

Frank Moore
 Algebra 901 Notes
 Professor: Tom Marley

Group Actions on Sets

Definition : Let G be a group on X a set. A **group action** (or just action) of G on X is a mapping:

$$\begin{aligned} G \times X &\rightarrow X \\ (g, x) &\mapsto gx \end{aligned}$$

Such the following properties hold:

$$\begin{aligned} g_1(g_2x) &= (g_1g_2)x & \forall g_1, g_2 \in G \\ 1x &= x & \forall x \in X \end{aligned}$$

Examples:

1. Translation of cosets : Let H be a subgroup of a group G , and let G/H denote the set of left cosets of H (Think $X = G/H$).

Let G act on G/H by $g \cdot (g'H) := (gg')H \quad \forall g, g' \in G$. The above defines an action (Check this out). (By definition, property (i) holds, as well as property (ii).

2. Conjugation : Let G act on itself via $g \cdot x := gxg^{-1} \quad \forall g, x \in G$. (Also check this out.)(we have the following:)

$$\begin{aligned} g_1 \cdot (g_2 \cdot x) &= g_1(g_2xg_2^{-1})g_1^{-1} \\ &= g_1g_2x(g_2^{-1}g_1^{-1}) \\ &= g_1g_2x(g_1g_2)^{-1} \\ &= (g_1g_2) \cdot x \end{aligned}$$

Remarks:

1. Suppose G acts on X . X is then called a G -set. Further suppose that $g \in G$. Then the map:

$$\begin{aligned} \phi_g : X &\rightarrow X \quad \text{is bijective} \\ x &\mapsto gx \end{aligned}$$

2. So, we have that ϕ_g is just a permutation of X , and we write $\phi_g \in \text{Perm}(X)$. Thus, each element of G gives rise to a permutation of X . So this gives rise to a homomorphism:

$$\begin{aligned} \phi : G &\rightarrow \text{Perm}(X) \\ g &\mapsto \phi_g \end{aligned}$$

Check that this is a group homomorphism. We have that $\phi_{gg'} : X \rightarrow X$ sending $x \mapsto gg'x$. So clearly we have $\phi(gg') = \phi_{gg'}$ by definition. We also have the following:

$$\phi(g)\phi(g') = \phi_g\phi_{g'}$$

which sends $x \xrightarrow{\phi_{g'}} g'x \xrightarrow{\phi_g} gg'x$. So the group structure is indeed preserved.

Definition: The kernel of the above mapping is called the **kernel of the action**.

$$g \in \text{the kernel of the action} \Leftrightarrow gx = x \quad \forall x \in X$$

Examples:

1. In the translation of cosets (G acting on G/H) the kernel is H ($h \cdot (gH) = gH \quad \forall g \in G$).
2. For conjugation, where G acted on G defined by:

$$g(h) = ghg^{-1}$$

$$g \in \text{kernel of this action} \Leftrightarrow gxg^{-1} = x \quad \forall x \in G \Leftrightarrow g \in Z(G)$$

Definition: An action is called **faithful** if the kernel of the action is the identity element of G .

Definition: Let X be a G -set and let $x \in X$. The **orbit** of x is defined to be:

$$Gx := \{gx \mid g \in G\}$$

Proposition: The G -orbits of X partition the set X .

Proof:

Since $x \in Gx$, $X \subseteq \bigcup_{x \in X} Gx$. So, suppose $Gx \cap Gy \neq \emptyset$, say $g_1x = g_2y$. Then, $x = g_1^{-1}g_2y$, and thus $Gx = (gg_1^{-1}g_2)y \in Gy$. So, $Gx \subseteq Gy$, and by symmetry $Gx = Gy$. So if they share even one point in common, then they are equal and thus a partition.

Definition: Let X be a G -set. Let $x \in X$. The **stabilizer**, denoted G_x , of x is

$$G_x := \{g \in G \mid gx = x\}$$

Remarks:

1. G_x is a subgroup of G (check this for yourself).
2. The kernel of the action is $\bigcup_{x \in X} G_x$ by definition.

Definition: An action is **transitive** if there is one orbit (which by the above theorem would be all of X).

Proposition Let X be a G -set. Let $x \in X$. Then the following equality holds.

$$|Gx| = [G : G_x]$$

and note that $|Gx|$ divides $|G|$ if G is finite.

Proof: We will do this by defining a bijective mapping from Gx to G/G_x . So define

$$\begin{aligned} f : G/G_x &\rightarrow Gx \\ gG_x &\mapsto gx \end{aligned}$$

Claim: f is well-defined and bijective.

$$\begin{aligned} g_1G_x = g_2G_x &\Leftrightarrow g_2^{-1}g_1 \in G_x \quad (\text{def'n of cosets}) \\ &\Leftrightarrow g_2^{-1}g_1x = x \quad (\text{in stabilizer}) \\ &\Leftrightarrow g_1x = g_2x \quad (\text{existence of inverse}) \end{aligned}$$

f is clearly surjective, so we have $|Gx| = [G : G_x]$.

Definition: Counting formula for G -sets: Let X be a G -set. Then

$$|X| = \sum [G : G_x]$$

Where the sum is over x in disjoint orbits.

Looking again at the translation of cosets, we had that G acted on G/H by $g(g'H) = (gg')H$. So, what do the orbits look like? We can look at the orbit of H , which is a perfectly good coset in G/H . So,

$$GH = \{gH \mid g \in G\}$$

It's easy to see that we only have one orbit, so this action is transitive. The aforementioned counting formula is not relevant here.

Let G be a group, H a subgroup, and let G act on G/H via $g \cdot xH := (gx)H$ where juxtaposition is the group operation. Note that $g \in G_{xH} \Leftrightarrow gxH = xH \Leftrightarrow x^{-1}gx \in H \Leftrightarrow g \in xHx^{-1}$. So we have that the stabilizer, G_{xH} is xHx^{-1} .

Remember that every group action induces a group homomorphism from the group to the permutations of the set, so we have:

$$\phi : G \rightarrow \text{Perm}(G/H).$$

The kernel of ϕ is $\ker \phi = \bigcap_{x \in G} xHx^{-1}$. This action is faithful $\Leftrightarrow \bigcap_{x \in G} xHx^{-1} = \{1\}$.

Remarks:

1. So if H is normal, the action is faithful $\Leftrightarrow H = \{1\}$, since $\ker(\phi) = H$ for H normal. In particular ϕ is injective because ϕ becomes $G \hookrightarrow \text{Perm}(G)$. Therefore G is isomorphic to a subgroup of permutations of G (Recall if $|X| = n$ then $\text{Perm}(X) \cong S_n$). Hence, if $|G| = n$, then G is isomorphic to a subgroup of S_n .
2. Since $\bigcap_{x \in G} xHx^{-1} = \ker \phi$, we see that $\bigcap_{x \in G} xHx^{-1} \triangleleft G$.

Exercise: Show that $\bigcap_{x \in G} xHx^{-1}$ is the largest normal subgroup contained in H .

Proposition: Let p be the smallest prime dividing $|G|$. Suppose \exists a subgroup H with $[G : H] = p$. Then H must be normal.

Proof: So we have the Cayley map:

$$\phi : G \rightarrow \text{Perm}(G/H) \cong S_p$$

Let $K = \ker \phi \subseteq H$. So we then have the induced map

$$\begin{aligned} \bar{\phi} : G/K &\hookrightarrow S_p \quad \text{is injective} \\ gK &\mapsto \phi(g) \end{aligned}$$

So, since $G/K \cong$ to some subgroup of S_n , $|G/K|$ divides $|S_p|$ by Lagrange's theorem. Hence $|G/K|$ divides $p!$. Therefore,

$$[G : K] = [G : H][H : K]$$

where we have $[G : H]$ by assumption. Thus, $[H : K]$ divides $(p-1)!$, but it also divides $|G|$. But p was the smallest prime dividing $|G|$ by assumption, so we have that $[H : K] = 1$. Thus, $H = K \triangleleft G$.

Corollary: If $[G : H] = 2$ then $H \triangleleft G$.

Back to Conjugation Example of Group Actions: Let G act on itself via $g \cdot x = gxg^{-1}$. So, the orbit $Gx = \{gxg^{-1} | g \in G\}$. These orbits are called **conjugacy classes** here. Notice that since the orbits partition the group, our conjugacy classes partition G .

Also notice that

$$\begin{aligned} g \in G_x &\Leftrightarrow gxg^{-1} = x \\ &\Leftrightarrow gx = xg \\ &\Leftrightarrow g \in C_G(x) = \{g \in G | gx = xg\} \end{aligned}$$

(where $C_G(x)$ is the centralizer of x in G). Recall from previous lecture that $|Gx| = [G : G_x] = [G : C_G(x)]$ in this case.

Hence we have

$$\begin{aligned} |Gx| = 1 &\Leftrightarrow G = C_G(x) \\ &\Leftrightarrow x \in \mathbb{Z}(G) = \{g \in G | ga = ag \quad \forall a \in G \end{aligned}$$

(where $\mathbb{Z}(G)$ denotes the center of the group.)

So we may refine our previous counting formula a little more to give better insight into the problem by removing all those orbits of the elements that are in the center of the group.

$$\begin{aligned} |G| &= \sum_x [G : C_G(x)] \\ &= |\mathbb{Z}(G)| + \sum_x [G : C_G(x)] \end{aligned}$$

where x runs over all distinct conjugacy classes in the first sum and all distinct conjugacy classes having 2 or more elements in the second sum. The above is known as the class formula.

Definition: Let p be a prime. A group of order p^n for some $n \geq 1$ is called a p -group.

Proposition: If G is a p -group, then $\mathbb{Z}(G) \neq \{1\}$.

Proof: If $\mathbb{Z}(G) = \{1\}$, then $|G| = p^n = 1 + \sum_i p^{\alpha_i}$ where $\alpha_i \geq 1$ because all orders of subgroups of G divide the order of G and $C_G(x)$ is a subgroup for all $x \in G$, so $[G : C_G(x)] = p^\alpha$ some $\alpha \geq 1$. If we mod out by p , we get that zero is equivalent to 1 mod p , a contradiction.

Exercise: If $G/\mathbb{Z}(G)$ is cyclic, then G is abelian.

Corollary: If $|G| = p^2$, p a prime, then G is abelian.

Proof: If $\mathbb{Z}(G) \neq G$ then $|\mathbb{Z}(G)| = p$ by Lagrange's, but that makes $|G/\mathbb{Z}(G)| = p$. Therefore $G/\mathbb{Z}(G)$ is cyclic, which in turn implies G is abelian, a contradiction.

Lemma: Let G be a finite abelian group and p a prime dividing $|G|$. Then G has an element of order p .

Proof: Induct on $|G|$. If $|G| = p$, then G is cyclic. Suppose $|G| > p$. Let $x \in G, x \neq 1$. We shall break this problem up into two cases:

1. If $p \mid o(x) = n$, then $o(x^{n/p}) = p$ and we are done.
2. If $p \nmid o(x) = n$, then $|G/\langle x \rangle| = \frac{|G|}{n} < |G|$. Also, p divides $|G/\langle x \rangle|$ since $p \nmid n$. By our inductive hypothesis, $|G/\langle x \rangle|$ has an element $\bar{y} = y\langle x \rangle$ of order p . Therefore we have $o(\bar{y}) \mid o(y) = m$. So, $o(y^{m/p}) = p$.

Some notes on normal subgroups:

1. Subgroups of G/H are of the form L/H where $H \subseteq L \subseteq G$.
2. $L/H \triangleleft G/H \Leftrightarrow L \triangleleft G$
3. If L/H is normal, then $(G/L)/(L/H) \cong G/H$.

Sylow's First Theorem: Let G be a finite group and suppose p^α divides $|G|$ for some $\alpha \geq 0$. Then G has a subgroup of order p^α . So this subgroup is then a p -group.

Proof: If $|G| = p^\alpha$, we are done, and assume that $|G| > p^\alpha$. We can create the following cases:

1. Suppose p divides $|\mathbb{Z}(G)|$. The center is abelian, so by the previous lemma we know $\exists x \in \mathbb{Z}(G) \mid o(x) = p$. Let $H = \langle x \rangle$. H is then normal in G since $x \in \mathbb{Z}(G)$. Then G/H is a group, and

$|G/H| = \frac{|G|}{p} < |G|$. Therefore $p^{\alpha-1}$ divides $|G/H|$ because p^α divided $|G|$ and $|H| = p$. Hence, by induction, G/H has a subgroup of order $p^{\alpha-1}$. So let L be a subgroup of G containing H such that $|L/H| = p^{\alpha-1}$. Therefore, $|L/H| = |L|/|H|$ which implies $|L| = |H| \cdot p^{\alpha-1} = p^\alpha$.

2. Suppose $p \nmid |\mathbb{Z}(G)|$. Then by the class formula:

$$|G| = |\mathbb{Z}(G)| + \sum_x [G : C_G(x)]$$

we must have that $p \nmid [G : C_G(x)] \forall x \notin \mathbb{Z}(G)$ by easily reducing mod p and looking at the residues. Therefore, p^α does divide $|C_G(x)| < |G|$ (why?), and by induction, $C_G(x)$ has a subgroup of order p^α , so G does as well.

Sylow's Theorem I: If p^α divides the order of G with p a prime, then G has a subgroup of order p^α .

Corollary: Cauchy's Theorem: Suppose p divides the order of G . Then G has an element of order p .

Definition: Suppose p^n divides the order of G , but p^{n+1} does not. Then a subgroup of G of order p^n is called a Sylow p -subgroup of G .

Recall: In the following notes, let H, K be finite subgroups of a group G , and define $HK := \{hk | h \in H, k \in K\}$.

1. $\frac{|H||K|}{|H \cap K|} = |HK|$
2. HK is a subgroup of $G \Leftrightarrow HK = KH$
3. If H or K is normal, then HK is normal.
4. If $H \subseteq N_G(K)$, then HK is a subgroup.

Definition: Suppose X is a G -set, $x \in X$ is called a fixed point of G if $G_x = G$, or equivalently, $Gx = \{x\}$.

Notation: Suppose p divides the order of G . Then $\text{Syl}_p(G) := \{\text{all Sylow } p\text{-subgroups}\}$ and $n_p := |\text{Syl}_p(G)|$.

Remark: If H is a subgroup of order n and $x \in G$ then xHx^{-1} is also a subgroup of order n , and xHx^{-1} is called a conjugate of H . Therefore, any conjugate of a Sylow p -subgroup is a Sylow p -subgroup. In addition, the number of conjugates of a subgroup H is $[G : N_G(H)]$.

Lemma 1: Let H be a p -subgroup of G and $P \in \text{Syl}_p(G)$ and suppose $H \subseteq N_G(H)$. Then $H \subseteq P$.

Proof: By one of the remarks, HP is a subgroup of G , and then

$$\begin{aligned} |HP| &= \frac{|H||P|}{|H \cap P|} = |P| \cdot \left(\frac{|H|}{|H \cap P|} \right) \\ &= |P| \cdot p^\alpha = p^{n+\alpha} \end{aligned}$$

Therefore, $\alpha = 0$, since $P \subseteq HP$ but P is a sylow p -subgroup . So, this implies $H = H \cap P \subseteq P$.

Lemma 2: Let X be a G -set and suppose G is a p -group. Let n be the number of fixed points of G . Then $|X| \equiv n \pmod{p}$.

Proof:

$$\begin{aligned} |X| &= \sum |Gx| \\ &= n + \sum |Gx| \end{aligned}$$

And since $|Gx|$ divides $|G|$, we know that

$$= n + \sum p^{\alpha_i}$$

For some $\alpha_i > 0$. Now modding out be p , we get

$$|X| \equiv n \pmod{p}.$$

Sylow's Second Theorem: Suppose for the following that p divides the order of G . Then

1. Any p -subgroup is contained in a Sylow p -subgroup.
2. All Sylow p -subgroups are conjugate.
3. $n_p = [G : N_G(P)]$ for any $P \in \text{Syl}_p(G)$, and in particular n_p divides $|G|/|P| = \frac{|G|}{p^n}$.
4. $n_p \equiv 1 \pmod{p}$.

Proof:

1. Let $P \in \text{Syl}_p(G)$ and let $X = \{xPx^{-1} | x \in G\}$. Then $|X| = [G : N_G(P)]$. Now let H be any p -subgroup of G , and let H act on X by conjugation (i.e. if $Q \in X$ then $h \cdot Q = hQh^{-1}$. Note that $p \nmid |X|$, since $P \subseteq N_G(X)$. By lemma 2, we have $|X| \equiv \text{fixed points of } H \pmod{p}$. Since $|X| \not\equiv 0 \pmod{p}$, \exists a fixed point of H in X , say Q . So, we know $hQh^{-1} = Q \forall h \in H$. But $Q \in X \subseteq \text{Syl}_p(G)$. The above implies that $H \subseteq N_G(Q)$ and by lemma 1, we have $H \subseteq Q$.
2. Let $P' \in \text{Syl}_p(G)$. By replacing H by P' in the previous argument, we get $P' \subseteq Q = xPx^{-1}$ (since xPx^{-1} has the same order of Q). Hence any two Sylow p -subgroups are conjugates, and thus $X = \text{Syl}_p(G)$.
3. By definition, $n_p := |X| = [G : N_G(P)]$.
4. Choose $P \in \text{Syl}_p(G)$ and $X = \{xPx^{-1} | x \in G\} = \text{Syl}_p(G)$. Let P act on X by conjugation. By the same argument as in 1, there exists a fixed point of P in X , say Q . This means that $yQy^{-1} = Q \forall y \in P$, thus $P \subseteq N_G(Q)$ which implies $P \subseteq Q$ which also implies $P = Q$. Hence, there is only one fixed point of P in X . By lemma 2, $n_p = |X| \equiv \text{number of fixed points} \equiv 1 \pmod{p}$.

Corollary: Let $P \in \text{Syl}_p(G)$. Then $P \triangleleft G \Leftrightarrow P$ is the unique sylow p -subgroup of G .

Recall Sylow's second theorem:

1. If H is a p -subgroup of G , then $H \subseteq P$ for some $P \in \text{Syl}_p(G)$.
2. $\text{Syl}_p(G) = \{xPx^{-1} \mid x \in G\}$ for any $P \in \text{Syl}_p(G)$. In other words, all Sylow p -subgroups are conjugate.
3. $n_p = [G : N_G(P)]$ for any $P \in \text{Syl}_p(G)$.
4. $n_p \equiv 1 \pmod{p}$.
5. $P \triangleleft G \Leftrightarrow n_p = 1$.

Lemma: Let G be a group and H, K be cyclic subgroups of G of orders m and n respectively. Suppose that $H \triangleleft G$ and $K \triangleleft G$. Also suppose that $(m, n) = 1$. Then HK is cyclic of order mn .

Proof: Let $H = \langle x \rangle$ and $K = \langle y \rangle$. Note that $H \cap K = \{1\}$ since $(m, n) = 1$. Now consider $xyx^{-1}y^{-1}$. We know that it is in $H \cap K$ because $xyx^{-1} \in K$ since K is normal and $yx^{-1}y^{-1} \in H$ since H is normal. So, $xy = yx$. So, $o(xy) = o(x)o(y)$, and $|HK| = \frac{|H||K|}{|H \cap K|} = mn$ so $HK = \langle xy \rangle$ and thus HK is cyclic.

Theorem: Suppose $|G| = pq$ where $p < q$ are primes, and $p \nmid (q - 1)$. Then G is cyclic.

Proof: Let $P \in \text{Syl}_p(G)$ and $Q \in \text{Syl}_q(G)$. n_p divides $q = \frac{|G|}{p}$ and is congruent to 1 mod p . So, $n_p \equiv 1$ or q , but $q \not\equiv 1 \pmod{p}$ by assumption. Therefore, we have $n_p = 1$ which would imply that $P \triangleleft G$. Also, n_q divides p and $n_q \equiv 1 \pmod{p}$ which implies $n_q = 1$ which implies that $Q \triangleleft G$. So by the previous lemma, we have that PQ is cyclic of order pq , so $G = PQ$ is cyclic.

Example: Suppose $|G| = 6$. Then either $G \cong \mathbb{Z}_6$ or $G \cong S_3$.

Proof: Let $P \in \text{Syl}_2(G)$ and $Q \in \text{Syl}_3(G)$. Then $Q \triangleleft G$ since $[G : Q] = 2$. So we have two cases, one where P is normal in G and one where P is not normal in G . If $P \triangleleft G$ then invoking the lemma we get that $G \cong \mathbb{Z}_6$. If $P \not\triangleleft G$ then considering that the Cayley map gives an isomorphism of groups, we see that $G \cong S_3$.

Example: Let G be a group of order pqr where $p < q < r$ are primes. Then one of its Sylow subgroups is normal.

Proof: We know the following is true:

1. n_p divides $qr \Rightarrow n_p = 1, q, r, qr$
2. n_q divides $pr \Rightarrow n_q = 1, r, pr$
3. n_r divides $pq \Rightarrow n_r = 1, pq$

Suppose that none of the Sylow subgroups are normal. Then $n_p \geq q, n_q \geq r, n_r = pq$. Since $P_i \cap P_j = \{1\} \forall P_i, P_j \in \text{Syl}_p(G)$, there are at least $q(p - 1)$ non-identity elements in the sylow p subgroups. Similarly, there are at least $r(q - 1)$ non-identity elements in the sylow q subgroups, and at least $pq(r - 1)$ non-identity elements in the sylow r subgroups. So adding these up, we get $pqr + rq - q - r$ non-identity elements of G , and since $r > q \geq 2$, we get a contradiction.

Example: Let G be a group of order $2^3 \cdot 7 \cdot 11 = 616$. Prove the Sylow 11 subgroup is normal.

Proof: n_{11} divides $2^3 \cdot 7$ and $n_{11} \equiv 1 \pmod{11}$, so $n_{11} = 1$ or 56 . Suppose $n_{11} > 1$. Let $Q \in \text{Syl}_{11}(G)$. So, we have $n_{11} = [G : N_G(Q)] = 56$, but $[G : Q] = 56$ so by orders we have $Q = N_G(Q)$.

Claim: Either the Sylow 2-subgroup or the Sylow 7-subgroup of G is normal.

Proof: Suppose the Sylow 7-subgroup is not normal. Then n_7 divides 88, and is congruent to 1 mod 7 which would imply that $n_7 = 8$. There are $8(7-1) = 48$ elements in the Sylow 7 subgroups and there are $56(11-1) = 560$ elements in the Sylow 11 subgroups, a total of 608. So, there are only enough elements left to form one Sylow 2 subgroup, and thus there is only one Sylow 2 subgroup which would imply that the Sylow 2 subgroup is normal.

So now, suppose the Sylow 2-subgroup is normal, and call it P . So, PQ is a subgroup of order 88. But Q is a Sylow subgroup of PQ . By Sylow's second theorem, $Q \triangleleft PQ$ therefore $PQ \subseteq N_G(Q) = Q$, a contradiction. A similar argument works for the Sylow 7-subgroup as well. So, the Sylow 11 subgroup of G is normal.

Example: Let G be a group of order $3 \cdot 5 \cdot 7 = 105$. Prove that the Sylow 5 and 7 subgroups are normal. Moreover, the Sylow 5 subgroup is contained in the center of the group.

Proof: Suppose $n_5 > 1$ and $n_7 > 1$. Then $n_5 = 21$ and $n_7 = 15$. This gives 84 non-identity elements in the Sylow 5 subgroups and $15 \cdot 6$ non-identity elements in the Sylow 7-subgroups. This is much bigger than 105 elements, so we conclude that either the Sylow 5 subgroup or the Sylow 7 subgroup is normal. Let $P \in \text{Syl}_5(G)$ and $Q \in \text{Syl}_7(G)$. Then PQ is a subgroup of order 35. Also notice that $[G : PQ] = 3$, so $PQ \triangleleft G$ since 3 is the smallest prime dividing the order of G . Also, PQ is cyclic, since $5 \nmid 7 - 1$. Let $P' \in \text{Syl}_5(G)$. Then $P' = yPy^{-1}$ for some $y \in G$, and $yPy^{-1} \subseteq yPQy^{-1} = PQ$. So P' is a Sylow 5-subgroup of PQ . Since P and P' are both Sylow 5-subgroups of PQ and PQ is abelian (cyclic), then $P = P'$. Hence $n_5 = 1$. The exact same argument works for $n_7 = 1$. For the last statement, we recall a lemma and give a definition.

Recall a Lemma: Let H, K be subgroups of G , and suppose that H, K are normal in G and that $H \cap K = \{1\}$. Then $hk = kh \quad \forall h \in H$ and $k \in K$.

Proof: Note that $hkh^{-1}k^{-1} \in H \cap K = \{1\}$.

Definition: Let H be a subgroup of G . Denote the centralizer of H in G , $C_G(H) := \{g \in G \mid gh = hg \quad \forall h \in H\}$. Note that this is a subgroup and $C_G(H) = G \Leftrightarrow H \subseteq Z(G)$.

Proof of $P \subseteq Z(G)$: Since P is cyclic, we have $P \subseteq C_G(P)$. Also, since PQ is cyclic, we have $Q \subseteq C_G(P)$. Let $R \in \text{Syl}_3(G)$. As P is normal, PR is a subgroup of G of order 15 and hence cyclic. Therefore, $R \subseteq C_G(P)$. Therefore, $G = PQR \subseteq C_G(P) \Rightarrow P \subseteq Z(G)$.

Definition: A **simple group** is a group $\neq \{1\}$, and whose only normal subgroups are 1 and itself. As an example, groups of prime order are simple.

Example: Prove that any group of order $144 = 2^4 \cdot 3^2$ is not simple.

Proof: We see that $n_3 = 1, 4$ or 16 . So, let $P \in \text{Syl}_2(G)$, $Q \in \text{Syl}_3(G)$. We break the argument up into cases.

1. $n_3 = 1$. We're done, because then the Sylow 3-subgroup is normal.
2. Suppose $n_3 = 4$. Recall $n_3 = [G : N_G(Q)] = 4$. By the Cayley map, we see that $\phi : G \rightarrow \text{Perm}(G/N_G(Q)) \cong S_4$. Since the order of G is less than the order of S_4 , we see we have a homomorphism with a non-trivial kernel. Since $\ker \phi$ is nontrivial and normal in G , G is not simple.

3. Suppose $n_3 = 16$. Let $Syl_3(G) = \{Q_1, \dots, Q_{16}\}$. We break this argument into cases as well.

- (a) $Q_i \cap Q_j = \{1\} \quad \forall i \neq j$. Then there are $16 \cdot 8 = 128$ non-identity elements on the sylow 3-subgroups, and there are 16 elements left to form the sylow 2-subgroup, and therefore its normal, causing G to not be simple.
- (b) $|Q_i \cap Q_j| = 3$ for some $i \neq j$. Reorder so that we have $|Q_1 \cap Q_2| = 3$. Consider $N = N_G(Q_1 \cap Q_2)$. Since $|Q_i| = 3^2$, we know that Q_i is abelian for all i , and therefore $Q_1 \cap Q_2$ is normal in both Q_1 and Q_2 . So we have both Q_1 and $Q_2 \subseteq N$. This implies $Q_1 Q_2 \subseteq N$. But $|Q_1 Q_2| = \frac{|Q_1||Q_2|}{|Q_1 \cap Q_2|} = 27$, hence $|N| > 27$ (because 27 does not divide the order of G). But, we also see that $9 \mid |N|$. So, we have $|N| = 36, 72$ or 144 , and thus $[G : N] \leq 4$, and by the Cayley map, we have $\phi : G \rightarrow \text{Perm}(G/N)$ to get $\ker \phi$ to be a nontrivial normal subgroup of G , hence G is not simple.

Example: Suppose $|G| = pqr$ with $p < q < r$ primes and suppose the sylow p -subgroup P is normal, and G/P is abelian. Prove that G is cyclic.

Proof: Let $Syl_q(G) = \{Q_1, \dots, Q_n\}$, $n = n_q$ and let $H_i = Q_i P$. Then H_i is a subgroup of G , as $P \triangleleft G$. H_i/P is a subgroup of G/P , and thus $H_i/P \triangleleft G/P$, $|H_i| = pq$, $|H_i/P| = q$, and $|G/P| = qr$. So, H_i/P is a sylow q -subgroup of G/P . But H_i/P is normal in G/P , so H_i/P is the only sylow subgroup of G/P , therefore $H_i/P = H_j/P \quad \forall i, j$. This implies that $H_i = H_j := H$, and also note that $Q_i \subseteq H$ for all i . In fact, Q_i are sylow q -subgroups of H and since $p < q$, there is only one sylow q -subgroup of H , and hence $n_q = 1$. Similarly, we can argue that $n_r = 1$. Thus, $P \triangleleft G, Q \triangleleft G, R \triangleleft G, P, Q, R$ cyclic of relatively prime orders, so by the lemma, $G = PQR$ is cyclic.

Direct Products of Groups:

Definition: The **external direct product** is defined to be the following: Let H_1, \dots, H_n be groups.

$$H_1 \times H_2 \times \dots \times H_n := \{(h_1, \dots, h_n) \mid h_i \in H_i\}$$

and the group operation is the componentwise operation in the respective group. For each i , let $H'_i = \{(1, \dots, h_i, \dots, 1) \mid h_i \in H_i\}$. Then the following hold (exercise):

1. Each H_i is a subgroup of G .
2. $H_i \cong H'_i$.
3. $H'_i \triangleleft G$
4. $G = H'_1 \cdots H'_n$.
5. $H'_i \cap H'_1 \cdots \hat{H}'_i \cdots H'_n = \{1\}$

Thus, the group G is 'built' out of the normal subgroups H'_1, \dots, H'_n in a special way.

Definition: Let G be a group and H_1, \dots, H_n subgroups of G . We say that G is an **internal direct product** of H_1, \dots, H_n if the following hold:

1. $H_i \triangleleft G$.
2. $G = H_1 \cdots H_n$.

$$3. H_i \cap H_1 \cdots \hat{H}_i \cdots H_n = \{1\}$$

In this case, we write $G = H_1 \times H_2 \times \cdots \times H_n$. Note that we use the same notation for both internal and external direct products. This is justified by the previous exercise and the following:

Exercise: If G is the internal direct product of H_1, \dots, H_n then G is isomorphic to the external direct product of H_1, \dots, H_n .

Proposition: Let G be a finite abelian group. Then G is the direct product of its sylow subgroups.

Proof: Suppose that $|G| = p_1^{n_1} \cdots p_k^{n_k}$, p_i distinct primes. Let P_i be a sylow p_i -subgroup. Then $P_i \triangleleft G$, $G = P_1 \cdots P_k$, and $P_i \cap P_1 \cdots \hat{P}_i \cdots P_k = \{1\}$, and therefore $G = P_1 \times P_2 \times \cdots \times P_k$, where P_i is an abelian group of order $p_i^{n_i}$.

Question: What do abelian groups of order p^n look like? From the structure theorem for finitely generated abelian groups, if P is abelian and $|P| = p^n$, then there exists **unique** integers $n_1 \geq n_2 \geq \cdots \geq n_k$ such that

$$P \cong C_{p_1^{n_1}} \times C_{p_2^{n_2}} \times \cdots \times C_{p_k^{n_k}}$$

where C_m is a cyclic group of order m .

Example: How many non-isomorphic abelian groups are there of order 2^5 ?

1. C_{32}
2. $C_{16} \times C_2$
3. $C_8 \times C_4$
4. $C_8 \times C_2 \times C_2$
5. $C_4 \times C_4 \times C_2$
6. $C_4 \times C_2 \times C_2 \times C_2$
7. $C_2 \times C_2 \times C_2 \times C_2 \times C_2$

Example: How many non-isomorphic abelian groups of order $2^5 \cdot 3^2 \cdot 5^3$ are there? There are 7 possibilities of the sylow 2-subgroup, 2 possibilities of the sylow 3-subgroup, and 3 possibilities for the sylow 5-subgroup. Therefore there are 42 “isomorphism classes” of abelian groups of order $2^5 \cdot 3^2 \cdot 5^3$.

Example: Let $|G| = 3 \cdot 5 \cdot 7$. Then $G = C_5 \times H$ where $|H| = 21$.

Proof: We’ve already proved that the Sylow 5-subgroup and Sylow 7-subgroup of G is normal. Let $P \in \text{Syl}_3(G)$, $Q \in \text{Syl}_5(G)$, $R \in \text{Syl}_7(G)$. So, $Q \triangleleft G$, and $R \triangleleft G$.

Let $H = PR$. Since $|G/R| = 15$, and $3 \nmid 5 - 1$, we know G/R is cyclic. Hence, $H/R \triangleleft \Rightarrow H \triangleleft G$. Since $G = PQR = QH$, $Q \cap H = \{1\}$ and both Q and H are normal, we see that $G = Q \times H$.

We’ll see later that there are only two non-isomorphic groups of order 21 (one abelian and one non-abelian), therefore there are only two non-isomorphic groups of order 105.

Automorphism Groups

Definition: Let G be a group. The **automorphism group** of G is defined by:

$$\text{Aut}(G) := \{\phi \mid \phi : G \rightarrow G \text{ is an isomorphism}\}$$

This is easily seen to be a group under the operation of composition.

The most easily understood automorphisms are those given by conjugation by an element:

Definition: Let $g \in G$, and define $\psi_g : G \rightarrow G$ which maps $x \in G$ to gxg^{-1} . Then ψ_g is a group homomorphism, with additional properties:

$$(\psi_g)^{-1} = \psi_{g^{-1}}, \psi_g \circ \psi_h = \psi_{gh}$$

ψ_g is called an **inner automorphism** of G .

The set of inner automorphisms:

$$\text{Inn}(G) := \{\psi_g \mid g \in G\}$$

is a subgroup of $\text{Aut}(G)$, and in fact, we see that $\phi\psi_g\phi^{-1} = \psi_{\phi(g)}$ for all $g \in G, \phi \in \text{Aut}(G)$, so we see that $\text{Inn}(G) \triangleleft \text{Aut}(G)$.

Finally, if one considers the surjective group homomorphism:

$$f : G \rightarrow \text{Inn}(G)$$

$$g \mapsto \psi_g$$

one sees that $\ker f = Z(G)$, giving $\text{Inn}(G) \cong G/Z(G)$.

Important Remark: Let $\psi \in \text{Inn}(G)$ and $H \triangleleft G$. Then $\psi|_H \in \text{Aut}(H)$. (Also note that $\psi|_H$ is in general not an inner automorphism of H).

We want to compute the automorphism group for some “easy” groups. First, let's recall the concept of a group of units:

Definition: Let R be a ring with identity. Let

$$R^* := \{u \in R \mid u \text{ is a unit of } R\}$$

Then R^* is a group under multiplication. For example, consider \mathbb{Z}_n^* , and it is easy to see that \mathbb{Z}_n^* is a group under multiplication of order $\phi(n)$ where ϕ is the Euler phi-function. Also, $M_{n \times n}(\mathbb{R})^* = GL_n(\mathbb{R})$. We are ready for a theorem.

Theorem: $\text{Aut}(C_n) \cong \mathbb{Z}_n^*$.

Proof: Let $C_n = \langle [a] \rangle$ and suppose $\phi : \langle [a] \rangle \rightarrow \langle [a] \rangle$ is an isomorphism. Suppose $\phi(a) = a^k$. Then $\phi(a^i) = \phi(a)^i = (a^k)^i$. Therefore, $\text{im } \phi = \langle [a^k] \rangle$. Since ϕ is surjective, $\langle [a^k] \rangle = \langle [a] \rangle$. Therefore $(k, n) = 1$, so $\bar{k} \in \mathbb{Z}_n^*$.

Now define

$$f : \text{Aut}(C_n) \rightarrow \mathbb{Z}_n^* \\ \phi \mapsto \bar{k} \text{ where } \phi(a) = a^k$$

f is well-defined: Suppose $\phi(a) = a^k = a^l$. Then $a^{k-l} = 1 \Rightarrow n|(k-l) \Rightarrow \bar{k} = \bar{l}$.

f is a homomorphism: Left as an exercise (easy to see).

f is a monomorphism: If $f(\phi) = \bar{1}$ then $\phi(a) = a$, and therefore $\phi = 1$.

f is an endomorphism: If $k \in \mathbb{Z}_n^*$ then $\langle [a^k] \rangle = \langle [a] \rangle$ which implies $\phi : \langle [a] \rangle \rightarrow \langle [a] \rangle$ which sends a to a^k is an automorphism of C_n . So $f(\phi) = \bar{k}$ and therefore f is onto.

Note that \mathbb{Z}_n is a cyclic group but \mathbb{Z}_n^* is not in general. For example, \mathbb{Z}_{15}^* has no element of order 8 (which is the order of the group). In fact, suppose $n = kl$ where $(k, l) = 1$ and $k, l > 2$. By the Chinese Remainder Theorem, we have $\mathbb{Z}_n \cong \mathbb{Z}_k \times \mathbb{Z}_l$ which implies that $\mathbb{Z}_n \cong (\mathbb{Z}_k \times \mathbb{Z}_l)^* \cong \mathbb{Z}_k^* \times \mathbb{Z}_l^*$, which is not cyclic, since $\phi(k)$ and $\phi(l)$ are both even (exercise).

Theorem: Let F be a field and H a finite subgroup of F^* . Then H is cyclic.

Proof: It is enough to show that each Sylow subgroup of H is cyclic, since H is abelian, this would mean that H is the direct product of cyclic subgroups of relatively prime order.) Hence, we may assume that $|H| = p^n$, for some prime p . Then

$$H \cong C_{p^{n_1}} \times C_{p^{n_2}} \times \cdots \times C_{p^{n_k}}$$

where $n_1 \geq n_2 \geq \cdots \geq n_k$. Hence $h^{p^{n_1}} = 1$ for all $h \in H$. If H is not cyclic, then $n_1 < n$, or equivalently, $k \geq 2$. Let $f(x) = x^{p^{n_1}} - 1 \in F[x]$. Since $f(h) = 0$ for all $h \in H \subseteq F$, $f(x)$ has at least p^n roots. But $p^n > p^{n_1}$, a contradiction.

Corollary: If p is prime, $\mathbb{Z}_p^* \cong C_{p-1}$, and in particular, $\text{Aut}(\mathbb{Z}_p) \cong C_{p-1}$.

Example: Find an automorphism of C_{13} of order 6.

We know that $\text{Aut}(C_{13}) \cong \mathbb{Z}_{13}^*$. As $2^6 \equiv -1 \pmod{13}$, we see that $\mathbb{Z}_{13}^* = \langle [2] \rangle$. So, we know that $2^2 = 4$ is an element of order 6 in \mathbb{Z}_{13}^* . Hence, letting $C_{13} = \langle [a] \rangle$, an automorphism of order 6 is given by:

$$\begin{aligned} \phi : C_{13} &\rightarrow C_{13} \\ a &\mapsto a^4 \end{aligned}$$

Example: Find $\phi \in \text{Aut}(C_{35})$ such that ϕ has order 12.

We know that $\text{Aut}(C_{35}) \cong \mathbb{Z}_{35}^* \cong \mathbb{Z}_5^* \times \mathbb{Z}_7^*$. The Chinese Remainder Theorem isomorphism:

$$\begin{aligned} \mathbb{Z}_{35}^* &\rightarrow \mathbb{Z}_5^* \times \mathbb{Z}_7^* \\ \bar{a} &\mapsto (\bar{a}, \bar{a}) \end{aligned}$$

Now, \mathbb{Z}_5^* is cyclic of order 4, and \mathbb{Z}_7^* is cyclic of order 6. An element of order 4 in \mathbb{Z}_5^* is $\bar{2}$, and an element of order 3 in \mathbb{Z}_7^* is $\bar{4}$. Hence, $(\bar{2}, \bar{4}) \in \mathbb{Z}_5^* \times \mathbb{Z}_7^*$ has order 12. Therefore, we see that 32 is an element of order 12 in \mathbb{Z}_{35}^* . Hence, setting $C_{35} = \langle [a] \rangle$, we see that an automorphism of order 12 is given by:

$$\phi : C_{35} \rightarrow C_{35}$$

$$a \mapsto a^{12}$$

Theorem: Let $p > 2$ be prime. Then $\mathbb{Z}_{p^n}^*$ is cyclic of order $p^n - p^{n-1}$.

Proof: We know that $|\mathbb{Z}_{p^n}^*| = \phi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$. Since $\mathbb{Z}_{p^n}^*$ is cyclic, it is enough to show all of its Sylow subgroups are cyclic.

Exercise: $(1+p)^{p^{n-1}} \equiv 1 \pmod{p^n}$ but $(1+p)^{p^{n-2}} \not\equiv 1 \pmod{p^n}$.

Therefore, we see that $[1+p]_{p^n} \in \mathbb{Z}_{p^n}^*$ is an element of order p^{n-1} . Therefore, the sylow p -subgroup of $\mathbb{Z}_{p^n}^*$ is cyclic. Now consider the group homomorphism defined by:

$$\begin{aligned} \psi : \mathbb{Z}_{p^n}^* &\rightarrow \mathbb{Z}_p^* \\ [a]_{p^n} &\mapsto [a]_p \end{aligned}$$

Note that since $(a, p^n) = 1 \Leftrightarrow (a, p) = 1$, we have

$$[a]_{p^n} \in \mathbb{Z}_{p^n}^* \Leftrightarrow [a]_p \in \mathbb{Z}_p^*$$

Therefore, we see that ψ is well-defined and surjective. Since $|\mathbb{Z}_{p^n}^*| = p^{n-1}(p-1)$ and $|\mathbb{Z}_p^*| = p-1$, we see that $|\ker \psi| = p^{n-1}$.

Let Q be a Sylow q -subgroup of $\mathbb{Z}_{p^n}^*$, with $q \neq p$. Then, since $Q \cap \ker \psi = \{1\}$, Q is isomorphic to a subgroup of \mathbb{Z}_p^* . Since \mathbb{Z}_p^* is cyclic and subgroups of cyclic groups are cyclic, we see that Q is cyclic, completing the proof.

Recall the Chinese Remainder Theorem: If $(m, n) = 1$ then the map:

$$\begin{aligned} f : \mathbb{Z}_{mn} &\rightarrow \mathbb{Z}_m \times \mathbb{Z}_n \\ [a]_{mn} &\mapsto ([a]_m, [a]_n) \end{aligned}$$

is a ring isomorphism. Therefore, we see that $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ as additive groups. In addition, there is also a group isomorphism $\mathbb{Z}_{mn}^* \cong \mathbb{Z}_m^* \times \mathbb{Z}_n^*$ as multiplicative groups.

Fact: If p is prime, then \mathbb{Z}_p^* is cyclic.

Theorem: Let $p > 2$ be prime. Then $\mathbb{Z}_{p^n}^*$ is cyclic of order $\phi(p^n) = p^{n-1}(p-1)$.

Proof: Of course $\mathbb{Z}_{p^n}^*$ is abelian. We also know that $\mathbb{Z}_{p^n}^*$ is the direct product of its sylow subgroups. So it is enough to show each of its sylow subgroups are cyclic. Let P be the sylow p -subgroup. Then $|P| = p^{n-1}$. As in the previous lecture, we see that $(1+p)$ has order p^{n-1} in $\mathbb{Z}_{p^n}^*$ so P is cyclic. So let Q be a sylow q -subgroup where q is a prime dividing $p-1$. Define a map:

$$\begin{aligned} h : \mathbb{Z}_{p^n}^* &\rightarrow \mathbb{Z}_p^* \\ [a]_{p^n} &\mapsto [a]_p \end{aligned}$$

is a well-defined group homomorphism (Note $[a]_{p^n} = [b]_{p^n} \Leftrightarrow p^n | a - b \Rightarrow p | a - b \Leftrightarrow [a]_p = [b]_p$. Also, $[a]_{p^n} \in \mathbb{Z}_{p^n}^* \Leftrightarrow (a, p^n) = 1 \rightarrow (a, p) = 1 \Leftrightarrow a \in \mathbb{Z}_p^*$. Also, we see that h is surjective (clearly), so we have $\mathbb{Z}_{p^n}^* / \ker h \cong \mathbb{Z}_p^*$. Therefore, as $Q \neq P$, we have $Q \cap \ker h = \{1\}$. Therefore, $h|_Q : Q \rightarrow \mathbb{Z}_p^*$ is injective, so Q is isomorphic to a subgroup of \mathbb{Z}_p^* , but \mathbb{Z}_p^* is cyclic, so Q is cyclic also.

Theorem: $\text{Aut}(C_n) \cong \mathbb{Z}_n^*$. We proved this last time.

Corollary: $\text{Aut}(C_{p^n})$ is cyclic of order $p^{n-1}(p-1)$ if $p > 2$.

Example: $\text{Aut}(C_{27})$ is cyclic of order 18. We notice that the order of $\bar{2}$ is 18. So, we see that the map

$$\begin{aligned}\phi : C_{27} &\rightarrow C_{27} \\ a &\mapsto a^2\end{aligned}$$

is an automorphism in $\text{Aut}(C_{27})$ of order 18. Also, we can see that

$$\begin{aligned}\psi : C_{27} &\rightarrow C_{27} \\ a &\mapsto a^6\end{aligned}$$

has order 6.

Suppose $G = C_p \times C_p \times \cdots \times C_p$ (n times). Since $C_p \cong \mathbb{Z}_p$ is a field, G is a \mathbb{Z}_p -vector space of dimension n . So we see that

$$\text{Aut}(G) \cong \text{Aut}(\mathbb{Z}_p^n)$$

Where the Aut's on the left are group automorphisms and the Aut's on the right are vector space automorphisms, which are the same as invertible linear transformations. So, as a remark, $\phi : \mathbb{Z}_p^n \rightarrow \mathbb{Z}_p^n$ is a group isomorphism $\Leftrightarrow \phi$ is a bijective linear transformation. We define the action of the vector space as follows:

Linearity: $\phi(\bar{a} + \bar{b}) = \phi(\bar{a}) + \phi(\bar{b})$.

Scalar Mult: $\phi(\bar{r} \cdot \bar{a}) = \bar{r}\phi(\bar{a}) = \phi(\bar{a}) + \phi(\bar{a}) + \cdots + \phi(\bar{a})$ (n times).

Another Remark:

$$\begin{aligned}\text{Aut}(C_p \times C_p \times \cdots \times C_p) &= \{\phi : \mathbb{Z}_p^n \rightarrow \mathbb{Z}_p^n\} \\ &= \{n \times n \text{ vertices over } \mathbb{Z}_p \text{ with determinant nonzero}\} \\ &= GL_n(\mathbb{Z}_p)\end{aligned}$$

Proposition: $|GL_n(\mathbb{Z}_p)| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$.

Proof: It is sufficient to count the number of bases of the vector space we are considering. In the first row, we have $p^n - 1$ choices, in the second row, we have $p^n - p$ choices, and so on, giving the proof.

Corollary: $|\text{Aut}(C_p \times C_p \times \cdots \times C_p)| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$.

Example: $|\text{Aut}(C_5 \times C_5)| = (5^2 - 1)(5^2 - 5) = 480$.

Semidirect Products:

Definition: Let H, K be groups and let $\phi : K \rightarrow \text{Aut}(H)$ be a group homomorphism. Define the (external) **semidirect product** of H and K (wrt ϕ) to be $H \rtimes_{\phi} K = \{(h, k) | h \in H, k \in K\}$ with the following operation:

$$(h_1, k_1)(h_2, k_2) := (h_1\phi(k_1)(h_2), k_1k_2)$$

Claim: This set under the operation listed above forms a group.

Proof:

Closed: The operation is clearly closed.

Associativity: Exercise.

Identity: $(1, 1)(h, k) = (1\phi(1)(h), k)$ and because homomorphisms take identity to identity (the identity map), we get $(1(h), k) = (h, k)$. For the other side, we see $(h, k)(1, 1) = (h\phi(k)(1), k) = (h \cdot 1, k) = (h, k)$ since $\phi(k)(1) = 1$ because automorphisms take identity to identity.

Inverse of (h, k) : Consider $(h, k)^{-1} = (\phi(k^{-1}(h^{-1}), k^{-1})$. Lets check if this works:

Right side: $(h, k)(\phi(k^{-1}(h^{-1}), k^{-1})) = (h\phi(k)[\phi(k^{-1}(h^{-1})], 1)$ by definition of the operation, and then we have $(h\phi(kk^{-1})(h^{-1}), 1)$ because ϕ was a homomorphism, and this gives $(h \cdot h^{-1}, 1) = (1, 1)$ because $\phi(kk^{-1}) = \text{identity on } H$.

Left side: $(\phi(k^{-1}(h^{-1}), k^{-1})(h, k) = (\phi(k^{-1}(h^{-1})\phi(k^{-1}(h), 1)$ by definition, which gives $(\phi(k^{-1}(h^{-1}h), 1)$ because $\phi(k^{-1})$ is an automorphism, which gives $\phi(k^{-1}(1), 1) = (1, 1)$.

Remark: Let $G = H \rtimes_{\phi} K$. Then the following hold:

- Let $H' = \{(h, 1) | h \in H\}$ and $K' = \{(1, k) | k \in K\}$. Then H' and K' are subgroups of G , and $H' \cong H$, $K' \cong K$. Also note that the funkiness of the semidirect product's operation goes away when either component is 1 in both of the elements in G .
- $G = H'K'$. $(h, k) = (h, 1)(1, k) \neq (1, k)(h, 1)$.
- $H' \cap K' = \{1\}$.
- $H' \triangleleft G$.

Proof: Let $(h', 1) \in H'$, and $(h, k) \in G$. Then $(h, k)(h', 1)(h, k)^{-1} = (h, k)(h, 1)(\phi(k^{-1}(h^{-1}), k^{-1})) = (*, 1) \in H'$.

Theorem: Let $G = H \rtimes_{\phi} K$. Then the following conditions are equivalent:

- ϕ is the trivial map ($\phi : k \mapsto 1_H \ \forall k \in K$).
- $G = H \times K$.
- $K' \triangleleft G$.

Proof: (1) \Rightarrow (2). $(h_1, k_1)(h_2, k_2) = (h_1h_2, k_1k_2)$ if ϕ is trivial, so $G = H \times K$. (2) \Rightarrow (3) is easy, since by definition, if you have G is a direct product of groups, $K' \triangleleft G$. (3) \Rightarrow (1): We know that $H' \triangleleft G$ and $H' \cap K' = \{1\}$. As K' is normal, we have $h'k' = k'h'$ for all $h' \in H'$ and $k' \in K'$, so the conjugation is trivial.

Corollary: $H \rtimes_{\phi} K$ is abelian $\Leftrightarrow \phi$ is trivial and H, K are abelian.

Example: Find the smallest odd integer n such that \exists a non-abelian group of order n . Smallest n that would work is 21, because $3|7-1$. So, try $C_7 \rtimes_{\phi} C_3$ where $\phi : C_3 \rightarrow \text{Aut}(C_7)$ with ϕ non-trivial. Note that $\text{Aut}(C_7) \cong Z_7^* \cong Z_6$. Say $C_3 = \langle a \rangle$ and $C_7 = \langle b \rangle$. To define ϕ with ϕ being nontrivial, we want $\phi(a)$ to be an automorphism of C_7 with order dividing 3 that is not 1, so the order of ϕ must be 3. So, we define ϕ as follows:

$$\begin{aligned} \phi : C_3 &\rightarrow \text{Aut}(C_7) \\ a &\mapsto \left[\begin{array}{c} \psi : C_7 \rightarrow C_7 \\ b \mapsto b^2 \end{array} \right] \end{aligned}$$

Note that the order of $\phi(a) = |\psi| = 3$ in the group of automorphisms of C_7 , so we have succeeded. So, we have $C_7 \rtimes_{\phi} C_3$ is a nonabelian group of order 21.

Note: Consider $C_p \rtimes_{\phi} C_q$, where $\phi : C_q \rightarrow \text{Aut}(C_p)$. Then there exists a nontrivial $\phi \Leftrightarrow q \nmid p-1$.

Theorem: Let $p < q$ be primes. Then \exists a non-abelian group of order $pq \Leftrightarrow q \equiv 1 \pmod{p}$.

Proof: “ \Rightarrow ”: If $q \not\equiv 1 \pmod{p}$, then any group of order pq is cyclic by the lemma. “*Leftarrow*”: Suppose $q \equiv 1 \pmod{p}$. Then $p|q-1 = |\text{Aut}(C_q)|$. Therefore, \exists an automorphism $\psi \in \text{Aut}(C_q)$ of order p . Define $\phi : C_p = \langle a \rangle \rightarrow \text{Aut}(C_q)$ which sends $a \mapsto \psi$, which is a nontrivial homomorphism and therefore $C_q \rtimes_{\phi} C_p$ is a nonabelian group of order pq .

Presentations: A way of describing groups and relations which define the group. If there are no relations, the group is said to be free. What follows is a loose description of presentations. A formal definition involves a look into free groups, and normal subgroups containing the relations.

Notation:

$$\langle x_1, \dots, x_n | w_1 = 1, \dots, w_n = 1 \rangle$$

where the w_i are ‘words’: $w_i = x_{i_1}^{\alpha_1}$ where $x_{i_j} \in \{x_1, \dots, x_n\}$. For example: $\langle x, y, z | x^2y = 1, xy^{-1}z^3 = 1 \rangle$ would be a presentation of some group.

Examples:

1. $\langle x | \emptyset \rangle$ is a presentation of the integers.
2. $\langle x | x^n = 1 \rangle = C_n$
3. $\langle x, y | \emptyset \rangle$ is a presentation of the free group on 2 elements.
4. $\langle x, y | xy = yx \rangle = \mathbb{Z} \times \mathbb{Z}$ which is the free abelian group on 2 elements.
5. $\langle a, b | a^2 = 1, b^2 = 1, ab = ba \rangle$ is $Z_2 \times Z_2$, also known as the Klein 4-group.
6. $D_8 = \langle x, y | x^4 = 1, y^2 = 1, yx = x^{-1}y \rangle$
7. $Q_8 = \langle x, y | x^4 = 1, x^2 = y^2, yx = x^{-1}y \rangle$.

Example: Create a presentation for the nonabelian group of order 21 we constructed last time: Let $G = C_7 \rtimes C_3$, $C_7 = \langle b \rangle$, $C_3 = \langle a \rangle$, ϕ is such that:

$$\phi : C_3 \rightarrow \text{Aut}(C_7)$$

$$a \mapsto \left[\begin{array}{l} \psi : C_7 \rightarrow C_7 \\ b \mapsto b^2 \end{array} \right]$$

Let $x = (b, 1)$, $y = (1, a)$. Notice that $o(x) = 7$ and $o(y) = 3$, and by the counting theorem, we have that $G = \langle x \rangle \langle y \rangle$. So, $G = \langle x, y \rangle$, and we investigate what relations define G . Obviously, we have $x^7 = 1$ and $y^3 = 1$. Consider:

$$\begin{aligned} yx &= (1, a)(b, 1) \\ &= (1\phi(a)(b), a) \\ &= (b^2, a) \end{aligned}$$

So, we see that $G = \langle x, y | x^7 = 1, y^3 = 1, yx = x^2y \rangle$.

Definition: Let G be an abelian group. Define $f : G \rightarrow G$ to send $a \in G$ to $a^{-1} \in G$. Since $f^2 = f \circ f = \text{Id}_G$, f is an automorphism of G . f is called the inversion map. $o(f) = 2$ unless $a^2 = 1 \ \forall a \in G$.

Example: Let $n > 2$ be an integer, $C_2 = \langle a \rangle$ be a cyclic group of order 2, and $C_n = \langle b \rangle$ be a cyclic group of order n . Define

$$\phi : C_2 \rightarrow \text{Aut}(C_n)$$

$$a \mapsto f$$

where f is the inversion map defined above. So, ϕ is non-trivial, and therefore $C_n \rtimes_{\phi} C_2$ is a nonabelian group of order $2n$ called the dihedral group. We now find a presentation for D_{2n} .

Let $x = (b, 1)$, $y = (1, a)$. As before, $G = \langle x, y \rangle = \{x^i y^j | 0 \leq i \leq n-1, 0 \leq j \leq 1\}$ since any power of x looks like $(b^n, 1)$ and any power of y looks like $(1, a)$. We know that $x^n = 1$, $y^2 = 1$ and considering yx , we see that $(1, a)(b, 1) = (b^{-1}, a) = x^{-1}y$. So, a presentation for D_{2n} is as follows:

$$D_{2n} = \langle x, y | x^n = 1, y^2 = 1, yx = x^{-1}y \rangle$$

Internal Semidirect Products:

Recall for direct products, we have that $G = HK$, $H \cap K = \{1\}$, and $H \triangleleft G$ and $K \triangleleft G$ together imply that $G = H \times K$.

Theorem/Definition: Let G be a group and suppose \exists subgroups H, K such that $G = HK$, $H \cap K = \{1\}$, and $H \triangleleft G$. Then \exists a homomorphism $\phi : K \rightarrow \text{Aut}(H)$ such that $G \cong H \rtimes_{\phi} K$.

In this situation, G is the internal semi-direct product of H and K . A note first, the notion of internal and external semi-direct product is only a formal distinction, since if H and K are groups, you can consider them living inside $G := H \rtimes_{\phi} K$. So, this terminology is justified by the previous isomorphism (i.e. the direct product).

Recall, in light of the above comment, we talked about $G = H \rtimes_{\phi} K$, and we noted that $G = H'K'$, $H' \triangleleft G$ and $H' \cap K' = \{1\}$, so we really have talked about this before.

Proof: Let $y \in K$ and consider the inner automorphism ψ_y on G :

$$\begin{aligned}\psi_y : G &\rightarrow G \\ x &\mapsto yxy^{-1}\end{aligned}$$

So, $\psi_y(H) = yHy^{-1} = H$ as $H \triangleleft G$. So, $\psi_y|_H \in \text{Aut}(H)$. Define ϕ to be the following:

$$\begin{aligned}\phi : K &\rightarrow \text{Aut}(H) \\ y &\mapsto \psi_y|_H\end{aligned}$$

This is clearly a group homomorphism. Now, define f to be the following:

$$\begin{aligned}f : H \rtimes_{\phi} G &\rightarrow G \\ (h, k) &\mapsto hk\end{aligned}$$

Clearly this map is well defined, is 1-1 and onto by assumption on the conditions of H and K , so what is left to show is that f is a group homomorphism.

$$\begin{aligned}f((h_1, k_1)(h_2, k_2)) &= f((h_1k_1h_2k_1^{-1}, k_1k_2)) \\ &= h_1k_1h_2k_1^{-1}k_1k_2 \\ &= h_1k_1h_2k_2 \\ &= f((h_1, k_1))f((h_2, k_2))\end{aligned}$$

Therefore, f is an isomorphism.

Theorem: Let G be a group of order $2p$ where p is a prime bigger than 2. Then $G \cong C_{2p}$ or $G \cong D_{2p} \cong C_p \rtimes C_2$.

Proof: Let $P \in \text{Syl}_2(G)$, $Q \in \text{Syl}_p(G)$. We know that $Q \triangleleft G$, as $[G : Q] = 2$, and $G = PQ$, and $P \cap Q = \{1\}$. So, $G = Q \rtimes_{\phi} P$ for some $\phi : Q \rightarrow \text{Aut}(P)$. Let $P = \langle y \rangle$ where $o(y) = 2$. So, $\phi(y)$ has order 1 or 2 in $\text{Aut}(Q)$. If $|\phi(y)| = 1$ then $\phi(y) = \text{Id}_Q$, so $G = Q \times P \cong C_2 \times C_p \cong C_{2p}$. Now $\text{Aut}(Q)$ is cyclic of order $p-1$. Therefore \exists exactly one element of order 2 in $\text{Aut}(Q)$, given by inversion. So $G \cong D_{2p}$ by our previous construction. I.e., if $Q = \langle x \rangle$, then $yxy^{-1} = x^{-1}$ or $yx = x^{-1}y$, so G has the presentation

$$G = \langle x, y \mid x^p = 1, y^2 = 1, yx = x^{-1}y \rangle \cong D_{2p}.$$

Lemma(Theorem): Let K be a cyclic group of order n , H an arbitrary group, and let $\phi_1, \phi_2 : K \rightarrow \text{Aut}(H)$ be group homomorphisms. Suppose $\phi_1(K)$ and $\phi_2(K)$ are conjugate subgroups of $\text{Aut}(H)$. Then $H \rtimes_{\phi_1} K \cong H \rtimes_{\phi_2} K$. Important special cases are when $\phi_1(K) = \phi_2(K)$ or when $\phi_1(K)$ and $\phi_2(K)$ are Sylow p -subgroups.

Proof:???

Major Example I: Classify all groups up to order 12. So, let $P \in \text{Syl}_2(G)$ and $Q \in \text{Syl}_3(G)$. By a homework problem (on groups of order p^2q , either P or Q is normal. Note first that we have 2 abelian ones, namely C_{12} and $C_2 \times C_2 \times C_3 \cong C_2 \times C_6$. We will break the nonabelian argument into cases.

1. $P \triangleleft G$. Therefore, $P \rtimes_{\phi} Q$ for some $\phi : Q \rightarrow \text{Aut}(P)$.
 - (a) Suppose $P \cong C_4$. So $\text{Aut}P \cong \mathbb{Z}_4^* \cong C_2$. Since $|Q| = 3$, $\phi : Q \rightarrow \text{Aut}(P)$ must be trivial, so no new nonabelian groups.
 - (b) Suppose $P \cong C_2 \times C_2$. So $\text{Aut}(P) \cong GL_2(\mathbb{Z}_2)$, and $|GL_2(\mathbb{Z}_2)| = 6$. Thus, if ϕ sends Q to a subgroup of order 3 in $\text{Aut}(P)$, we get a nontrivial homomorphism and since $\phi(Q)$ is a sylow 3-subgroup, we see there is only one non-abelian group in this case, namely $(C_2 \times C_2) \rtimes_{\phi} C_3$. Note that this is A_4 .
2. $Q \triangleleft G$. So $G = Q \rtimes_{\phi} P$ and $\text{Aut}(Q) \cong \mathbb{Z}_3^*$. So $\phi : P \rightarrow \text{Aut}(Q)$.
 - (a) Say $P \cong C_4$, and set $P = \langle x \rangle$ and $Q = \langle y \rangle$. Define $\phi : P \rightarrow \text{Aut}(Q)$ by sending x to the inversion map on Q . Therefore, conjugation by an element from P inverts an element in Q . So, a presentation is: $\langle x, y \mid x^4 = 1, y^3 = 1, xyx^{-1} = y^{-1} \rangle$. This is not isomorphic to A_4 since the sylow 2-subgroup is not normal.
 - (b) Suppose $P \cong C_2 \times C_2$. Suppose that $\phi : P \rightarrow \text{Aut}(Q)$ is nontrivial. Then ϕ must be surjective as $|\text{Aut}(Q)| = 2$. Therefore, $|\ker \phi| = 1$. Let $\ker \phi = \langle a \rangle$. Then $\phi(a) = \text{Id}_Q$. But $\phi(a)$ really is conjugation by a , so $aq a^{-1} = q$ for all $q \in Q$. Let $H = \langle a \rangle$. Then HQ is a subgroup of G as $Q \triangleleft G$. Also, we have that $|HQ| = 6$, hence $HQ \triangleleft G$ by indexes. Also, since $o(a) = 2$ and $o(y) = 3$ and $ay = ya$, $o(ay) = 6$ so that $HQ \cong C_6$. Let $b \notin \ker \phi$, and let $K = \langle b \rangle$ (note that $o(b) = 2$). Also, note that $K \cap HQ = \{1\}$ so that $G = HQ \rtimes_{\phi} K$ where ϕ is again the map sending b to inversion on HQ . This group is exactly D_{12} .

Major Example II: Classify all groups up to order $20 = 2^2 \cdot 5$. Let $P \in \text{Syl}_2(G)$ and $Q \in \text{Syl}_5(G)$. By Sylow's Theorems, we immediately have that $Q \triangleleft G$. Also, set $Q = \langle y \rangle$. Therefore, we have that $G \cong Q \rtimes_{\phi} P$, where $\phi : P \rightarrow \text{Aut}(Q) \cong \mathbb{Z}_5^*$.

1. Case 1: $P \cong C_4$. Let $P = \langle x \rangle$. Then we know that $\phi(x)$ is an automorphism of order 1, 2, or 4.
 - (a) If $o(\phi(x)) = 1$, then ϕ is the trivial map and so $G = Q \times P \cong C_{20}$.
 - (b) If $o(\phi(x)) = 2$, then ϕ is the inversion map, so we have that $G = \langle x, y \mid x^4 = 1, y^5 = 1, xyx^{-1} = y^4 \rangle$.
 - (c) If $o(\phi(x)) = 4$, then in this case $\phi(P) = \text{Aut}(Q)$. By the theorem from last class any two such ϕ 's give rise to isomorphic semidirect products. Let $\phi(x)$ be the automorphism sending $y \mapsto y^2$. Then $xyx^{-1} = y^2$ so we have that $G = \langle x, y \mid x^4, y^5, xyx^{-1} = y^2 \rangle$.
2. Case 2: $P \cong C_2 \times C_2$. Consider $\ker \phi$ where $\phi : P \rightarrow \text{Aut}(Q)$. Note that $|\ker \phi| = 1, 2$ or 4 .
 - (a) $|\ker \phi| = 4$: Then ϕ is the trivial map and hence $G = C_2 \times C_2 \times C_5$.
 - (b) $|\ker \phi| = 1$: Cannot happen since $C_2 \times C_2 \not\cong \mathbb{Z}_5^*$.
 - (c) $|\ker \phi| = 2$: Let $x \in \ker \phi \setminus \{1\}$. Therefore $\phi(x)$, which is conjugation by x , induces the trivial map on Q , so that $xqx^{-1} = q$ for all $q \in Q$. Let $H = \langle x \rangle Q$. Then $|H| = 10$ and H is abelian so we have that $H \cong C_{10}$. Also, by indexes, H is normal in G . So, glue the groups together via the inversion map again and you get D_{20} as in the case where we were looking at groups of order 12.

Lemma: Suppose $m \nmid n$ where $m, n \in \mathbb{Z}^+$. Let $s \in \mathbb{Z}$ such that $(s, m) = 1$. Then there exists a $t \in \mathbb{Z}$ such that $(s + tm, n) = 1$.

Lemma: Let $\phi : C_n \rightarrow C_m$ be a surjective group homomorphism, and let $C_n = \langle a \rangle$ and $C_m = \langle b \rangle$. Then $b = \phi(a^r)$ where $(r, n) = 1$. Just use the above lemma to prove this result - follow your nose.

Theorem: Let K be a cyclic group of order n and H an arbitrary group. Let $\phi_1, \phi_2 : K \rightarrow \text{Aut}(H)$ be two group homomorphisms such that $\phi_1(K)$ and $\phi_2(K)$ are conjugate. Then $H \rtimes_{\phi_1} K \cong H \rtimes_{\phi_2} K$.

Proof: Let $K = \langle a \rangle \cong C_n$. Then $\phi_2(K) = \sigma\phi_1(K)\sigma^{-1}$ for some $\sigma \in \text{Aut}(H)$. Then note that $\sigma\phi_1(K)\sigma^{-1} = \sigma\phi_1(\langle a \rangle)\sigma^{-1} = \langle \sigma\phi_1(a)\sigma^{-1} \rangle$. Now apply the lemma to $\phi : K \rightarrow \langle \sigma\phi_1(a)\sigma^{-1} \rangle$. Then $\sigma\phi_1(a)\sigma^{-1} = \phi_2(a^r)$ for some r with $(r, n) = 1$. Now, notice that for any $s \in \mathbb{Z}$, we have that

$$\sigma\phi_1(a^s)\sigma^{-1} = \sigma\phi_1(a)^s\sigma^{-1} = (\sigma\phi_1(a)\sigma^{-1})^s = \phi_2(a^r)^s = \phi_2((a^s)^r)$$

Therefore, for any $x \in K$, we have that $\sigma\phi_1(x)\sigma^{-1} = \phi_2(x^r)$, i.e. $\sigma\phi_1(x) = \phi_2(x^r)\sigma$. Now we may define our isomorphism:

$$\begin{aligned} f : H \rtimes_{\phi_1} K &\rightarrow H \rtimes_{\phi_2} K \\ (h, k) &\mapsto (\sigma(h), k^r) \end{aligned}$$

Now we check that it is in fact an isomorphism.

- **1-1:** If $f(h, k) = (1, 1)$, then $\sigma(h) = 1$ and so $h = 1$ since σ was an automorphism of H . If $k^r = 1$, $o(k) \mid r$ so $o(k) = 1$ since we had that $(r, n) = 1$. Therefore, $k = 1$.
- **Onto:** Let $(h', k') \in H \rtimes_{\phi_2} K$. Since σ is onto, $\exists h \in H$ such that $\sigma(h) = h'$. Since $(r, n) = 1$, $rs + nt = 1$ for suitable s and t . Then $k' = (k')^1 = (k')^{rs+nt} = ((k')^s)^r$ (as the n term goes away since K is cyclic of order n). So, let $k = (k')^s$. Then $f(h, k) = (h', k')$.
- **Hom:**

$$\begin{aligned} f((h_1, k_1)(h_2, k_2)) &= f(h_1\phi_1(k_1)h_2, k_1k_2) \\ &= (\sigma(h_1\phi_1(k_1)h_2), k_1^r k_2^r) \\ &= (\sigma(h_1)\sigma(\phi_1(k_1)h_2), k_1^r k_2^r) \\ &= (\sigma(h_1)\phi_2(k_1^r)\sigma(h_2), k_1^r k_2^r) \\ &= (\sigma(h_1), k_1^r)(\sigma(h_2), k_2^r) \\ &= f(h_1, k_1)f(h_2, k_2) \end{aligned}$$

Major Example III: Let's compute all groups of order 30. Let $P \in \text{Syl}_2(G)$, $Q \in \text{Syl}_3(G)$ and $R \in \text{Syl}_5(G)$.

Either Q or R are normal:

Proof: If not, $n_3 = 10$ and $n_5 = 6$ by Sylow's theorems. This is way too many elements since the intersections of these have to be trivial.

So, let $P = \langle x \rangle$. By the above claim, we have that QR is a subgroup of G , and we know that QR is the cyclic group of order 15. Furthermore, since $[G : QR] = 2$, we know that $QR \triangleleft G$. Hence, $G \cong QR \rtimes_{\phi} P$ where $\phi : P \rightarrow \text{Aut}(QR) \cong \mathbb{Z}_{15}^*$. If ϕ is trivial, then G is cyclic of order 30, and if ϕ is the map that sends

x to inversion, then $G = D_{30}$ as before. So, we have that $G \cong C_{15} \rtimes_{\phi} C_2$ where $\phi : C_2 \rightarrow \text{Aut}(C_{15}) \cong Z_{15}^*$. Note that there are 3 elements of order 2 in $\text{Aut}(C_{15})$, namely -1 (inversion), 4 and 11. So we have 3 nontrivial choices for $\phi(a)$:

1. $\phi(a) : C_{15} \rightarrow C_{15}$ where $\phi(a)(b) = b^{-1}$, the inversion map. Here, $G \cong D_{30}$.
2. $\phi(a) : C_{15} \rightarrow C_{15}$ where $\phi(a)(b) = b^4$. Then we have a presentation $\langle x, y \mid x^2 = 1, y^{15} = 1, xyx^{-1} = y^4 \rangle$.
3. $\phi(a) : C_{15} \rightarrow C_{15}$ where $\phi(a)(b) = b^{11}$. Then we have a presentation $\langle x, y \mid x^2 = 1, y^{15} = 1, xyx^{-1} = y^{11} \rangle$.

Now how can we tell these groups apart? Lets consider their centers. The possible orders for $Z(G)$ to force G to be a nonabelian group are 1, 3, 5 (since if $G/Z(G)$ is cyclic, G is abelian). In all cases, note that $Z(G)$ is cyclic, so lets say that $Z(G) = \{1\}$ or $Z(G) = \langle b^5 \rangle$, the unique Sylow 3-subgroup or $Z(G) = \langle b^3 \rangle$, the unique Sylow 5-subgroup. It can be checked that each of the above groups has exactly one of the above as its center. Just look at $\phi(a)(b^5)$ and $\phi(a)(b^3)$ to see if they are in the kernel, as that means conjugation by that element is trivial, i.e. it is in the center.

Definition: Let G be a group, and H a subgroup of G . Then H is called a characteristic subgroup of G provided $\phi(H) = H$ for all $\phi \in \text{Aut}(G)$. We will write $H \text{ Char } G$. Note that in general, it is enough to show that $\phi(H) \subseteq H$ for all $\phi \in \text{Aut}(G)$.

Remarks:

1. $H \text{ Char } G$ implies that $H \triangleleft G$, since $\text{Inn}(G) \subset (\text{indeed a normal subgroup of}) \text{Aut}(G)$.
2. $H \triangleleft G \not\Rightarrow H \text{ Char } G$. For example, let $G = V_4$ (the Klein 4-group). Then $\phi(\langle a \rangle) = \langle b \rangle$ for an automorphism ϕ , but $\langle a \rangle$ is normal in G . Therefore, $\langle a \rangle$ is not characteristic.
3. If $|H| < \infty$ and H is the unique subgroup of order $|H|$, then $H \text{ Char } G$, just by comparing the orders of H and $\phi(H)$ and noting that since ϕ is an automorphism we have that $\phi(H) = H$ because H is the only subgroup of that order.
4. If G is cyclic of finite order, then every subgroup is characteristic. (Corollary of the above)
5. If $P \in \text{Syl}_p(G)$ then $P \triangleleft G \Leftrightarrow P \text{ Char } G$. (Also a corollary to the above)
6. If $K \triangleleft H$ and $H \triangleleft G$ we know that this does not imply that $K \triangleleft G$. (Take, for example, D_8 , and $H = \{1, x^2, y, x^2y\}$ and $K = \langle y \rangle$. Then $K \triangleleft H$ and $H \triangleleft G$ but $K \not\triangleleft G$.)
7. We do have the following facts, however:
 - (a) $K \text{ Char } H$ and $H \text{ Char } G$ implies that $K \text{ Char } G$. (restrict an automorphism of G to H to get an automorphism of H since $H \text{ Char } G$. Then apply this to K).
 - (b) $K \text{ Char } H$ and $H \triangleleft G$ implies that $K \triangleleft G$. (consider inner automorphisms of G)
 - (c) Let $P \in \text{Syl}_p(G)$. Then $P \triangleleft H$ and $H \triangleleft G$ implies that $P \triangleleft G$.

Definition: Let G be a group. Then the commutator subgroup of G is the subgroup generated by the set $\{aba^{-1}b^{-1} \mid a, b \in G\}$, and is denoted by G' or $G^{(1)}$.

Remarks:

1. G is abelian if and only if $G' = \{1\}$.
2. G' Char G : Let $\phi \in \text{Aut}(G)$. It's enough to show that $\phi(G') \subseteq G'$. Let $aba^{-1}b^{-1} \in G'$. Then $\phi(aba^{-1}b^{-1}) = \phi(a)\phi(b)\phi(a)^{-1}\phi(b)^{-1} \in G'$, hence G' Char G . Hence in particular, we have that $G \triangleleft G$.

Proposition: Let H be a subgroup of G . Then $G' \subseteq H \Leftrightarrow H \triangleleft G$ and G/H is abelian.

Proof: " \Rightarrow ": G' Char G so $G' \triangleleft G$, but in G/G' , we have that $xy = yx$ so that G/G' is abelian. Therefore, $H/G' \triangleleft G/G'$ by the correspondence theorem, and therefore, $H \triangleleft G$. Also, the third isomorphism theorem tells you that G/H is the quotient of abelian groups and hence abelian.

" \Leftarrow ": Suppose $H \triangleleft G$ and G/H is abelian. Let $a, b \in G$. Then $aHbH = bHaH$ which implies that $aba^{-1}b^{-1} \in H$, so $G' \subseteq H$.

Definition: Let higher commutator subgroups of G we define as follows: $G^{(0)} = G$, $G^{(1)} = G'$, and in general, $G^{(i+1)} = (G^{(i)})'$ (the commutator subgroup of the i th commutator). The sequence of subgroups

$$\dots \triangleleft G^{(i+1)} \triangleleft G^{(i)} \triangleleft \dots \triangleleft G^{(1)} \triangleleft G^{(0)} = G$$

is called the **derived series** of G . Note that any factor groups of the above are abelian, and furthermore we have that $G^{(i+1)}$ Char $G^{(i)}$ and by transitivity we have that $G^{(i)}$ Char G for all i .

Definition: A sequence of subgroups of G

$$\{1\} = H_n \triangleleft H_{n-1} \triangleleft \dots \triangleleft H_1 \triangleleft H_0 = H$$

is called a **normal series** for G . The factor groups for the series are $\{H_i/H_{i+1}\}$.

A **solvable series** for G is a normal series in which the factor groups are abelian. G is said to be **solvable** if it has a solvable series.

Examples:

1. If G is abelian, then G is solvable.
2. Let $G = D_{2n} = C_n \rtimes C_2$. Then $\{1\} \triangleleft C_n \triangleleft D_{2n}$ is a solvable series for D_{2n} .
3. Let $G = A_4$. We know that $P \triangleleft A_4$ where $P \in \text{Syl}_2(G)$. Therefore, we have that $\{1\} \triangleleft P \triangleleft A_4$ is a solvable series for A_4 (in fact, $A'_4 = P$).

Theorem: Let G be a group. Then G is solvable $\Leftrightarrow G^{(n)} = \{1\}$ for some n .

Proof: " \Leftarrow " This direction is trivial since if $G^{(n)} = \{1\}$ for some n , then the derived series for G gives us a solvable series.

" \Rightarrow ": Suppose that $\{1\} = G_n \triangleleft G_{n-1} \triangleleft \dots \triangleleft G_1 \triangleleft G_0 = G$ is a solvable series for G . First we prove a claim:

Claim: $G^{(i)} \subseteq G_i$ for all i .

Proof of Claim: The case $i = 0$ is trivial, since both are G . So, suppose that $G^{(i)} \subseteq G_i$ for some i . We know that G_i/G_{i+1} is abelian, so $G_{i+1} \supset G'_i \supset (G^{(i)})' = G^{(i+1)}$. Therefore, $G^{(n)} = G_n = \{1\}$. Therefore, we have that $G^{(n)} = \{1\}$, as desired. The gist of this argument is that the derived series is as short as any solvable series could possibly be, however it is in practice often very hard to compute all the derived subgroups by hand.

Lemma: Let $\phi : A \rightarrow B$ be a group homomorphism. Then $\phi(A^{\{n\}}) = \phi(A)^{(n)} = (\text{im}\phi)^{\{n\}}$, for all $n \geq 0$.

Proof: We proceed by induction on n . When $n = 0$, the result is trivial. Let $n = 1$. Since A' is generated by $S = \{aba^{-1}b^{-1}\}$ we know that $\phi(A')$ is generated by $\phi(S) = \{\phi(a)\phi(b)\phi(a)^{-1}\phi(b)^{-1}\}$. But $\phi(A)'$ is generated by the same elements, so $\phi(A)' = \phi(A')$. The general case is identical to this one.

Corollary: Let $\phi : A \rightarrow B$ be a group homomorphism. If A is solvable then so is $\text{im}\phi$.

Theorem: Let G be a group, and H a subgroup of G . Then if G is solvable then so is H . Furthermore, suppose $H \triangleleft G$. Then G is solvable $\Leftrightarrow H$ is solvable and G/H is solvable.

Proof: Clearly, we have that $H^{(i)} \subseteq G^{(i)}$. If G is solvable then $G^{(n)} = \{1\}$ for some n and hence $H^{(n)} = \{1\}$, so H is solvable. For the second assertion, let us prove the forward direction first. So, let G be solvable. By the first assertion, H is solvable. Consider $\phi : G \rightarrow G/H$ the natural surjection. By the corollary, we have that G/H is solvable. For the reverse direction, suppose H and G/H are solvable. Let $\phi : G \rightarrow G/H$ be as above. We know G/H is solvable so $(G/H)^{(n)} = \{1\}$. But $\phi(G^{(n)}) = \phi(G)^{(n)} = (G/H)^{(n)} = \{1\}$. Therefore, $G^{(n)} \subset \ker \phi = H$. As H is solvable, $H^{(k)} = \{1\}$ for some k . So $G^{(n+k)} = \{1\}$ so that G is solvable.

Theorem: Let G be a p -group, p a prime. Then G is solvable.

Proof: Say $|G| = p^n$. Use induction on n . If $n \leq 2$, then G is abelian so automatically solvable. Suppose that $n \geq 3$. We know that $\exists H \leq G$ so that $|H| = p^{n-1}$. Since $[G : H] = p$ we immediately have that $H \triangleleft G$. Thus H is solvable by induction, and G/H is cyclic so solvable. So G is solvable.

Example: Any group of order $1998 = 2 \cdot 3^3 \cdot 37$ is solvable.

Proof: Let $Q \in \text{Syl}_3(G)$. By Sylow's theorems, $Q \triangleleft G$, and also Q is cyclic, so Q is solvable. So it is enough to show that G/Q is solvable. Let G' be any group of order $2 \cdot 3^3$. Then the Sylow 3-subgroup is normal and by the last theorem, it is solvable. Also, G'/P is cyclic, so solvable, thus G' is solvable.

Burnside's Theorem (1904): Any group of order $p^n q^l$ where p and q are primes, is solvable.

Feit-Thompson's Theorem (1963): Any group of odd order is solvable.

Theorem: A_5 is simple. First we prove a couple of claims:

Claim 1: Suppose that $H \triangleleft A_5$, where H is a proper subgroup. Then $5 \nmid |H|$.

Proof of Claim 1: Suppose $5 \mid |H|$. Then H contains a Sylow 5-subgroup of A_5 . As $H \triangleleft A_5$, H contains all conjugates of this Sylow 5-subgroup. Therefore H contains all elements of order 5. The elements of order 5 are 5-cycles. There are $4!$ 5-cycles. So H contains at least 24 elements plus the identity so 25 elements. Since $|H| \mid 60$ and $|H| < 60$, $|H| = 30$. But any group of order 30 has a normal Sylow 3-subgroup by our earlier discussion, hence a contradiction.

Claim 2: If A_5 is not simple then A_5 contains a normal subgroup of order 2, 3, or 4.

Proof of Claim 2: Let H be a proper normal subgroup of A_5 . By Claim 1, $|H| = 2, 3, 4, 6$ or 12 . If

$|H| = 6$ then the Sylow 3-subgroup of H (and of A_5) is normal by Sylow's theorems. Therefore $P \triangleleft G$. If $|H| = 12$, then the Sylow 2 or Sylow 3 subgroup of H is normal in H and hence in A_5 .

Proof of Theorem: Assume that A_5 is not simple. Let K be the normal subgroup given by claim 2. Then $|A/K| = 30, 20, 15$. Then the Sylow 5-subgroup H/K or A/K is normal. Then $H \triangleleft A_5$, but $|H/K| = 5$ contradicting claim 1. Therefore A_5 is simple. Note that A_n is simple for $n \geq 5$.

Corollary: S_n is not solvable for $n \geq 5$. Indeed, if S_5 were solvable, then so is A_5 . But A_5 is simple and nonabelian, so not solvable. Hence S_5 is not solvable. Since S_5 is isomorphic to a subgroup of S_n for $n \geq 5$, S_n is not solvable.