = e$, and every element of G is uniquely expressible as $x^a y^b$, $0 \le a \le 6$, $0 \le b \le 2$. What we need to know, to determine the group structure, is the expression of $y \cdot x$. Since K is normal, $yx \in yK = Ky$ so $yx = x^\alpha y$ for some $0 \le \alpha \le 6$, ie. $yxy^{-1} = x^\alpha$. This determines the group law.

- Further investigation $\Rightarrow$ in fact there exists a unique non abelian group of order 21 up to isom. The best way to prove existence is to construct it explicitly, eg. as a subgroup of S_7 or of something else. This is on the homework!

Next time, we'll look at the proof of the Sylow theorems. For now, a couple comments:

1) Recall: $\forall g \in G$, the order of g divides $|G|$; but the converse does not hold: in general, $k \mid |G| \not\Rightarrow \exists g \in G$ of order k.

A corollary of Sylow's first theorem (existence of Sylow p-subgroups) is that the converse does hold for primes.

Corollary: if $p \mid |G|$ and p is prime then G contains an element of order p.

Pf: Let $H \subset G$ be a Sylow p-subgroup, and let $g \in H$ st. $g \neq e$. Since the order of g divides $|H| = p^e$, it is p^k for some $1 \le k \le e$. Now $g^{p^{k-1}}$ has order p. $\square$

2) For a p-group ($|G| = p^n$), Sylow tells us exactly nothing!

Namely, a Sylow p-subgroup has p^n elements, and the only such is G itself.

Thus, in the Sylow approach to classification, p-groups are the hardest to classify.

In fact, the number of different p-groups grows dramatically with the exponent n!

Eg. for $p=2$: $\exists$ 1 group of order $2^1 = 2$ (cyclic)

1	group of order	$2^1 = 2$	(cyclic)
2	—— " ——	$2^2 = 4$	$(\mathbb{Z}/4,\ \mathbb{Z}/2 \times \mathbb{Z}/2)$
5		$2^3 = 8$	
14		$2^4 = 16$	
51		$2^5 = 32$	... (and already 56092 for $2^8 = 256$)