9/16

Free abelian groups & finitely generated abelian groups §2.1, 2.2

A (too) optimistic goal would be to classify all groups up to isomorphism. But for important classes of groups, this is possible. We will do it for a subclass (finitely generated) of abelian groups.

First we need to talk about free abelian groups.

Def'n Let G be an abelian group. A subset $B \subseteq G$ is called a basis (or base) is every element $g \in G$ has a unique expression as $g = \sum_{i=1}^{n} m_i x_i$ with $m_i \in \mathbb{Z}$ and $x_i \in B$.

(Here and throughout we use additive notation for abelian groups)

G is called free if it posseses a basis.

Rmk: This is very similar to notion of basis in linear algebra (over a field) except that the coefficients are in $\mathbb{Z}$.

Thm Let G be a free abelian group and let B_1, B_2 be two bases of G. Then the cardinalities of B_1 and B_2 are the same.

Def'n The rank of a free abelian group G is the cardinality of (any one of its) bases.

Thm Let G be a free abelian group of finite rank n. Then $G \cong \mathbb{Z}^n$.

Rmk: In fact even for G of infinite rank ω we have $G \cong \mathbb{Z}^{\omega}$ if this is interpreted suitably (have to use direct sum rather than direct product).

Rmk: We have presentation $\mathbb{Z}^n = \langle x_1, x_2, \ldots, x_n \mid x_i x_j = x_j x_i \rangle$ (making the generators commute makes all elements commute).

Just like every group is a quotient of a free group, every abelian group is a quotient of a free abelian group. We will restrict our attention to finitely generated abelian groups because these are more tractable.

Thm Let G be a finitely generated abelian group, generated by n elements $x_1, \dots, x_n$. Then $G \cong \mathbb{Z}^n / H$ for some subgroup $H \leq G$.

All of the previous theorems are relatively straightforward. Now we come to the classification theorem, which is more involved:

Thm (Classification of Finitely Generated Abelian Groups)
Let G be a finitely generated abelian group, then there are unique integers $r \geq 0$, $m_1, m_2, \dots, m_k$ with $m_1 \geq 2$ and $m_1 | m_2 | \cdots | m_k$ "divides"
such that $G \cong \mathbb{Z}^r \oplus \mathbb{Z}/m_1\mathbb{Z} \oplus \mathbb{Z}/m_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_k\mathbb{Z}$.

Of course, we can have $r=0$ (if G is finite) or $k=0$ (if G is free).

Def'n An element $x \in G$ of a (not necessarily abelian) group G is called torsion if $x^n = 1$ for some $n \geq 1$.

In an abelian group G, the set $Tor(G)$ of torsion elements (which in additive notation have $nx = 0$ for some $n \geq 1$) forms a subgroup, called the torsion subgroup (or torsion part) of G.

G is called torsion-free if $Tor(G) = \{0\}$ and in general $G/Tor(G)$ is called the torsion-free part of G.

So the classification says that for an finitely-gen. abelian gr. G, the torsion part is $\mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_k\mathbb{Z}$ and the torsion-free part is $\mathbb{Z}^r$.

Cor For G a fin. gen. abelian gp., also can write G uniquely as

$$G \simeq \mathbb{Z}^r \oplus \mathbb{Z}/p_1^{s_1}\mathbb{Z} \oplus \mathbb{Z}/p_2^{s_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_\ell^{s_\ell}\mathbb{Z}$$

where the $p_1, p_2, \ldots, p_\ell$ are prime numbers (allowed to repeat).

Pf of corollary from thm: If n and m are coprime then $\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$ (exercise for you!)

Thus if $m = p_1^{a_1} p_2^{a_2} \cdots p_\ell^{a_\ell}$ is the prime factorization of m, then $\mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/p_1^{a_1}\mathbb{Z} \oplus \mathbb{Z}/p_2^{a_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_\ell^{a_\ell}\mathbb{Z}$. ☒

Remark The integers $m_1 | m_2 | \cdots | m_k$ from thm are the invariant factors of G. The prime powers $p_1^{s_1}, \ldots, p_\ell^{s_\ell}$ from cor. are the elementary divisors of G.

E.g. $G = \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ is the invariant factor representation, equiv. to $G = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, elementary divisor rep.

So how to prove classification of fin. gen. abelian groups?

We know $G \simeq \mathbb{Z}^n/H$ for some subgroup $H \leq \mathbb{Z}^n$.

Normally (haha) we've been quotienting by kernels of homomorphisms, but since we're dealing with abelian gp's, we can quotient by images.

The cokernel, $\mathrm{coker}(\varphi)$, of a homomorphism $\varphi: \mathbb{Z}^m \to \mathbb{Z}^n$ is $\mathbb{Z}^n/\mathrm{im}(\varphi)$, the codomain mod the image.

We can represent φ by a $n \times m$ matrix: $y_1, \ldots, y_m$ are gen's of $\mathbb{Z}^m$; with integer coeff's; $x_1, \ldots, x_n$ are gen's of $\mathbb{Z}^n$

φ represented by M

e.g. $\begin{bmatrix} 3 & 0 & 1 \\ 2 & 1 & -4 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = [\underbrace{3y_1 + y_3}_{\cdot x_1}, \underbrace{2y_1 + y_2 - 4y_3}_{\cdot x_2}]$ for $y_1, \ldots, y_3 \in \mathbb{Z}$.

Small exercise: We can take m finite, i.e., we only need to impose finitely many relations.

So any fin. gen. ab. gp. G is of form $G \simeq \mathrm{coker}(\varphi)$ for some $\varphi: \mathbb{Z}^m \to \mathbb{Z}^n$.
So we need to understand structure of cokernels of $\mathbb{Z}$-matrices.

<u>Thm</u> (<u>Smith</u> <u>Normal</u> <u>Form</u>) Let $\varphi: \mathbb{Z}^m \to \mathbb{Z}^n$ be a homo. represented by a $n \times m$ matrix M with coeff's in $\mathbb{Z}$.
Then $M = SDT$ where T $n \times n$ matrix, S $m \times m$ matrix are <u>invertible</u> <u>over</u> $\mathbb{Z}$ and $D = (d_{ij})$ is a $\mathbb{Z}$-matrix whose off-diagonal $(i \neq j)$ entries are zero and whose diagonal entries $m_i = d_{i,i} \geq 0$ satisfy $m_1 \mid m_2 \mid m_3 \mid \cdots \mid m_K$.

<u>E.g.</u> A matrix in SNF looks like $D = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 6 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$. The cokernel will be $\mathrm{coker}(D) = \cancel{\mathbb{Z}/1\mathbb{Z}} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/0 \cdot \mathbb{Z}$
$= \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ in the form we want!

Since multiplying on left and right by invertible over $\mathbb{Z}$ matrices does not change the $\mathbb{Z}$-image, this proves the classification!

To prove the Smith Normal Form theorem, we need an <u>algorithm</u> that tells us how to convert M to SNF via a series of $\mathbb{Z}$-invertible row and column operations:

e.g. $M = \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix} \xrightarrow[\text{col from 1st}]{\text{sub. 2nd}} \begin{bmatrix} 1 & 1 \\ -2 & 2 \end{bmatrix} \xrightarrow[\text{and add 1st row to 2nd}]{\text{sub. 1st col from 2nd,}} \begin{bmatrix} 1 & 0 \\ 0 & 4 \end{bmatrix} = D$ ✓

<u>Think</u>: RREF and Gaussian elimination. But I skip the full description of the SNF algorithm.

<u>Remark</u>: In fact SNF works for <u>free modules</u> over any <u>PID</u> (<u>Principal</u> <u>Ideal</u> <u>Domain</u>). We may return to this later in the semester... //

9/18

Action of a group on a set §2.4

Groups are often collections of symmetries. Let's take this idea further.

Def'n Let G be a group and X a set. An action of G on X is a function $G \times X \to X$, denoted $(g,x) \mapsto g \cdot x$, such that $e \cdot x = x$ $\forall x \in X$ and $(gh)x = g(hx)$ $\forall g,h \in G, x \in X$.

E.g. The symmetric group S_n acts on $X = \{1,2,\dots,n\}$ by $\sigma \cdot i = \sigma(i)$ for all $\sigma \in S_n$, $i \in X$.

In fact, in general an action of G on X is the same as a homomorphism $G \to S_X$ (the symmetric group of bijections $X \to X$) where $g \in G$ is sent to the function $g \cdot x$, for $x \in X$.
We say the action is faithful if this homomorphism is a monomorphism, i.e., if $g \cdot x = x$ $\forall x \in X$ implies $g = e$.

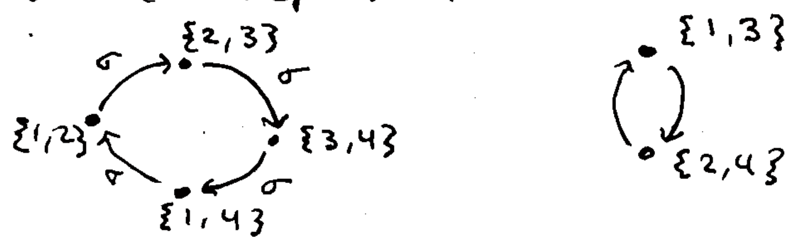
Prop. Every group G acts faithfully on itself $X = G$ by (left) translation: $g \cdot h = gh$.
Proof: Straightforward. $\boxtimes$

Cor (Cayley) Every finite group G of order n embeds as a subgroup of the symmetric group S_n.

Any embedding of G as a subgroup $G \leq S_n$ gives an action of G on $[n] := \{1,2,3,\dots,n\}$.
E.g. $G = \mathbb{Z}/4\mathbb{Z} \cong \langle \sigma \rangle \leq S_4$ with $\sigma = (1,2,3,4)$

gives standard action of G on $\{1,2,3,4\}$.
But from this we can get more actions on other sets...

For example, G also acts on $X = \binom{[4]}{2} = \{2\text{-element subsets of } [4]\}$ in a natural way: $\sigma \cdot S = \{\sigma(i) : i \in S\}$ $\forall\, S \in X$.
We can represent this action via this directed graph:



$\Leftarrow$ 2 orbits of $G \curvearrowright X$

<u>Prop.</u> Let $G \curvearrowright X$ ("G act on X"). Define $x \sim y$ for $x, y \in X$ if $\exists\, g \in G$ s.t. $g \cdot x = y$. Then $\sim$ is an equiv. rel. on X.

<u>Def'n</u> When $G \curvearrowright X$ the equivalence class $\bar{x}$ of $x \in X$ under this equivalence relation is called the <u>orbit</u> of x.

<u>Prop.</u> Let $G \curvearrowright X$ and $x \in X$. Then $G_x = \{g \in G : g \cdot x = x\}$ is a subgroup of G.

<u>Def'n</u> This G_x is called the <u>stabilizer</u> of $x \in X$.

<u>Thm</u> (Orbit-Stabilizer Theorem) Let $G \curvearrowright X$. Then for any $x \in X$, the cardinality of the orbit of x is $[G : G_x]$.
In particular if G is finite, size of orbit of x is $\dfrac{|G|}{|G_x|}$.

<u>Pf.</u> Notice $gx = hx$ for $g, h \in G \iff g^{-1}h\,x = x \iff g^{-1}h \in G_x \iff hG_x = gG_x$ so elements in x's orbit are in bijection w/ cosets of stabilizer G_x $\boxtimes$

<u>E.g.</u> In the previous example, taking $S = \{1,2\}$, the stabilizer is $G_{\{1,2\}} = \{e\}$, and orbit has size $4 = \frac{4}{1}$.
But with $S' = \{1,3\}$, the stabilizer is $G_{\{1,3\}} = \{e, \sigma^2\}$ and orbit has size $2 = \frac{4}{2}$.

We said before that G acts on itself via (left) translation, but there is another action of G on itself that is very important:

Def'n G acts on $X = G$ by conjugation $(g, h) \mapsto ghg^{-1}$.
We always write this as ghg^{-1} to avoid confusion with $g \cdot h$.
The orbit of $x \in G$ under the conjugation action is called the conjugacy class of x, i.e., $\{gxg^{-1} : g \in G\}$.
The stabilizer of $x \in G$ under the conjugation action is called the centralizer of x, denoted $C_G(x) = \{g \in G : gx = xg\}$.

Def'n The center of G, denoted $Z(G)$, is the set of elements in G that commute with all elements of G, i.e. $Z(G) = \{g \in G : gh = hg \ \ \forall h \in G\}$.

Prop. $Z(G)$ is a normal subgroup of G.
Pf: Straightforward. ∎

Prop. $Z(G) = \{g \in G : C_G(x) = G\}$. Pf: Again, immediate from definition ∎

Thm (Class Equation) Let G be a finite group and let $x_1, \dots, x_n$ be representatives of the conjugacy classes of G.
Then $|G| = \sum_{i=1}^{n} [G : C_G(x_i)]$.
If $x_1, \dots, x_m$ are representatives of the conjugacy classes that contain more than one element, then
$$|G| = |Z(G)| + \sum_{i=1}^{m} [G : C_G(x_i)].$$

Pf: The conjugacy classes partition G, so the first equality is clear from the orbit-stabilizer theorem.
Then notice $x \in Z(G) \Leftrightarrow [G : C_G(x)] = 1$, so 2^{nd} equality follows. ∎

Let's use the class equation to say something about finite p-groups; an important class of finite groups.

<u>Def'n</u> G is a finite <u>p-group</u> (for p a prime number) if the order of G is p^n for some $n \geq 0$.

<u>Thm</u> Let G be a nonabelian finite p-group. Then $Z(G)$ is a nontrivial normal subgroup ($\neq \{e\}$ or G), so G is <u>not</u> simple.

<u>Pf</u>: Look at the class equation $|G| = |Z(G)| + \sum_{i=1}^{m} [G : C_G(x_i)]$.
By ~~assumption~~ Lagrange's thm, p divides $[G : C_G(x_i)]$ for all the x_i, since $[G : C_G(x_i)] \neq 1$ (or else these x_i would be in $Z(G)$). Also clearly p divides $|G|$ by assumption. So then p divides $|Z(G)|$. But $|Z(G)| \neq 0$ since $e \in Z(G)$. So $Z(G)$ must have some other element in it besides e, and so $Z(G)$ is nontrivial. Also $Z(G) \neq G$ since G is nonabelian. ☒

We also showed on the homework that the only groups G that have no nontrivial subgroups are $\mathbb{Z}/p\mathbb{Z}$ for p prime, hence these are the only abelian simple groups.

<u>Cor</u> The only finite simple p-groups are $\mathbb{Z}/p\mathbb{Z}$.

<u>Note</u>: A more general definition of p-group is a group G such that the order of every $g \in G$ is a power of p. We will see soon (using Cauchy's thm) why this matches our definition in the case of finite groups.

We will develop more tools to show that finite groups of various orders cannot be simple, in order to possibly understand all finite simple groups (a big goal!)

9/23

The Sylow Theorems §2.5

We have seen how the arithmetic properties of n have a strong influence on the structure of a finite group G of order n, e.g., Lagrange's Theorem says the order of every subgroup H of G divides n. But not every divisor appears as the order of a subgroup.

E.g. The alternating group A_5 of order 60 is simple, so it cannot have a subgroup of order 30 (index $2 \Rightarrow$ normal).

Similarly, order of any element $g \in G$ must divide n, but not every divisor of n appears as an order. However every prime divisor of n does appear as an order, as we now show.

Theorem (Cauchy) Let G be a finite group of order n and let p be a prime number dividing n. ~~There~~ there is $g \in G$ of order p.

To prove this we need a lemma about $\mathbb{Z}/p\mathbb{Z}$ actions:

Lemma Let G be a finite group of order p^n for p a prime acting on a finite set S. Let $S_0 = \{x \in S : gx = x \ \forall g \in G\}$ be the set of singleton orbits under G. Then $|S| \equiv |S_0| \mod p$.

Pf: $|S| = |S_0| + \sum_{\mathcal{O}} |\mathcal{O}|$ where the sum is over all non-singleton orbits $\mathcal{O}$. By the orbit-stabilizer theorem and Lagrange, p divides each $|\mathcal{O}|$, which means $|S| \equiv |S_0| \mod p$. ◻

Pf of Cauchy's thm: Let $S = \{(g_1, g_2, \dots, g_p) : g_i \in G,\ g_1 \cdot g_2 \cdots g_p = e\}$.

Notice that $g_1, \dots, g_{p-1}$ can be arbitrary if we set $g_p = (g_1 \cdots g_{p-1})^{-1}$, which means that $|S| = n^{p-1}$. Next notice that $\mathbb{Z}/p\mathbb{Z} = \langle \sigma \rangle$ acts on S by setting $\sigma \cdot (g_1, \dots, g_p) = (g_p, g_1, \dots, g_{p-1})$ (since if $g_1 \cdots g_p = e$ then $g_p g_1 \cdots g_{p-1} = g_p g_1 \cdots g_p g_p^{-1} = g_p e g_p^{-1} = e$).

So by the lemma, $|S_0| \equiv |S| \equiv 0 \mod p$ since p divides n.

But notice $S_0 = \{(g, g, \dots, g) : g^p = e\}$, and it contains at least $(e, e, \dots, e)$ but since $p \mid |S_0|$ it means there is a nonidentity $g \in G$ which has $g^p = e$, i.e. an element of order p. ◻

The Sylow theorems are a strong generalization of Cauchy's thm. which say that not only does a finite group G of order n have an element of order p is $p \mid n$, it has a subgroup of order p^m where p^m is the biggest power of p dividing n.

<u>Def'n</u> A group G is a <u>p-group</u> (for p a prime) if every $g \in G$ has order a power of p. For G finite, by Cauchy's thm this is equivalent to G having order p^n for some $n \geq 0$.

A subgroup $H \leq G$ of a group G is called a <u>Sylow</u> <u>p-subgroup</u> if H is a p-group and it is <u>maximal</u> among p-groups that are subgroups of G (i.e. not a proper subgroup of any p-subgroup of G).

<u>Thm</u> (The Sylow Theorems). Let G be a finite group of order $p^n m$ where p is a prime and $p \nmid m$ and $n \geq 1$. Then:

1) (1st Sylow Thm) All Sylow p-subgroups of G have order p^n.

2) (2nd Sylow Thm) All Sylow p-subgroups of G are conjugate, i.e., if $P \leq G$ is a fixed Sylow p-subgroup, then all Sylow p-subgroups are gPg^{-1} for $g \in G$.

3) (3rd Sylow thm) Let n_p be the number of Sylow p-subgroups of G. Then $n_p \equiv 1 \mod p$ and also n_p divides m.

<u>Remark</u>: It can be shown that a finite p-group G of order p^n has subgroups of order p^k for all $0 \leq k \leq n$. (We may discuss this later when we talk about "solvable" groups.) In particular it contains a subgroup of order p, which must be cyclic, hence it has an element of order p. In this way the 1st Sylow theorem is indeed a strengthening of Cauchy's thm (although we will use Cauchy's theorem to prove the Sylow thms...)

Remark: If you can show that $n_p = 1$, where $n_p = \#$ Sylow p-subgroups of G, then from the 2nd Sylow Thm it follows that the unique Sylow p-subgroup of G is normal. In this way one can use Sylow thms to prove various groups G have nontrivial normal subgroups, i.e., are not simple.

To prove the Sylow theorems, we need a few more definitions:

Def'n Let $H \leq G$ be a subgroup of a group G. The normalizer of H in G is $N_G(H) = \{g \in G : gHg^{-1} = H\}$. It is the largest subgroup of G in which H is normal.

Prop. $N_G(H)$ is a subgroup of G, with $H \trianglelefteq N_G(H)$. Pf: straightforward $\boxtimes$

Now let's think about normalizers of p-subgroups of a finite gp. G:

Lemma If H is a p-subgroup of a finite group G, then
$$[N_G(H) : H] \equiv [G : H] \bmod p.$$

Pf: Let S be the left cosets of H in G and let H act on S by translation (i.e. $h(xH) = hxH$). Then $|S| = [G:H]$ and $xH \in S_0 \Leftrightarrow hxH = xH$ for all $h \in H \Leftrightarrow x^{-1}hx \in H$ $\forall h \in H$ $\Leftrightarrow x \in N_G(H)$. Thus $|S_0|$ is the # of cosets xH with $x \in N_G(H)$, i.e. $|S_0| = [N_G(H) : H]$. That $[N_G(H):H] \equiv [G:H] \bmod p$ follows from previous lemma $\boxtimes$

Cor If H is a p-subgroup of G such that p divides $[G:H]$ then $N_G(H) \neq H$.

The idea to prove 1st Sylow theorem is to use Cauchy's thm and the above corollary to repeatedly enlarge a p-subgroup of G until it has the maximum possible order p^n. But we need one more result to do this.

Thm (4th Isomorphism Theorem) Let $N \trianglelefteq G$ be a normal subgroup of a group G. Then there is a bijective correspondence between the subgroups of G containing N and all the subgroups of G/N that sends $K \le G$ to K/N.
Furthermore, K/N is normal in $G/N \iff K$ is normal in G.

Pf of 1st Sylow thm: By Cauchy's thm, G contains a $g \in G$ of order p. Assume by induction that G has a subgroup H of order p^i for $1 \le i < n$, we will show it has one of order p^{i+1}. By previous lemma & corollary, $1 < |N_G(H)/H| = [N_G(H):H] \equiv [G:H] \equiv 0 \mod p$, so $p \mid |N_G(H)/H|$.
Thus again by Cauchy, $N_G(H)/H$ contains a subgroup of order p, which by 4th isomorphism theorem is of form H_1/H where H_1 is a subgroup of $N_G(H)$ containing H. H is normal in H_1 since it's normal in $N_G(H)$.
So $|H_1| = |H||H_1/H| = p^i \cdot p = p^{i+1}$ and we are done. ☒

Pf of 2nd Sylow thm: Let P be a fixed Sylow p-subgp of G and H any p-subgroup. We will show $\exists g \in G$ such that $gHg^{-1} \le P$. Let S be the left cosets of P in G and let H act on S by translation, as before.
Then $|S_0| \equiv |S| (= [G:P]) \mod p$ by the lemma, and $p \nmid [G:P]$
So $|S_0| \neq 0$, i.e., $\exists gP \in S_0$. Then $gP \in S_0 \iff hgP = gP \;\forall h \in H$ $\iff g^{-1}hgP = P \;\forall h \in H \iff g^{-1}Hg < P \iff gPg^{-1}$ contains H. ☒

Pf of 3rd Sylow thm: By 2nd Sylow theorem, n_p is the # of conjugates of a fixed Sylow p-subgroup P. But this is $[G:N_G(P)]$, a divisor of $|G|$, and $p \nmid [G:N_G(P)]$ so indeed $n_p \mid m$.
Now let S be all Sylow p-subgroups of G and let P act on S by conjugation. Note $Q \in S_0 \iff xQx^{-1} = Q \;\forall x \in P \iff P \le N_G(Q)$, but P and Q are Sylow p-subgroups of $N_G(Q)$ and so are conjugate by 2nd Sylow thm and Q is normal in $N_G(Q)$, so this is only possible if $Q = P$.
Thus by our lemma, $|S| \equiv |S_0| = 1 \mod p$, hence indeed $n_p \equiv 1 \mod p$. ☒

9/25

§ 2.7, 2.8

Solvable and nilpotent groups, and subnormal series

We now study certain classes of groups that are "close" to abelian. We also use composition series to explain why simple groups are important.

Def'n Let G be a group and $a, b \in G$. The commutator of a and b is $[a,b] = aba^{-1}b^{-1}$. Notice that if a and b commute then $[a,b] = e$. For two subsets $S, T \subseteq G$ we define $[S,T] = \{[s,t] : s \in S, t \in T\}$.

Def'n The commutator subgroup, or derived subgroup, G' of G is $G' = [G,G]$. Notice that $[G,G] = \{e\} \Leftrightarrow G$ is abelian, and so G' measures how "non-abelian" G is.

Prop. $G' \trianglelefteq G$ is a normal subgroup of G. Pf: Straightforward. ☐

Rmk: In fact, G' is the "smallest" normal subgroup of G such that G/G' is abelian.

Def'n The derived series of G is the sequence of subgroups

$$\cdots \trianglelefteq G^{(3)} \trianglelefteq G^{(2)} \trianglelefteq G^{(1)} \trianglelefteq G^{(0)} = G$$

where $G^{(0)} = G$ and $G^{(i+1)} = [G^{(i)}, G^{(i)}] \left(= G^{(i)\prime}\right)$ for $i \geq 0$.

We say G is solvable if its derived series terminates at the trivial group after a finite number of steps, i.e., there is n such that

$$\{e\} = G^{(n)} \trianglelefteq \cdots \trianglelefteq G^{(1)} \trianglelefteq G^{(0)} = G.$$

Def'n The lower central series of G is the sequence of subgroups

$$\cdots \trianglelefteq G_2 \trianglelefteq G_1 \trianglelefteq G_0 = G$$

where $G_{i+1} = [G_i, G]$ for $i \geq 0$ and $G_0 = G$.

The upper central series of G is the sequence of subgroups

$$\{e\} = Z_0 \trianglelefteq Z_1 \trianglelefteq Z_2 \trianglelefteq \cdots$$

where Z_{i+1} is the subgroup of G with $Z_{i+1}/Z_i = Z(G/Z_i)$ for $i \geq 0$ and $Z_0 = \{e\}$. (So note $Z_1 = Z(G)$ is the center of G).

Rmk: Again it is easy to show the normality of these subgroups.

Prop. If the lower central series of G terminates at the trivial group in n steps, i.e., $\{e\}=G_n \trianglelefteq \cdots \trianglelefteq G_1 \trianglelefteq G_0 = G$, then the upper central series terminates at G in n steps; i.e. $\{e\}=Z_0 \trianglelefteq Z_1 \trianglelefteq \cdots \trianglelefteq Z_n = G$ and vice-versa. Pf: Skipped, see text book. ☒

Def'n G is called nilpotent (of nilpotency class n) if its lower/upper central series terminates (in n steps).

Prop. If G is nilpotent then it is solvable.

Pf: Just notice that $G^{(i)} \leq G_i$ for all $i \geq 0$. ☒

E.g. Consider $G = D_4$, the dihedral group of symmetries of a square. Recall $G = \langle r, s : r^4 = s^2 = (sr)^2 = 1 \rangle = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$.
We can compute $[sr^i, r^j] = sr^i r^j sr^i r^{-j} = r^{-i-j} r^{i-j} = r^{-2j}$
and $[sr^i, sr^j] = sr^i sr^j sr^i sr^j = r^{-i} r^j r^{-i} r^j = r^{2(j-i)}$
and all other commutators are trivial. Hence it follows that $G_0 = G$, $G_1 = [G_0, G_0] = \{e, r^2\}$, $G_2 = [G, G_1] = \{e\}$ so that G is nilpotent of nilpotency class 2.

Rmk: Of course the nilpotent groups of nilpotency class 1 are the abelian groups.

E.g. Consider $G = S_3 = \{e, (12), (13), (23), (123), (132)\}$, symmetric group on 3 letters.
We can compute $[(12), (13)] = (12)(13)(12)(13) = (123)$ and similarly for other 2-cycle pairs and $[(123), (12)] = (123)(12)(132)(12) = (132)$ and similarly for other 3-/2-cycle pairs, and other commutators are trivial.
Thus, $G_0 = G$, $G_1 = [G_0, G_0] = \{e, (123), (132)\}$, $G_2 = [G, G_1] = G_1, \ldots$ and so G is not nilpotent. But $G^{(0)} = G$, $G^{(1)} = [G^{(0)}, G^{(0)}] = \{e, (123), (132)\}$, $G^{(2)} = [G^{(1)}, G^{(1)}] = \{e\}$, so G is solvable.

Notice D_4 has order 2^3 while S_3 has order $2 \cdot 3$. In fact...

Thm A finite p-group G is always nilpotent.

Pf: Recall that we used the class formula to show that a nontrivial finite p-group G always has $Z(G) \neq \{e\}$. Thus in the upper central series of a finite p-group, the subgroups always get strictly larger until they reach all of G. ☒

Actually a finite nilpotent group is just a direct product of p-groups.

Thm A finite nilpotent group G is the direct product of its Sylow subgroups.

Pf: Skipped, see text book.

Rmk: The name "nilpotent" comes from the operator $[g, \cdot]$ being nilpotent (high enough power is trivial) for each $g \in G$.

Rmk: The name "solvable" comes from Galois theory and the solvability of polynomials by radicals. Next semester...

In a sense, all solvable groups are built out of cyclic groups. To see how, let's introduce notion of composition series:

Def'n Let G be a group. A subnormal series is a sequence of subgroups of G: $\{e\} = A_0 \trianglelefteq A_1 \trianglelefteq \cdots \trianglelefteq A_n = G$ where each A_i is a proper normal subgroup inside of A_{i+1} (but not nec. inside G).

E.g. When they terminate in finitely many steps, the derived series, lower central series, and upper central series are subnormal series.

Def'n A composition series of G is a subnormal series $\{e\} = A_0 \trianglelefteq A_1 \trianglelefteq \cdots \trianglelefteq A_n = G$ for which each A_{i+1}/A_i quotient group is simple. Equivalently, A_i is a maximal proper normal subgroup of A_{i+1} for all i.

The reason composition series are significant is:

Thm (Jordan-Hölder) In any two composition series of a group G, the (multi)set of quotient groups A_{i+1}/A_i are the same.

Pf: Again skipped, see textbook. $\boxtimes$

So any (finite) group G has associated to it a canonical (multi) collection of (finite) simple groups that it is "made out of." And...

Thm A (finite) group G is solvable if and only if all quotient groups A_{i+1}/A_i in its composition series are abelian (hence of form $\mathbb{Z}/p\mathbb{Z}$ for p prime).

The idea behind the proof of this theorem are two lemmas:

Lemma If $N \trianglelefteq G$ is a normal subgroup of G and N and G/N are solvable, then so is G.

Lemma If all the quotient groups in a subnormal series are abelian, then we can extend this to a composition series whose quotient groups are all abelian.

See the book for detailed proofs.

As a corollary, we see that all finite groups of order less than 60 are solvable, since 60 is the order of A_5, the smallest nonabelian simple finite group.

The Jordan-Hölder theorem explains why simple (finite) groups are significant, and next time we will discuss the classification of finite simple groups, which was a major achievement in group theory in the 20th Century!