Definition. Let G be a group and X a set. A (left) group action of G on X is a map

$$G \times X \longrightarrow X \qquad \text{(written } g \cdot x \text{ or } gx)$$

satisfying the following.

(1) $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$ for all $g_1, g_2 \in G$, $x \in X$

(2) $1 \cdot x = x$ for all $x \in X$.

Examples. (1) Let $G = \mathrm{Sym}(n)$ and $X = \{1, \dots, n\}$.
Then, for $\sigma \in G$, the map

$$\begin{aligned} G \times X &\longrightarrow X \\ (\sigma, x) &\longrightarrow \sigma(x) \end{aligned}$$

defines an action.

(2) Let G be the image of D_n in $GL_2(\mathbb{R})$, as discussed before, and let

$$X = \{1, \zeta, \zeta^2, \zeta^3, \dots, \zeta^{n-1}\}$$
$$= \left\{(1,0), \left(\cos\frac{2\pi}{n}, \sin\frac{2\pi}{n}\right), \left(\cos\frac{4\pi}{n}, \sin\frac{4\pi}{n}\right), \dots, \left(\cos\frac{2\pi(n-1)}{n}, \sin\frac{2\pi(n-1)}{n}\right)\right\}$$

Then G acts on X. (Verify!)

(3) Vector spaces: Given V over a field F, the multiplicative group $F^\times$ acts on V.

(You can multiply elements of V by elements of F.)

Really you get a module for the ring F.

9.2.

(4) Let $\mathbb{H} = \{ z \in \mathbb{C} : \operatorname{Im}(z) > 0 \}$ (the "upper half plane").

Exercise. The group $SL_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_{2\times 2}(\mathbb{Z}) : \det = 1 \right\}$ acts by linear fractional transformations

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \circ z = \frac{az + b}{cz + d}.$$

What is to be checked?

(1) This does map $\mathbb{H} \longrightarrow \mathbb{H}$.

(2) The "associative law".

(5) G acts on itself by left multiplication:

$$g \cdot h = gh.$$

(6) G acts on itself by conjugation.

$$g \cdot h = g h g^{-1}.$$ (The notation is confusing!)

(7) Let X = functions $\{1, \dots, n\} \longrightarrow \mathbb{C}$, $G = \operatorname{Sym}(n)$.

Exercise. ~~The map~~ Writing

$$(g \cdot f)(x) = f(gx)$$

does not, in general, define a group action of G on X.

But, writing

$$(g \circ f)(x) = f(g^{-1} x)$$ does.

9.3.

(8) ~~An example similar to ...~~

Let V be a f.d. vector space.

Then $GL(V)$ acts on V by

$$\phi \cdot v = \phi(v).$$

(9.) Again, let V be a fd vector space,

let $V^* = \mathrm{Hom}(V, F)$ be its dual space.

Then $GL(V)$ acts on V. The map

$$(g \circ f)(v) = f(gv)$$

does not define a left group action.

But $(g \cdot f)(v) = f(g^{-1} v)$

and $(g \cdot f)(v) = f(g^T v)$ do.

~~Proposition~~

Note that an action of a group G on X gives an injective homomorphism

$$G \longrightarrow \mathrm{Sym}(X)$$

$$g \longrightarrow \pi_g = \{ x \to gx \}.$$

Must prove:

(1) This defines a permutation (i.e. bijection) on X for each g, i.e. Really do get a map $G \to \mathrm{Sym}(X)$

(2) it's a group homomorphism.

9.4

(1) Show that π_g has a two-sided inverse, namely $\pi_{g^{-1}}$. For all x,

$$(\pi_{g^{-1}} \circ \pi_g)(x) = \pi_{g^{-1}}(\pi_g(x))$$ (def. of function composition)

$$= g^{-1} \cdot (g \cdot x)$$ (by def. of π_g)

$$= (g^{-1} g) \cdot x$$ (group action axiom)

$$= 1 \cdot x$$

$$= x$$ (" " ").

Same for $\pi_g \circ \pi_{g^{-1}}$.

(2) Must prove: $\pi_{gh} = \pi_g \circ \pi_h$ as elements of $\mathrm{Sym}(X)$.

For all $g, h \in G$, $x \in X$,

$$\pi_{gh}(x) = (gh)(x)$$
$$\pi_g \circ \pi_h(x) = g(h(x))$$
] Same by group action axioms.

<u>Cayley's Theorem</u>. Every group is isomorphic to a subgroup of a symmetric group.

<u>Proof</u>. Saw earlier, G acts on itself by left multiplication, so the map

$$g \longrightarrow \pi_g = \{h \to gh\}$$

is a homomorphism $G \longrightarrow \mathrm{Sym}(G)$.

It is <u>injective</u> because if $h = gh$ for all $h \in G$, then $g = 1$. (Indeed if $h = gh$ for <u>any</u> $h \in G$, then $g = 1$.)

9.5. $\overset{10/1}{\text{Centralizers}}$:

Definition. Let G be a group, with $A \subseteq G$ a subset. Then the centralizer of A is

$$C_G(A) = \{ g \in G : gag^{-1} = a \text{ for all } a \in A \}$$
$$= \{ g \in G : ga = ag \text{ for all } a \in A \}$$
$$= \{ \text{elts. of } G \text{ which commute with every element of } A \}.$$

If $A = \{a\}$ is a singleton, write $C_G(a)$.

Proposition. This is a subgroup of G (for arbitrary subsets A)

Prove it as an exercise.

The center of G, $\underset{\text{auf Deutsch}}{Z(G)} = C_G(G)$

$$= \{ g \in G : hg = gh \text{ for all } h \in G \}.$$

Note that $Z(G) = G \iff G$ is abelian.

Exercise. Find non-abelian examples of G for which $Z(G) = \{e\}$ and for which $Z(G) > \{e\}$.

The normalizer of A is

$$N_G(A) = \{ g \in G : \underbrace{gAg^{-1}}_{\text{This is } \{gag^{-1} : a \in A\}} = A \}.$$

Conjugation preserves A as a set, not necessarily pointwise. So $C_G(A) \leq N_G(A)$.

Exercise. Come up with an example where these are different.

10.2.

The stabilizer of a group action.

Def. Suppose a group G acts on X and $x \in X$.
The stabilizer of x in G is

$$G_x = \mathrm{Stab}_G(x) = \{ g \in G : g \cdot x = x \}.$$

The kernel of the action is

$$\bigcap_{x \in X} G_x = \{ g \in G : g \cdot x = x \text{ for all } x \in X \}.$$

Exercise. (1) These are subgroups.

(2) Recall the action of $G = SL_2(\mathbb{Z})$ on $\mathbb{H}$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \circ z = \frac{az+b}{cz+d}.$$

(a) What is the kernel of the action?

(b) Can you find a point in $\mathbb{H}$ with larger stabilizer?

(c) Can you find infinitely many?

Note that (b) $\to$ (c). Why?

Given your favorite z, then another element in the same orbit looks like γz for some $\gamma \in G$.

Now, if $gz = z$
then $g\gamma z$ may not be γz
But $(\gamma g \gamma^{-1}) \gamma z = gz$.

10.3. In other words.

Suppose G acts on a set X, and x_1 and x_2 are in the same orbit. This means $gx_1 = x_2$ for some $g \in G$.

(~~since~~ Check: this is an equivalence rel'n)

Then, $\mathrm{Stab}_G(x_1)$ and $\mathrm{Stab}_G(x_2)$ are conjugate;

$$\mathrm{Stab}_G(x_2) = g\,\mathrm{Stab}_G(x_1)\,g^{-1}.$$

(This is an equivalence relation too)

Example. (My favorite!)

Let $V = \{ au^3 + bu^2v + cuv^2 + dv^3 : a, b, c, d \in \mathbb{C} \}$

be the vector space of binary cubic forms.

(1) Prove that $G = GL_2(\mathbb{C})$ acts on V via

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \circ f(u, v) = f(\alpha u + \gamma v, \beta u + \delta v).$$

(2) The kernel of the action is cyclic of order 3.

(3) (Challenge!) If $f \in V$, then

$$\mathrm{Stab}_G(f) \begin{cases} \text{has size } 18 \text{ if } f \text{ doesn't have a repeated root} \\ \text{is infinite if it does.} \end{cases}$$

10.4. Definition. A group H is cyclic if it can be generated by a single element, i.e. if

$$H = \{x^n : n \in \mathbb{Z}\} \text{ for some } x \in H.$$

We call x a generator.

Note that x^{-1} is also a generator.

Example. Let

$C_n = \langle x \mid x^n = 1 \rangle$, the cyclic group of order n.

Compute the orders of all elements of C_5 and C_6.

[Do at board]

If the group is abelian, we often write

$$H = \{nx : n \in \mathbb{Z}\}.$$

Example. $\mathbb{Z}$ is also cyclic ("infinite cyclic") because 1 and only -1 are generators.

Example. S_n (for $n \geq 3$), D_n (for $n \geq 2$). Not cyclic.

Anything not abelian.

However, ~~in~~ any group G, ~~the~~ ~~for~~ for each $g \in G$, the set

$\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$ (subject to relations in G)

is a cyclic subgroup.

10.5 $\equiv$ 11.1.

Some elementary propositions.

Prop. If $H = \langle x \rangle$, then $|H| = o(x)$, and:

(1) if $|H| = n < \infty$, then $x^n = 1$ and $H = \{1, x, x^2, \dots, x^{n-1}\}$.

(2) If $|H| = \infty$, then $x^n \neq 1$ for $n \neq 0$ and $x^a \neq x^b$ for all $a \neq b \in \mathbb{Z}$.

Proof. (1) The elements are distinct, because n is minimal such that $x^n = 1$ and $x^r = x^s \Rightarrow x^{r-s} = 1$.

Conversely, we've enumerated all of them:
An element in H looks like x^m for some $m \in \mathbb{Z}$.
Writing $m = qn + r$, with $0 \leq r < n$, $x^m = x^{qn+r} = (x^n)^q x^r = x^r$.

(2) is similar.

Prop. Let G be any group and $x \in G$, $m, n \in \mathbb{Z}$.
If $x^n = 1$ and $x^m = 1$ then $x^d = 1$ with $d := (m, n)$.
(2) If $x^m = 1$ for some $m \in \mathbb{Z}$, then $o(x) = |x|$ divides m.

Proof. (1) Use the Euclidean algorithm to write

$$d = mr + ns \quad \text{for some } r, s \in \mathbb{Z}.$$

Then $x^d = x^{mr+ns} = (x^m)^r (x^n)^s = 1$.

(2) $x^m = 1$ and $x^{o(x)} = 1$. Since $o(x)$ is minimal, $(o(x), m) = 1$ and $o(x) \mid m$.

11.2.

Some more boring propositions.

(1) Any two cyclic groups of the same order are isomorphic.

(2) A subgroup of a cyclic group is cyclic.

(3) You can compute the order of any elt. of a cyclic group.

We're more or less skipping the rest of Ch. 2.
But put the pretty pictures on the overhead.

Quotients.

Definition. If $X \xrightarrow{\varphi} Y$ is a map of $\{$sets, groups, $\cdots$, schemes$\}$, pretty much anything other than

then the fibers of φ are the sets
$$\{\varphi^{-1}(a)\} \text{ as } a \text{ ranges over } Y.$$

Example. Consider a surjective linear transformation $\mathbb{R}^3 \xrightarrow{\phi} \mathbb{R}^2$.

Its kernel will be a line.

What do the fibers look like?

Claim. $\phi^{-1}(w) = v + \operatorname{Ker}(\phi)$, where v is an arbitrary elt. of $\phi^{-1}(w)$, for each $w \in \mathbb{R}^2$.

Proof. If $v \in \phi^{-1}(w)$, then
$$v' \in \phi^{-1}(w) \Longleftrightarrow \phi(v') = w = \phi(v) \Longleftrightarrow \phi(v'-v) = 0$$
$$\Longleftrightarrow v' - v \in \operatorname{Ker}(\phi).$$

11.3 = 12.1

In groups, as with vector spaces, the kernel of a homomorphism $G \xrightarrow{\phi} H$ is

$$\ker(\phi) = \{ g \in G : \phi(g) = 1 \}.$$

Then $\ker(\phi)$ and $\mathrm{Im}(\phi)$ are subgroups of G and H respectively. (See DF p.75 for some basic properties.)

Proposition. Given $G \xrightarrow{\phi} H$ and let $K = \ker(\phi)$. Then, for any $h \in \mathrm{Im}(\phi)$, and any preimage $g \in \phi^{-1}(h)$,

$$\varphi^{-1}(h) = gK \quad \text{and}$$
$$\varphi^{-1}(h) = Kg.$$

Proof in both cases is the same!

Definition. A subgroup $N \leq G$ is normal if $gN = Ng$ for all $g \in G$. So, kernels of homomorphisms are normal.

Definition. If $N \leq G$ ~~is~~ is a subgroup, its left cosets are $\{ gN : n \in N \}$

right cosets are $\{ Ng : n \in N \}$.

(If N is normal these coincide.) Note. All of them have size $|N|$.

Example. If $G = \mathbb{Z}$, $N = n\mathbb{Z}$, then the cosets are of the form $a + n\mathbb{Z}$ for $a \in \mathbb{Z}$. There are n of them.

Example. Let $G = D_n$. Then C_n is a normal subgroup. It has one coset.

11.4. = 12.2

Example. The cosets of $SL_n(\mathbb{C})$ in $GL_n(\mathbb{C})$ are the sets of the form

$$\{g \in GL_n(\mathbb{C}) : \det(g) = t\}$$

for each fixed $t \in GL_n(\mathbb{C})$.

~~Def~~ **Proposition.** Let N be a normal subgroup. Then the cosets of N in G form a group, with group operation

$$(Na) \cdot (Nb) = Nab.$$

This is called the quotient group of G by N and written G/N.

Proof. What's to prove? That it is well defined. If $Na = Nc$ and $Nb = Nd$, then $Nab = Ncd$.

~~The nicest way is to show that~~

If $Na = Nc$ then $a = n_1 c$ for some $n_1 \in N$, similary $b = n_2 d$.

We have
$$\begin{aligned} Nab &= N n_1 c n_2 d \\ &= N c n_2 d && (Nn = N \text{ for any } n \in N) \text{ (doesn't use normality)} \\ &= c N n_2 d && \text{(normality)} \\ &= c N d && \cancel{\text{normal}}\ (Nn = N) \\ &= N c d && \text{and we're done.} \end{aligned}$$

Alternative proof. Do it setwise,

$$Nab = \{rs : r \in Na, s \in Nb\}.$$

More or less the same.

11.5 = 12.3.

Example. $\mathbb{Z}/n\mathbb{Z} = \{\{a + n\mathbb{Z} : n \in \mathbb{Z}\} : a \in \mathbb{Z}\}$

$= \{n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \dots (n-1) + n\mathbb{Z}\}$.

$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a+b) + n\mathbb{Z}$.

Example. Always have $G/G = 1$ and $G/1 \cong G$.

~~Example. There exists a surjective homomorphism $Sym(n) \to \{\pm 1\}$ for every $n \geq 2$~~ True! But, on second thought, not relevant now.

Lagrange's Theorem. If H is a subgroup of the finite group G, then $|H| \mid |G|$.

Proof. This is because every left or right coset of H has the same size:

There is a bijection

$$\begin{aligned} H &\longrightarrow Hg \\ h &\longrightarrow hg. \end{aligned}$$

(note: not a homomorphism)

In addition, if two right cosets (or two left cosets) intersect, then they coincide:

Suppose $Hg \cap Hg' \neq \phi$.

Then we have $hg = h'g'$ for some $h, h' \in H$

So $g' = (h')^{-1}hg$

and $Hg' = H(h')^{-1}hg = Hg$,

because $Hh = H$ for any $h \in H$.

~~11.6~~ 12.4

So the right cosets partition G,

$$G = Hg_1 \sqcup Hg_2 \sqcup \cdots \sqcup Hg_k$$

This means disjoint union, no overlap.

So $|G| = |H| \cdot \#$ of right cosets.

Definition. If $H \leq G$ is a subgroup, the index $[G:H]$ (or $|G:H|$) is the number of right cosets of H in G.

If G is finite, then $[G:H] = \dfrac{|G|}{|H|}$.

Makes sense even if not.

Cor. If $x \in G$, $o(x) \mid |G|$, so $x^{|G|} = 1$ for all $x \in G$.

Proof. $\langle x \rangle$ is a subgroup.

Cor. Any group of order p is cyclic.

Proof. Take $1 \neq x \in G$. Then $\langle x \rangle$ is a subgroup of G, and has order p.

Theorem. (Sylow) If G is a finite group of order $p^a \cdot m$ with $(p,m)=1$, then G has a subgroup of order p^a.

(Also p: Cauchy.)

Will prove later!

12.5 ≈ 13.1.

Additional propositions.

(1) If H and K are finite subgroups of a group, then with

$$HK = \{hk : h \in H,\ k \in K\}$$

we have
$$|HK| = \frac{|H|\,|K|}{|H \cap K|}.$$
(HK may or not be a subgroup)

(2) If H and K are subgroups of a group, then

$$HK \text{ is a subgroup} \iff HK = KH.$$

Isomorphism Theorems.

#1. If $\varphi : G \to H$ is a homomorphism, then $\ker(\varphi) \trianglelefteq G$ and $G/\ker(\varphi) \cong \varphi(G)$.

Already saw the normality.

There's a picture!

This is the natural projection map $g \to g\,\mathrm{Ker}(\varphi) = \mathrm{Ker}(\varphi)g$.

$$\begin{tikzcd}
G \arrow[r, "\pi"] \arrow[dr, "\varphi"'] & G/\mathrm{Ker}(\varphi) \arrow[d, dashed, "\theta"] \\
 & H
\end{tikzcd}$$

We choose θ to make this commute:

$$\theta(\mathrm{Ker}(\varphi)\cdot g) = \varphi(g).$$

Prove: (0) It's well defined.
(1) It's a homomorphism.
(2) It's injective. (3) Its image is $\mathrm{Im}(\varphi)$.

13.2.

(0) If $\mathrm{Ker}(\varphi)\cdot g = \mathrm{Ker}(\varphi)\cdot g'$

then $g' = n\cdot g$ for some $n \in \mathrm{Ker}(\varphi)$ and

~~Ker(g) = *~~

$\varphi(g') = \varphi(n)\varphi(g) = \varphi(g)$.

(1) $\theta(\mathrm{Ker}(\varphi)\cdot gg') = \varphi(gg')$

and $\theta(\mathrm{Ker}(\varphi)\cdot g)\,\theta(\mathrm{Ker}(\varphi)\cdot g') = \varphi(g)\varphi(g')$.

(2) $\theta(\mathrm{Ker}(\varphi)\cdot g) = 1 \iff \varphi(g) = 1$

$\iff g \in \mathrm{Ker}(\varphi)$

$\iff \mathrm{Ker}(\varphi)\cdot g = \mathrm{Ker}(\varphi)$.

(3) Tautology. $\varphi(g)$ is in the image for all $g \in G$, by construction.

#2. Preliminaries.

Let N be a normal subgroup of G, and H any subgp.

Claim. NH is a subgroup of G.

Could give a messy proof, but this is better:

$$G \xrightarrow{\varphi} G/N$$

$$H \longrightarrow \varphi(H)$$

Images of subgroups under homomorphisms are subgroups.

So are inverse images.

$$NH = \varphi^{-1}(\varphi(H)).$$

And N is normal in NH, since it is normal in G.

13.3.

Isomorphism Theorem #2. (Diamond)

Let $N \trianglelefteq G$ and $H \leq G$. Then $H \cap N \trianglelefteq H$ and
$H/(H \cap N) \cong NH/N$.

$$\begin{tikzcd}
& G \arrow[d, dash] & \\
& NH \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, phantom, "\text{iso}"] & \\
N \arrow[dr, dash] & & H \arrow[dl, dash] \\
& H \cap N &
\end{tikzcd}$$

Proof. Consider the quotient homomorphism
$$G \xrightarrow{\varphi} G/N.$$
Restricted to H, we get a surjective homomorphism
$$H \longrightarrow HN/N$$
whose kernel is $H \cap N$. Done by first thm.

Isomorphism Theorem #3. ("invert and cancel")

Let G be a group and H, K normal subgroups with $H \leq K$. Then $K/H \trianglelefteq G/H$ and
$$\frac{G/H}{K/H} \cong G/K.$$

Proof. Define a homomorphism
$$G/H \longrightarrow G/K$$
$$Hg \longrightarrow Kg$$
which is WD because $H \leq K$. Its kernel is K/H.

13.4 Isomorphism Theorem #4. (Correspondence)

Let $\varphi : G \to H$ be a surjective homomorphism with $N = \mathrm{Ker}(\varphi)$. Define the sets of subgroups:

$$S = \{ U : N \le U \le G \}$$

$$T = \{ V : V \le H \}$$

Then $\varphi(\cdot)$ and $\varphi^{-1}(\cdot)$ are inverse bijections between S and T. They respect:

Containment (if $U_1 \leftrightarrow V_1$ and $U_2 \leftrightarrow V_2$, then $U_1 \le U_2 \longleftrightarrow V_1 \le V_2$.)

Indices (if above, $[U_2 : U_1] = [V_2 : V_1]$)

Normality (if above, $U_1 \triangleleft U_2 \longleftrightarrow V_1 \triangleleft V_2$)

Factor groups (if above, $U_2/U_1 \cong V_2/V_1$).

Partial proof. (the rest is an exercise.)

(1) Why $\underbrace{\varphi(\varphi^{-1}(V)) = V}_{}$ and $\underbrace{\varphi^{-1}(\varphi(U)) = U}_{}$?

This is a tautology, assuming $V \le \mathrm{Im}(\varphi)$.

This is not quite a tautology. Certainly not true as sets.

Why, if $\varphi(g) \in \varphi(U)$, $g \in U$?

Here, says $Ng = Nh$ for some $h \in U$, so $g = nh \in NU = U$.

The rest are all fairly easy.

14.1. More on permutation groups.

The structure of S_n.

wrong

Inside Sym(3), (1 2 3) may be written

$\sigma = (1\ 2\ 3) = (1\ 3)(1\ 2) = (1\ 2)(1\ 3)(1\ 2)(1\ 3) = (1\ 2)(2\ 3)$

A 2-cycle is called a transposition.

Prop. For each n, Sym(n) is generated by transpositions.

Proof. Declare it to be obvious, or:

each $\sigma \in$ Sym(n) is a product of cycles, and

$$(a_1\ a_2 \cdots a_m) = (a_1\ a_m)(a_1\ a_{m-1}) \cdots (a_1\ a_2).$$

Theorem. There exists a surjective homomorphism

$$\varepsilon : \mathrm{Sym}(n) \longrightarrow \pm 1,$$

whose kernel, the alternating group Alt(n), (or A_n) consists of products of even numbers of transpositions.

In particular, every transposition maps to -1, and no element can be written as both an even product and an odd product.

Proof 1. (cheating) Map Sym(n) $\longrightarrow GL_n(\mathbb{Z})$

Let a basis for $\mathbb{C}^n$ be $\{v_1, \dots, v_n\}$

and map $\sigma : i \to \sigma(i)$ to $\{v_i \to v_{\sigma(i)}\}$.

Take the determinant.

This is cheating, because it relies on the existence of the determinant function.

14.3 ?[illegible] 15:1 Orbits and counting:

Prop: Suppose a group G acts a set A.
For each $a \in A$, the size of the orbit of a is equal to $[G : \mathrm{Stab}_G(a)]$.

Proof. We prove that ~~[illegible]~~ the orbits are in bijection with the left cosets, via

$$g\,\mathrm{Stab}_G(a) \xrightarrow{\theta} ga.$$

Clearly the map θ (which is just a map of sets) is surjective onto the orbit of a.

Why is it injective?
If $ga = g'a$, then $(g')^{-1} g \in \mathrm{Stab}(a)$
So $g \in g'\,\mathrm{Stab}(a)$ and vice versa.
So $g\,\mathrm{Stab}_G(a) = g'\,\mathrm{Stab}_G(a)$. //

Consider G acting on itself by conjugation.

$$g \cdot a = gag^{-1} \quad \text{for all } g, a \in G.$$

The orbits are called the conjugacy classes of G.

Proposition. Let $g \in G$. The size of the conjugacy class of g is equal to $[G : \underbrace{C_G(g)}_{\text{the centralizer of } g \text{ in } G}]$.

Proof. This is the above!
The stabilizer of the action is, by def,

$$\{h \in G : hgh^{-1} = g\} = \{h \in G : h \text{ commutes with } g\}$$
$$= C_G(g).$$

14.4 = 15.2

Example. $G = \mathrm{Sym}(3)$

Conjugacy class	Representative	Centralizer
e	e	G
$\{(1\,2),(1\,3),(2\,3)\}$	$(1\,2)$	$\{(1\,2), e\}$
$\{(1\,2\,3),(1\,3\,2)\}$	$(1\,2\,3)$	$\{(1\,2\,3), (1\,3\,2), e\}$.

Theorem. (The Class Equation)
Let G be a finite group, and let $g_1, \ldots, g_r$ be representatives of the $\underbrace{\text{nontrivial}}_{\text{i.e. excluding the singletons, which form the center of } G.}$ conjugacy classes of G.

Then $$|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(g_i)].$$

Proof. Because ~~con~~ dividing into conjugacy classes is a partition of G,

$$|G| = |Z(G)| + \sum_{i=1}^{r} \#\{\text{conjugacy class of } g_i\}$$
$$= |Z(G)| + \sum_{i=1}^{r} [G : C_G(g_i)] \quad \text{by above.}$$

~~14.5.~~ 15.3.

We can use this to prove things!

Corollary. Suppose G is a group of prime power order, $|G| = p^a$. Then $Z(G) \neq 1$.

Proof. We have

$$p^a = |Z(G)| + \sum_{i=1}^{r} [G : C_G(g_i)].$$

Now, for each g_i, $C_G(g_i)$ is a power of p
(by Lagrange's thm, since it is a subgp of G)
and $C_G(g_i) \neq G$ for each g_i
(otherwise, by definition, $g_i \in Z(G)$)
so $[G : C_G(g_i)]$ is divisible by p.

$$\text{So } |Z(G)| = \underbrace{p^a}_{\substack{\text{divisible}\\ \text{by } p}} - \underbrace{\sum_{i=1}^{r} [G : C_G(g_i)]}_{\substack{\text{divisible}\\ \text{by } p}}$$

and $p \mid |Z(G)|$. In particular, $|Z(G)| \neq 1$.

Conjugation in Sym(n).

Proposition. Conjugate permutations in Sym(n) have the same cycle structure.

If $\sigma = (a_1\, a_2 \cdots a_{k_1})(b_1\, b_2 \cdots b_{k_2}) \cdots$

then $\tau\sigma\tau^{-1} = (\tau(a_1)\, \tau(a_2) \cdots \tau(a_{k_1}))(\tau(b_1) \cdots \tau(b_{k_2}) \cdots)$

Think about it. e.g. $\tau\sigma\tau^{-1}$ sends

$\tau(a_1) \to a_1 \to a_2 \to \tau(a_2)$

15.4.

The converse is true.

Prop. If two elts. of Sym(n) have the same cycle structure, they are conjugate.

The proof is to write out the elts of Sym(n) side by side and define τ as in the above.

Example. Structure of Sym(5).

Conj. class	Size	Size of centralizer of any element
e	1	120
2-cycles	10	12
3-cycles	20	6
4-cycles	30	4
5-cycles	24	5
2 + 2	15	8
2 + 3	20	6

Can you actually compute the centralizers? Try!

← If we didn't screw up, this should be 120.

15.5. Consequence.

Proposition. A_5 is a simple group.

Here a group G is simple if it has no nontrivial normal subgroups. ("Nontrivial": other than $\{1\}$ or G.)

Lemma. Let G be any group. If $H \triangleleft G$, then H is a union of conjugacy classes of G.

i.e. if C is a c.c. of G, then $C \cap H$ is C or ϕ.

Proof. If $g \in H$, then since H is normal we have $xgx^{-1} \in H$ for all $x \in G$.

Structure of A_5. Contains e, 3-cycles, 5-cycles, 2 + 2.

~~If $H \triangleleft A_5$, then $|H|$ is some sum of 1, 20, 24, 15 including the 1.~~

~~So: 1, 21, 25, 16, 45, 36, 40, 60.~~

~~Only 1 and 60 divide 60.~~

Oops, no, this is WRONG because $H \triangleleft A_5$ is not necessarily a union of conjugacy classes in S_5, only in A_5.

$(\longrightarrow)$

15.6

Conjugacy classes in A_5.

e : 1.

3-cycles (20) : All conjugate in A_5.

Why? $C_{A_5}((1\ 2\ 3)) = \langle(1\ 2\ 3)\rangle$.

(Think about it. Substitute 1 2 3 with different numbers. Can only get 2 3 1 or 3 1 2.)

So size 3, and $20 \times 3 = 6$.

2 + 2 (15) : $C_{A_5}((1\ 2)(3\ 4))$.

The centralizer in <u>S_5</u> :

Generated by $(1\ 2), (3\ 4), (1\ 3)(2\ 4)$. A group of 8 elements with both even and odd perms. So 4 must lie in A_5.

5-cycles : (24) $C_{A_5}((1\ 2\ 3\ 4\ 5))$

$= C_{S_5}((1\ 2\ 3\ 4\ 5))$

$= \langle(1\ 2\ 3\ 4\ 5)\rangle$.

So this conjugacy class breaks into two.

Our decomp. into conjugacy classes is

$$60 = 1 + 15 + 20 + 12 + 12.$$

Now check : No subset of $\{1, 15, 20, 12, 12\}$ including 1 adds to any divisor of 60.

So there can be no normal subgroup!

16.1 (Class equ; prime powers).

Prop. If G is a group of order p^2 (p prime), then G is abelian.

Partial proof. By previous, $Z(G) \neq 1$. So

$\underbrace{G/Z(G)}_{\text{note! } Z(G) \text{ is automatically normal.}}$ has size 1 or p.

If it has size 1 then $Z(G) = G$ as desired.

In any case it is ~~abelian~~ cyclic.

To finish:

Exercise. If $G/Z(G)$ is cyclic then G is abelian.

Automorphisms. Def. Let G be a group. Any isomorphism $G \xrightarrow{\sim} G$ is called an automorphism of G.

Write $\mathrm{Aut}(G)$ for the group of automorphisms.

Prop. There is a homomorphism

$$G \longrightarrow \mathrm{Aut}(G)$$
$$g \longrightarrow \{x \to gxg^{-1}\}.$$

Readily checked. In general, neither injective nor surjective.

Prop. Let $H \triangleleft G$. Then there is a homomorphism

$$G \longrightarrow \mathrm{Aut}(H)$$
$$g \longrightarrow \{x \to gxg^{-1}\}.$$

Same proof.

Moreover the kernel is $C_G(H)$ (immediate).

So $G/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$.

16.2

__Proposition__. Let K be __any__ subgroup of G.

Then, for each $g \in G$, $K \cong gKg^{-1}$.

If K is always __normal__, then $K = gKg^{-1}$. So it's more interesting if K is not normal.

M

16.2.

Def. An automorphism of G is called inner if it coincides with conjugation by g, for some $g \in G$.

$\mathrm{Inn}(G)$ is the subgroup of $\mathrm{Aut}(G)$ of such.

By previous, $\mathrm{Inn}(G) \cong G/Z(G)$.

Examples.

G is abelian $\longleftrightarrow$ $\mathrm{Inn}(G) = 1$

$Z(D_4) = \langle r^2 \rangle$, so $\mathrm{Inn}(D_4) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$.
(Can you find them all?)

$Z(S_n) = 1$ for $n \geq 3$, so $\mathrm{Inn}(S_n) \cong S_n$.

An automorphism is outer if it is not inner.

Example/ Exercise. Prove that $\mathrm{Aut}(D_4) \neq \mathrm{Inn}(D_4)$:

$r \to r$, $s \to sr$ defines an automorphism of D_4 which is not conjugation by any elt. of D_4.

Indeed, $\mathrm{Aut}(D_4) \cong D_4$. Prove this and construct an automorphism explicitly.

Example. $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^{\times}$ — invertible elts. in: $\{a \in \mathbb{Z}/n\mathbb{Z} : (a,n)=1\}$. group law: multiplication
which has order $\varphi(n)$.

(Note that $\mathrm{Inn}(\mathbb{Z}/n\mathbb{Z})$ is trivial.)

The isomorphism is given by

$$\{1 \to a\} \longleftarrow a$$
$$\{x \to ax\}$$

16.3.

Why is this an automorphism?

(1) The map $x \to ax$ maps 1 to another generator iff $(a, n) = 1$. (Check.)

Conversely, if $(a,n) > 1$, no multiple of a is a generator.

(2) It is clearly injective

(3) It is surjective because 1 has to go somewhere, and a homomorphism is determined by its values on a generating set!

Example. Let G be a group of order pq, p and q prime with $p \leq q$ and $p \nmid q-1$.

Then G is abelian.

Proof. If $Z(G) \neq 1$, then by earlier argument $G/Z(G)$ is cyclic and G is abelian.

If every nonidentity elt of G has order p, the class equation will read

$$pq = |G| = |Z(G)| + \sum [G : C_G(g_i)]$$

$$= 1 + kq \qquad \text{impossible.}$$

So there is an elt. x of order q. Write $H = \langle x \rangle$.
Then H is normal in G, and $C_G(H) = H$ since $Z(G) = 1$.

$G/H = N_G(H)/C_G(H)$ is a group of order p, isomorphic to a subgroup of $\mathrm{Aut}(H)$. But $|\mathrm{Aut}\, H| = q-1$ so $p \mid q-1$.

12.1.

Cauchy's theorem.

Let G be a finite group. If $p \mid |G|$ then G has an elt. of order p.

Proof for abelian groups. Induction on $|G|$.

Choose $1 \neq x \in G$. If $p \mid o(x)$ then $x^{o(x)/p}$ works.

Otherwise, let $N = \langle x \rangle$ with $N \trianglelefteq G$.

By induction $p \mid |G/N|$ so G/N contains yN of order p. So $y^p \in N$ even though $y \notin N$. This implies that y has order divisible by p (fact about cyclic groups -- check it).

Proof for non-abelian groups. Induction again.

Write down the class equation

$$\# G = \# Z(G) + \sum [G : C_G(g_i)]$$

If any proper subgroup of G has order divisible by p, done by induction.

Otherwise, $p \nmid \# Z(G)$

$p \nmid \# C_G(g_i)$ so $p \mid [G : C_G(g_i)]$

and so p divides every term above except for $\# Z(G)$. (Impossible!)

17.2.

Lemma. (Fixed point congruence)

Let G be a <u>p-group</u> (i.e. $|G| = p^k$ for some k) acting on a finite set X. Then

$$\# X \equiv \# \{\text{fixed points}\} \pmod p.$$

Proof.

$$\# X = \sum_{\substack{x_i \text{ orbital} \\ \text{representative}}} \#(\text{orbit of } x_i)$$

$$= \sum_{x_i} [G : \mathrm{Stab}_G(x_i)]$$

$$= \#\{\text{fixed points}\} + \underbrace{\sum_{\substack{x_i \\ \text{not a} \\ \text{fixed point}}} [G : \mathrm{Stab}_G(x_i)]}_{\text{Each of these divides } p^k, \text{ and is not } 1.}$$

■

Cor. If a finite group G acts on a finite set X:

* If $p \nmid |X|$, then there is at least one fixed point of the action.

* If $p \mid |X|$, then the number of fixed points is divisible by p.

17.3 .

Example. Let G be a p-subgroup of $GL_n(\mathbb{Z}/p)$.

(Can compute: $\# GL_n(\mathbb{Z}/p) = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$
so at least one exists.)

Make it act on $(\mathbb{Z}/p)^n$ as usual.

Since $p \mid (\mathbb{Z}/p)^n$, there is ~~at~~ one least p fixed points:
There could be zero except that 0 is fixed by everything.

So: There is a nontrivial simultaneous eigenvector for G (with eigenvalue 1).

Sylow's Theorem. [Crib from K. Conrad's notes ~!]

18.1. Proofs of the Sylow theorems. (see K. Conrad's notes)

Recall. Suppose a p-group G (i.e., $|G|=p^k$) acts on a finite set X.

Then,
$$\#X \equiv \#\underbrace{\{\text{fixed points}\}}_{\mathrm{Fix}_G(H)} \pmod p.$$

Throughout, let G be a finite group with $|G|=p^k m$, $(p,m)=1$.

Sylow Existence. G has a subgroup of order p^i for $0\le i\le k$.

Proof. Induction on i. $i=0$ is trivial.

Suppose $|H|=p^i$; then H acts on the set of left cosets G/H: $H \curvearrowright G/H$

$$h\cdot gH = hgH.$$

We have $|G/H| \equiv |\mathrm{Fix}_H(G/H)| \bmod p$.

What are the fixed cosets?

$$\begin{aligned}
hgH = gH \ \forall h\in H &\iff hg\in gH \quad \text{for all } h\in H \\
&\iff g^{-1}hg \in H \quad \text{"} \\
&\iff g^{-1}Hg \subseteq H \\
&\iff g^{-1}Hg = H \ \text{b/c } |g^{-1}Hg|=|H| \\
&\iff g\in N(H).
\end{aligned}$$

So $\mathrm{Fix}_H(G/H) = \{gH : g\in N(H)\} = N(H)/H$, which is a group

with $[G:H] \equiv [N(H):H] \bmod p$.

18.2 when $|H| = p^i$ and $i < k$, then both sides are divisible by p.

Have to use Cauchy's theorem: $N(H)/H$ contains a subgroup of order p.

Use the correspondence theorem (iso theorems):

It is of the form H'/H where $|H'| = |H| \cdot p = p^{i+1}$

and we're done.

Sylow Conjugacy. Let P, Q be p-Sylow subgroups (i.e. $|P| = |Q| = p^i$) Then P and Q are conjugate.

Proof. Q acts on the left cosets G/P, again by left multiplication, with

$$[G:P] \equiv |\mathrm{Fix}_Q(G/P)| \mod p.$$

Since the LHS is not divisible by p, RHS $\neq 0$.

There is a fixed point in G/P, i.e. we have $qgP = gP$ for some $g \in G$ and all $q \in Q$ simultaneously.

So $qg \in gP$, so $q \in gPg^{-1}$ for all $q \in Q$

so $Q \subseteq gPg^{-1}$

so $Q = gPg^{-1}$ since same size

DONE.

18.3.

<u>Sylow counting</u>. Let n_p = # of p-Sylow subgroups.

Then $n_p \equiv 1 \pmod p$.

<u>Proof</u>. Let any p-Syl P act on $\mathrm{Syl}_p(G)$ by conjugation.

Then $n_p \equiv \#\{\text{fixed points}\} \bmod p$.

What is a fixed point? $Q \in \mathrm{Syl}_p(G)$ s.t. $gQg^{-1} = Q$ for all $g \in P$.

One such is P. Any others?

If Q is such, then $P \le N(Q)$, so P and Q are p-Sylow subgroups in <u>$N(Q)$</u> and hence conjugate in $N(Q)$. But $Q \trianglelefteq N(Q)$ and hence conjugate only to itself. So $P = Q$.

Counting #2: $n_p \mid m$.

<u>Proof</u>. Now make G act by conjugation on $\mathrm{Syl}_p(G)$.

This group action has <u>one orbit</u>, so $n_p \mid |G|$.

Since $n_p \equiv 1 \pmod p$, $n_p \mid |G|$.

<u>Counting #3</u>: $n_p = [G : N(P)]$ where P is any p-Sylow subgroup and $N(P)$ is its normalizer.

<u>Proof</u>. Same action as #2:

$$n_p = [G : \text{stabilizer of } G \text{ acting by conj. on } P]$$
$$= [G : N(P)].$$

18.4.

Cor. The p-Sylow subgroup of G is unique if and only if it is normal.

Application. If $|G| = 15$ then G is cyclic.

Proof. $n_3 \equiv 1 \pmod 3$ and divides 5

$n_5 \equiv 1 \pmod 5$ and divides 3

So the 3- and 5-Sylow subgroups of G are unique.

Let H_3 be the 3-Syl, H_5 be the 5-Syl.

Write $H_3 = \langle x \rangle$ and $H_5 = \langle y \rangle$.

Then xy is not in H_3 or H_5, so order is not 3 or 5.

Since $o(xy) \mid 15$, $o(xy) = 15$!

Exercise. For what other values of $|G|$ does this work?

Example. If $|G| = 12$, then either G has a normal 3-Sylow subgroup (more later...) or $G \cong A_4$.

Proof. Since $n_3 \equiv 1 \pmod 3$ and $n_3 \mid 4$, if $n_3 \neq 1$ then $n_3 = 4$, and G has 8 elts. of order 3.

Moreover, for any 3-Syl subgroup P, $[G : N_G(P)] = n_3 = 4$

So $N_G(P) = P$.

G acts by conjugation on its 3-Sylow subgroups.

Obtain

$$\varphi : G \to S_4.$$

The kernel is $\bigcap_{P \in Syl_3(G)} N_G(P) = \bigcap_P P = 1$.

18.5. So G is isomorphic to a subgroup of S_4.

What is $G \cap A_4$?

G has 8 elts. of order 3

There are 8 elts. of order 3 in S_4 and they are all in A_4.

So $|G \cap A_4| \geq 8$. Since it divides 12, $|G| = |A_4|$.

Note also: The 3-Sylow subgroups of A_4 are not normal, so such a group does actually exist.

Finally: The remaining elts. of A_4 are of order 2

So the 2-Sylow subgroup of A_4 is unique, hence normal.

Proposition. If G is a group of order 30, it has a group of order 15 [isomorphic to $\mathbb{Z}/15$] (and hence cyclic by above).

Proof. Let $P \in Syl_5(G)$ and $Q \in Syl_3(G)$.

Previously showed. If P or Q is normal in G, then PQ is a subgroup of G. (And it has 15 elts. So done.)

Now $n_5 = 1$ or 6

$n_3 = 1$ or 10 $\quad (\equiv 1 \pmod 3)$ and divides 30)

If neither P nor Q is normal then $n_5 = 6$, $n_3 = 10$, and G contains at least

$$1 + \underbrace{6 \cdot 4}_{\text{nontrivial elts. in 5-Sylows}} + \underbrace{10 \cdot 2}_{\text{nontrivial elts in 3-Sylows}} = 45 \text{ elements.}$$

Oops.

19.2

18.6.

Note. In fact we have $n_5 = 1$, $n_3 = 1$.

We've now accounted for 15 elements out of 30, and don't have room for the rest!

(to next)

14.3
~~18.07~~

Prop. If $|G| = 60$ and $n_5 > 1$ then G is simple.

Proof. Suppose otherwise, that $H \lhd G$ with $H \neq 1, G$.
By the usual numerology $n_5 = 6$. If $P \in Syl_5(G)$
then $[G : N_G(P)] = 6$ so
$|N_G(P)| = 10$.

Now, if $5 \mid |H|$ then since H is normal it must contain all six 5-Sylow subgroups, hence at least 25 elements.
Hence $|H| = 30$, but this contradicts previous example.

If $|H| = 6$ or 12, H has a normal Sylow subgroup P.
Since H is normal in G, its G-conjugates must live in H. But $P \lhd H$, so $P \lhd G$.

So can assume $|H| = 2, 3, 4$ and is normal.
G/H has size $30, 20$, or 15.
We showed in the cases 30 and 15, there is a normal 5-Syl subgroup. Can do smth similar with 20.
Its preimage Q has size $10, 15$, or 20 respectively.
It must also be normal in G (since the correspondence theorem preserves normality). But 5 divides it.
Contradicts first part!

Cor. A_5 is simple.

Proof. Find two 5-Sylow subgroups.

19.4 Simplicity of A_n.

Theorem. A_n is simple for $n \geq 5$.

[Not true for $n = 4$: $\{(1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \trianglelefteq A_4$.

Proof. Induction on n. Assume $n \geq 6$, $H \trianglelefteq A_n =: G$.
(nontrivial)

For each $i \in \{1, \dots, n\}$, write $G_i = \mathrm{Stab}_G(i)$
with $G_i \cong A_{n-1}$.

Assume first: Some element $1 \neq \tau \in H$ fixes some i.

Then $\tau \in H \cap G_i$ and $H \cap G_i \trianglelefteq G_i$.

By induction $G_i \cong A_{n-1}$ is simple so $H \cap G_i = G_i$.
$G_i \subseteq H$.

But then H must contain all the G_i's, since A_n is transitive.

By combinatorics we're already done with this case, $|H| > \frac{1}{2}|G|$.

Alternatively write any $\sigma \in A_n$ as

$$\sigma = \sigma_1 \sigma_2 \cdots \sigma_k$$

each product of two transpositions.

Since $n > 5$, each σ_j is in some G_i, hence σ is in H.

Contradiction.

19.5.

So: Can assume, no nontrivial elt. of H fixes anything.

If H contains τ whose cycle decomposition has any k-cycle with $k \geq 3$,

$$\tau = (a_1 \; a_2 \; a_3)(b_1 \; b_2 \; \cdots) \cdots$$

Then choose $\sigma \in G$ fixing a_1 and a_2 but not a_3.
($n \geq 5$, so we can do this.)

$$\sigma \tau \sigma^{-1} = (a_1 \; a_2 \; \sigma(a_3))(\sigma(b_1) \; \sigma(b_2) \; \cdots)$$

Now both τ and $\sigma\tau\sigma^{-1}$ are in H and send $a_1 \to a_2$.
So $\tau^{-1}\sigma\tau\sigma^{-1}$ fixes a_1 and is nontrivial since $\tau \neq \sigma\tau\sigma^{-1}$.

So no (≥ 3)-cycles in the decomposition.

Finally, we're down to

$$\tau = (a_1 \; a_2)(a_3 \; a_4)(a_5 \; a_6) \cdots$$

Let $\sigma = (a_1 \; a_2)(a_3 \; a_5)$, then

$$\sigma \tau \sigma^{-1} = (a_1 \; a_2)(a_5 \; a_4)(a_3 \; a_6) \cdots$$

Same pattern as before: τ and $\sigma\tau\sigma^{-1}$ act the same on a_1 but aren't identical.

We're done!

19.~~6~~ 20.1 Direct and semidirect products.

If $G_1, \ldots, G_k$ are groups, their <u>direct product</u> $G_1 \times G_2 \times \cdots \times G_k$ is the set of k-tuples $(g_1, g_2, \cdots, g_k)$ with $g_i \in G_i$ for each i.

The group operation is defined componentwise.

Similarly, can take $\prod_{\alpha \in S} G_\alpha$, direct product of infinitely many groups.

Some elementary propositions. (0) These are groups.

(1) $G_1 \times \cdots \times G_k$ is infinite if any G_i is, and otherwise $|G_1 \times \cdots \times G_k| = |G_1| \cdots |G_k|$.

(2) If you rearrange the G_i you get an isomorphic group.

(3). There are <u>projection homomorphisms</u>

$$G_1 \times \cdots \times G_k \longrightarrow G_{i_1} \times \cdots \times G_{i_r}$$

where $\{i_1, \ldots, i_r\}$ is any subset of $\{1, \ldots, k\}$. The kernel is isomorphic to the product of the G_j with j not any of the i's.

(4). Given homomorphisms $G \xrightarrow{\phi_i} H_i$ you get a product homomorphism

$$G \xrightarrow{\phi_1 \times \cdots \times \phi_k} H_1 \times \cdots \times H_k$$

$$g \longrightarrow (\phi_1(g), \cdots, \phi_k(g)).$$

19.7.20.2

Example. Let $G = \mathbb{R} \times \mathbb{R}$. Consists of

(a, b) : $a, b \in \mathbb{R}$,

$$(a, b) + (c, d) = (a+c, b+d).$$

Then $\mathrm{Aut}(G) = GL_2(\mathbb{R})$. This is precisely the definition!

(or is it....?)

Example. Let $G = \mathbb{Z}/3 \times \mathbb{Z}/5$.

Then $G \cong \mathbb{Z}/15$.

We saw it before. Easier proof:

$$\mathbb{Z}/15 \longrightarrow \mathbb{Z}/3 \times \mathbb{Z}/5$$

$$a \longmapsto (a, a).$$

It's a direct product of two quotient maps.

Hence a group hom.

Kernel is trivial. Both sides same side, hence onto.

Chinese Remainder Theorem.

Let $q_1, q_2, \cdots, q_n$ be pairwise coprime. Then, the homomorphism

$$\mathbb{Z}/q_1 \cdots q_n \xrightarrow{\phi} \mathbb{Z}/q_1 \times \cdots \times \mathbb{Z}/q_n$$

is ~~...~~ an isomorphism.

ϕ = (reduce mod q_1, ... reduce mod q_n).

Indeed, if $A \trianglelefteq G$ and $B \trianglelefteq G$ with $A \leq B$ then there is a commutative diagram

$$\begin{tikzcd}
G \arrow[rr, "g \to gB"] \arrow[dr, "g \to gA"'] & & G/B \\
& G/A \arrow[ur, "gA \to gB"'] &
\end{tikzcd}$$

and a special case (after taking direct products) is

$$\begin{tikzcd}
\mathbb{Z}/q_1 \cdots q_n \arrow[r, "\sim"] & \mathbb{Z}/q_1 \times \cdots \times \mathbb{Z}/q_n \\
\mathbb{Z} \arrow[u] \arrow[ur] &
\end{tikzcd}$$

which implies that (since the map $\mathbb{Z} \to \mathbb{Z}/q_1 \cdots q_n$ is obviously onto)

we can simultaneously solve systems of congruences.

Note. This all works for ring homs.

Classification of FG abelian groups.

Theorem.

(1) Let G be a FG abelian group; then

$G \cong \mathbb{Z}^r \times H$ with r a nonneg integer, H finite.

20.4

(2) If H is a <u>finite</u> abelian group, can write

$H \cong \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_r$ where each n_i divides the next.

Moreover, this representation is unique (among those following these rules).
(But there may be other ways to write e.g. $\mathbb{Z}/3 \times \mathbb{Z}/5 = \mathbb{Z}/15$.)

<u>Example</u>. Write down all iso. classes of abelian groups of order 180.

You probably had to do this for the GRE. [Sol'n omitted]

<u>Theorem</u>. Let G be a group with subgroups H, K with:

(1) H, K normal in G

(2) $H \cap K = 1$.

Then $HK \cong H \times K$. (Call HK the <u>internal direct product</u>)

We already established that HK is a group.

Why ~~is it abelian~~ do H and K commute? To show $hk = kh$, show $hkh^{-1}k^{-1} = 1$ for all $h \in H, k \in H$:

$$hkh^{-1}k^{-1} = h\underbrace{(kh^{-1}k^{-1})}_{\in H} = \underbrace{(hkh^{-1})}_{\in K}k^{-1} \in H \cap K = 1.$$

So define

$$HK \xrightarrow{\varphi} H \times K$$
$$hk \longrightarrow (h, k).$$

A homomorphism because
$$\varphi(h_1k_1h_2k_2) = \varphi(h_1h_2k_1k_2)$$
$$= (h_1h_2, k_1k_2)$$
$$\varphi(h_1k_1)\varphi(h_2k_2) = (h_1, k_1)(h_2, k_2).$$

<u>Surjective</u> by construction.

Injective because any elt. in the kernel is in $H \cap K$.

20.5.

Now suppose that G is a group with subgroups N and K such that N (only) is normal.

Assume further that $G = NK$ and $N \cap K = 1$.

~~Still true~~

Still true as before: Every elt. of G can be written uniquely in the form nk with $n \in N$ and $k \in K$.

But N is no longer required to commute with K.

Group law:

$$(n_1 k_1)(n_2 k_2)$$

$$= \underbrace{n_1 (k_1 n_2 k_1^{-1})}_{\text{elt. of } N} \underbrace{k_1 k_2}_{\text{elt. of } K}.$$

This is like a "twisted direct product" which we call a semidirect product.

The point: We have a map $K \xrightarrow{\phi} \mathrm{Aut}(N)$

$k \longrightarrow$ conjugation by k

$n \longrightarrow knk^{-1}$

or $n \cdot k$

and our group law is

$$(n_1 k_1)(n_2 k_2) = (n_1 \cdot k_1 \cdot n_2)\, k_1 k_2.$$

21.1. Semidirect products.

The construction.

Let $G = NK$ w/ N normal and $N \cap K = 1$.

Then each $g \in G$ can be written uniquely as $g = nk$ with $n \in N$ and $k \in K$, and

$$(n_1 k_1)(n_2 k_2)$$
$$= n_1 (k_1 n_2 k_1^{-1}) k_1 k_2$$
$$= n_1 \underbrace{(k_1 \cdot n_2)}_{\text{action by conjugation}} k_1 k_2 .$$

Here we get a map $K \xrightarrow{\phi} Aut(N)$

$k \longrightarrow$ conj. by k.

Can reverse the construction.

Def. Given groups N and K, and a hom $K \xrightarrow{\phi} Aut(N)$ inducing a left action of K on N, the semidirect product $N \rtimes_\phi K$ (or $N \rtimes K$) is the group of tuples (n, k) with group operation

$$(n_1, k_1)(n_2, k_2) = (n_1\, k_1 \cdot n_2, k_1 k_2).$$

21.2.

Basic properties.

(1) This construction defines a group G. [write it out!]

(2) The sets

$$\{(n,1) : n \in N\}$$
$$\{(1,k) : k \in K\}$$

are subgroups of G, and the "obvious" maps define isomorphisms to N and K.

If we identify N and K with their isomorphic images,

(3) $N \cap K = 1$ (obvious)

(4) $N \trianglelefteq G$, and $G/N \cong K$.

$$(n,k) \longrightarrow k.$$

(5) Combining (2) and (4), we see the quotient map has a section:

$$\begin{tikzcd} (n,k) \arrow[r] & k \\ G \arrow[r] & G/N \arrow[l, dashed, bend left, "k"] \end{tikzcd}$$

Note that quotients don't always have sections.

e.g. no homomorphism $\mathbb{Z}/5\mathbb{Z} \xrightarrow{\phi} \mathbb{Z}$,

such that

$$\begin{tikzcd} \mathbb{Z} \arrow[r, bend left, "\text{quotient}"] & \mathbb{Z}/5\mathbb{Z} \arrow[l, bend left, "\phi"] \end{tikzcd}$$

commutes.

Similarly with

$$\begin{tikzcd} 1 \arrow[r] & 1 \\ \mathbb{Z}/8\mathbb{Z} \arrow[r, bend left] & \mathbb{Z}/4\mathbb{Z} \arrow[l, dashed, bend left, "??"] \end{tikzcd}$$

(6) Within G, $k n k^{-1} = k \cdot n = \varphi(k) n$.

21.3

Most of these are straightforword.

Inverses.

What is $(n,k)^{-1}$?

If $(n,k)^{-1} = (n_1, k_1)$, want

$$(n,k)\cdot(n_1, k_1) = (1,1)$$

i.e. $(n\, k\cdot n_1,\ k k_1) = (1,1)$.

So demand $k_1 = k^{-1}$

and $k\cdot n_1 = n^{-1}$

i.e. $n_1 = k^{-1}\cdot n^{-1}$.

So : $(n,k)^{-1} = (k^{-1}\cdot n^{-1},\ k^{-1})$.

Check that it's an inverse on the other side as well.

Normality of N.

Compute $(n,k)\,(n_1, 1)\,(k^{-1}n^{-1}, k^{-1})$.

We don't really have to compute it.

Looks like a direct product in the second factor

so we win for free.

The relation $knk^{-1} = k\cdot n$:

$$(1,k)\,(n,1)\,(1,k^{-1})$$
$$= (1,k)\cdot(k\cdot n, 1) = (k\cdot n, 1).$$

21.4.

Proposition. TFAE, given $N, K, \varphi : K \to \mathrm{Aut}(N)$.

(1) $N \rtimes K$ is just a direct product. More specifically, the set map $N \rtimes K \longrightarrow N \times K$ is a group homomorphism (since isomorphism).

(2) The map $\varphi : K \longrightarrow \mathrm{Aut}(N)$ is the trivial map; equivalently, the action is trivial ($k \cdot n = n$ for all k, n)

(3) $K \triangleleft (N \rtimes K)$.

(2) $\to$ (1), (3) is, I think clear.

(3) $\to$ (2). Recall $knk^{-1} = k \cdot n$.

We saw before, if N and K are both normal, $N \cap K = 1$, then N and K commute with each other.

Examples.

Dihedral groups $D_n = C_n \rtimes \mathbb{Z}/2$

or $C_n \rtimes C_2$.

Need a map $C_2 \longrightarrow \mathrm{Aut}(C_n)$.

$0 \longrightarrow$ (trivial)

$1 \longrightarrow (x \to x^{-1})$

So D_n consists of pairs (r^i, s^j) subject to

$$(r^i, s^j) \cdot (r^m, s^k) = (r^i, s^k \cdot r^m, s^{j+k}).$$

~~Since $\varphi k = 0$ or 1, this says:~~

$$\cancel{(r^i, s^j) \cdot (r^m, 1) = (r^{i+m}, s^j)}$$

$$\cancel{(r^i, s^j) \cdot (r^m, s) = (r}$$

21.5.

So what's the group law?

$$(r^i, s)\cdot(r^j, s^k) = (r^{i-j}, s^{k+1})$$

$$(r^i, 1)\cdot(r^j, s^k) = (r^{i+j}, s^k).$$

In particular,

$$(1, s)\cdot(r^j, 1) = (r^{-j}, s) = (r^{-j}, 1)\cdot(1, s).$$

Equivalent to usual writing in terms of generators and relations.

Generalization. Let A be any abelian group. Then, since $(xy)^{-1} = x^{-1}y^{-1}$, the map $x \to x^{-1}$ is an automorphism.

Get a semidirect product $A \rtimes C_2$ in the same way.

Example. $\cancel{Z_3 \rtimes_\varphi Z_4}$ nooo! never do this $C_3 \rtimes_\varphi C_4$, where

$$C_4 \xrightarrow{\varphi} \mathrm{Aut}(C_3)$$
$$C_4 = \langle k \rangle$$
$$k \longrightarrow \text{inversion}.$$

This is the group $\langle n, k \mid n^3 = k^4 = 1,\ knk^{-1} = n^{-1} \rangle$

Claim. It is not isomorphic to A_4 or D_6.

Proof. Its 2-Sylow subgroups are cyclic.

21.6

<u>Example</u>. The Fro<u>benius</u> group F_ℓ, defined by

$$F_\ell = C_\ell \rtimes_\varphi C_{\ell-1}$$

$$\begin{array}{ccc} \varphi : C_{\ell-1} & \longrightarrow & \mathrm{Aut}(C_\ell) \\ \| & & \\ \langle k \rangle & & \\ k & \longrightarrow & \{ n \to n^g \}, \end{array}$$

where g is a pr<u>imitive</u> <u>root</u> modulo ℓ:

$$g^{\ell-1} \equiv 1 \pmod{\ell} \text{ and } g^i \not\equiv 1 \pmod{\ell} \text{ for } 0 < i < \ell - 1.$$

22.1.

Recall that <u>semidirect products</u> $N \rtimes_\varphi K$ were constructed from groups N, K and an action of K on N.

$$(n_1, k_1)(n_2, k_2) = (n_1\, k_1 \cdot n_2,\ k_1 k_2).$$

K and N embed as subgroups with N normal.

Can do the other way. If $G = NK$, $N \trianglelefteq G$, $N \cap K = 1$, then $G \cong N \rtimes_\varphi K$ with the action being conjugation.

<u>Example</u>. Let G be a group of order pq, $p<q$ prime.

Then $n_q \mid p$ and $n_q \equiv 1 \pmod q$ (Sylow's thm)
so the q-Sylow subgroup is unique, call it Q.
It's thus normal in G.
Writing P for <u>any</u> p-Sylow, $G \cong Q \rtimes_\varphi P$ for some

$$\varphi : P \to \mathrm{Aut}(Q).$$

it is cyclic but I don't recall proving this!

$\mathrm{Aut}(Q)$ is ~~cyclic~~ abelian of order $q-1$:
the elements of $\mathrm{Aut}(Q) = \mathrm{Aut}(C_q)$ are $x \to x^a$ for $a \pmod q$ not equal to 0.

Now ~~Ker(φ)~~ $\mathrm{Im}(\varphi)$ is a subgroup of this.
If $\underline{p \nmid q-1}$, get the trivial map only and
G is a direct product, hence cyclic.

22.2.

Suppose $p \mid q-1$. Now use: $\mathrm{Aut}(C_q)$ is cyclic.

Write $x \to x^g$ for a primitive root $g \pmod q$

(Easily proved using field theory)

Write $P = \langle y \rangle$ and $\langle \gamma \rangle$ for the unique subgroup of $\mathrm{Aut}(Q)$ of order p.

(A generator is $x \to x^{g^{\frac{q-1}{p}}}$.)

There are p possible automorphisms

$$\varphi_i : P \longrightarrow \mathrm{Aut}(Q)$$
$$y \mapsto i \longrightarrow \{ x \longrightarrow x^{g^{i \cdot \frac{q-1}{p}}} \}.$$

The trivial homomorphism gives $P \times Q \cong \mathbb{Z}/pq$.

The rest all give semidirect products $Q \rtimes P$.

But wait. They're all the same!

$$Q \rtimes_{\varphi_i} P = \langle \alpha, \beta \mid \alpha^q = \beta^p = 1,\ \beta\alpha\beta^{-1} = \alpha^{g^{i \cdot \frac{q-1}{p}}} \rangle$$
$$= \langle \quad " \quad \mid \quad " \quad \beta\alpha\beta^{-1} = (\alpha^i)^{g \cdot \frac{q-1}{p}} \rangle.$$

So there is an isomorphism

$$Q \rtimes_{\varphi_1} P \xrightarrow{\sim} Q \rtimes_{\varphi_i} P$$
$$\beta \longrightarrow \beta$$
$$\alpha \longrightarrow \alpha^i.$$

not quite right. Can you fix?

Example (wreath products).

Let N be a group, and $H \subseteq \mathrm{Sym}(k)$ for some n.

Then $N \wr H := \underbrace{(N \times \cdots \times N)}_{k \text{ copies}} \rtimes_\varphi H$,

where $H \longrightarrow \mathrm{Aut}(N \times \cdots \times N)$ is given by

$$\sigma \cdot (n_1, n_2, \ldots, n_k) = (n_{\sigma^{-1}(1)}, \ldots, n_{\sigma^{-1}(k)}).$$

Exercise. Check that it works out, and that you really do need the -1.

Example. Groups of order 12.

They are all semidirect. Get $\mathbb{Z}/12$, $\mathbb{Z}/2 \times \mathbb{Z}/6$, A_4, our previous "new" example of order 12, a semidirect product which is iso to $S_3 \times C_2$.

Exact sequences. (more later)

Suppose $G_1, \ldots, G_n$ are groups with homomorphisms $\varphi_1, \ldots, \varphi_{n-1}$. The sequence

$$1 \xrightarrow{\varphi_0} G_1 \xrightarrow{\varphi_1} G_2 \xrightarrow{\varphi_2} G_3 \xrightarrow{\varphi_3} \cdots \longrightarrow G_n \xrightarrow{\varphi_n} 1.$$

You can also write 0 here for the trivial group.

is an exact sequence if $\mathrm{Im}(\varphi_i) = \mathrm{Ker}(\varphi_{i+1})$ for each i.

(Note φ_0 is trivial, so demand φ_1 injective)
φ_n is trivial, demand φ_{n-1} surjective.)

22.4.

Example.

$$0 \longrightarrow \mathbb{Z} \xrightarrow{x \to nx} \mathbb{Z} \xrightarrow{\phi} \mathbb{Z}/n\mathbb{Z} \longrightarrow 0$$

ϕ : quotient map

is an exact sequence, because:

* $\mathbb{Z} \xrightarrow{x \to nx} \mathbb{Z}$ is injective;
* $\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ is surjective;
* the kernel of ϕ is exactly $n\mathbb{Z}$.

In general, if $N \triangleleft G$,

$$0 \longrightarrow N \xhookrightarrow{\text{inclusion}} G \longrightarrow N/G \longrightarrow 0$$

is exact.

Example.

$$0 \longrightarrow \mathbb{Z} \xhookrightarrow{n \to 2\pi i n} \mathbb{C} \xrightarrow{\exp} \mathbb{C}^* \longrightarrow 0$$

is exact.

Here $\mathbb{C}$ is the additive group of complex numbers

$\mathbb{C}^\times$ is the multiplicative group (excludes 0)

Kernel of the exponential map is $2\pi i \mathbb{Z}$

and exp is surjective.

(see this in complex geometry.)

22.5.

Ex. For any semidirect product $G = N \rtimes_\varphi H$, have an ES

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r] & N \rtimes_\varphi H \arrow[r, "\psi"'] & H \arrow[r] \arrow[l, dashed, bend right, "\sigma"'] \arrow[d, phantom, "\cong" rotate=90] & 0. \\ & & & G/N & \end{tikzcd}$$

Moreover it is split: the dotted line exists, such that $\psi \circ \sigma$ is the identity on H.

You can reverse this construction. Suppose you have an ES

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r, "\phi"] & G \arrow[r, "\psi"] & H \arrow[r] \arrow[l, dashed, bend left, "\sigma"] & 0 \end{tikzcd}$$

where σ is a splitting, and we regard N as a subgroup of G via ϕ (which is injective!)

σ is also injective.

Proof. Suppose $\sigma(h) = 0$; ~~with $\psi(\sigma(h)) = h$~~ ~~$= \psi(0)$)~~

Then $\psi(\sigma(h)) = h$ but this is $\psi(0) = 0$.

So H and N embed in G and $G = N \rtimes H$.

The ~~map~~ map $H \longrightarrow \mathrm{Aut}(N)$ is conjugation in G, determined by σ.

So this data is equivalent too!

p-groups.

Recall. G is a p-group if $|G| = p^a$ for some a.
[DF table of small order]

If $|G| = p$, then G is cyclic.

if $|G| = p^2$, G is $(\mathbb{Z}/p)^2$ or $\mathbb{Z}/p^2$.
(Sketch proof. Class equation $\Rightarrow Z(G) \neq 1$.
G has a normal subgroup of order p if not abelian.
Find a complement.)

if $|G| = p^3$ .... see the end of Ch. 5.5.

Basic properties of p-groups. Let P be one such.

1. $Z(P) \neq 1$.
2. If H is a nontrivial normal subgroup of P then $H \cap Z(P) \neq 1$.
   So every normal subgroup of order p is central.
3. If $H \trianglelefteq P$ then whenever $p^b \mid |H|$, H contains a subgroup of order p^b which is normal in P.
   (Interesting with $H = P$!)
4. If $H < P$ (i.e. is a proper ~~set~~ subgp of) then $H < N_P(H)$.
5. Let H be a maximal subgroup of P.
   (i.e. $\nexists H'$ with $H < H' < P$ (and $H \neq P$))
   (note: P is not considered a max'l subgp of itself)
   Then $H \trianglelefteq P$ and is of index p.

Proofs. Recall the class equation

$$|P| = |Z(P)| + \sum_{\substack{g_i \\ \text{nontriv conj.} \\ \text{classes}}} [P : C_P(g_i)] .$$

(1) follows because everything in the sum is divisible by p.

(2) will apply class equation to H.
Since H is <u>normal</u> it is a union of P-conjugacy classes.

Have $$|H| = |Z(P) \cap H| + \sum [P : C_P(g_i)]$$
sum: over nontriv conj. classes <u>in P</u>

So $p \mid |Z(P) \cap H|$ by previous argument
<u>Note</u>: $|Z(P) \cap H|$ is not necessarily $|Z(H)|$!

(3) Induct on a (i.e. $|P| = p^a$)
Assume $a > 1$, $H \neq 1$.
By (2), $H \cap Z(P) \neq 1$, by Cauchy's Thm $H \cap Z(P)$ contains a normal subgp Z of order p.

Look in $P/Z =: \overline{P}$ with order p^{a-1}, $\overline{H} := H/Z \trianglelefteq \overline{P}$.
By induction, $\overline{H}$ contains subgroups of order $1, p, p^2, \ldots, |\overline{H}|$ normal in $\overline{P}$.

Use correspondence theorem, normality + indices are preserved!
consider the inverse images under quotient map.

23.3

(4) Induct on $|P|$ again, can assume $|P| > p^2$.

Let $H < P$.

Recall $Z(P) \neq 1$, so if $Z(P) \not\subseteq H$ then

$\langle H, Z(P) \rangle \subseteq N_P(H)$ and that's bigger than H.

Otherwise, pass to $P/Z(P)$ and use correspondence again.

(5). If H is a maximal subgroup, then $H < N_P(H)$

so by (4) $\underline{H \triangleleft P}$.

Then P/H is a p-group with no nontrivial subgroups.

Only possible if $|P/H| = p$.

Nilpotent and solvable groups, composition series.

Suppose we have a series of groups

$$1 = G_0 \subseteq G_1 \subseteq G_2 \subseteq \cdots \subseteq G_k = G.$$

Interested in various properties of these.

<u>Def</u>. If, for each i, $G_i \triangleleft G_{i+1}$ and G_{i+1}/G_i is <u>simple</u>,

this is called a <u>composition series</u>.

Note: You can't refine one further (by def.)

N<u>ot</u> assumed that the G_i are all normal in G.

<u>Jordan - Hölder Theorem</u>. If G is a nontrivial finite group,

(1) G has a composition series

(2) Any two composition series have the same factors G_{i+1}/G_i up to reordering.

23.4

Def. For any group G, define the upper central series

$Z_0(G) = 1$

$Z_1(G) = Z(G)$

and for each i, ~~choose~~ writing $\pi_i : G \to G/\underbrace{Z_i(G)}$

set $Z_{i+1} = \pi^{-1}(Z(G/Z_i(G)))$.

Yes, these are all normal.

Obtain a sequence of subgroups

$$Z_0(G) \leq Z_1(G) \leq Z_2(G) \leq \cdots,$$

this is the upper central series.

Def. G is nilpotent if we ever get G.

Note. If G is finite, then can't go on forever.
Either the UCS reaches G or it gets stuck.
It gets stuck iff $G/Z_i(G)$ has trivial center for some i.

Example. p-groups ~~is~~ are nilpotent.
Proof: $G/Z_i(G)$ will also be a p-group, and never have trivial center.

Example. Abelian groups.

The big theorem. TFAE, for a finite group.
1. G is nilpotent.
2. For all $H < G$, $H < N_G(H)$.
3. Every p-Sylow subgroup (for all p) is normal in G
4. G is the direct product of its p-Sylow subgroups.
5. (Not to be proved here) Every maximal subgroup is normal.

23.5 = 24.1

Proof. (4) → (1). Jack up the proof that p-groups are nilpotent.

(1) → (2) as before:

If $Z(G) \not\subseteq H$, then $\langle H, Z(G)\rangle$ normalizes H

Otherwise pass to $G/Z(G)$.

This is nilpotent by construction, so by induction on $|G|$

(1) → (2) in $G/Z(G)$. Now use correspondence.

(2) → (3) [Slightly sketchy]

Let P be a p-Sylow, $N = N_G(P)$.

But $P \trianglelefteq N_G(N)$ also. So $N_G(N) \leq N$, so $= N$.

(3) → (4) Let $P_1, \dots, P_r$ be the p-Sylows.

~~Their product is direct~~

They're all normal and intersect in the identity,

so by previous results product is direct.

[Use induction to be more precise.]

There is also an upper central series

$G^0 = G$

$G^1 = [G, G] = \langle \underbrace{[h,k]}_{h^{-1}k^{-1}hk} : h \in G, k \in G \rangle$

$G^2 = [G, G^1] = \langle \quad " \quad : h \in G, k \in G^1 \rangle$

$\vdots$

So $G^0 \supseteq G^1 \supseteq \cdots$

H terminates if the other one does.

24.2.

Solvable groups:

Def. A group G is solvable if there exists a series

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_s = G$$

with each H_{i+1}/H_i abelian.

One way to tell: Given G, define the derived series

$G^{(0)} = G$

$G^{(1)} = [G, G]$

$G^{(2)} = [G^{(1)}, G^{(1)}]$ so $G^{(i)} \subseteq G^i$ for each i.

etc.

Thm. G is solvable $\Longleftrightarrow$ $G^{(n)} = 1$ for some $n \geq 0$.

Proof. If G is solvable w/ series as above,

prove $G^{(i)} \subseteq H_{s-i}$ as above.

By induction, assume $G^{(i)} \subseteq H_{s-i}$, prove $G^{(i+1)} \subseteq H_{s-(i+1)}$.

Have $G^{(i+1)} = [G^{(i)}, G^{(i)}] \subseteq [H_{s-i}, H_{s-i}]$.

Must argue $[H_{s-i}, H_{s-i}] \subseteq H_{s-(i+1)}$ if $H_{s-i}/H_{s-(i+1)}$ abelian.

Look at the image of any $[x,y] = x^{-1}y^{-1}xy$ in the quotient $H_{s-i}/H_{s-(i+1)}$.

It's abelian, so the image is 1. And that's it!

24.3. Conversely, if $G^{(n)} = 1$, the series
$$1 = G^{(n)} \lhd G^{(n-1)} \lhd \cdots \lhd G^{(0)} = G \quad \text{works.}$$

In general, must prove for any group H that $[H, H]$ is normal in H with abelian quotient.

A clever way of proving $[H, H] \lhd H$.

Let $\sigma : H \to H$ be <u>any</u> automorphism of H (conjugation or otherwise)

Then
$$\sigma([x, y]) = \sigma(x^{-1}y^{-1}xy) = \sigma(x)^{-1}\sigma(y)^{-1}\sigma(x)\sigma(y)$$
$$= [\sigma(x), \sigma(y)]$$

So σ sends commutators to commutators.

And then $H/[H, H]$ is abelian by essentially the same argument as before. Let $x, y \in H$, $\bar{x}, \bar{y}$ images in $[H, H]$.

Must show ~~x~~ $\bar{x}\bar{y} = \bar{y}\bar{x}$, i.e. $\bar{x}^{-1}\bar{y}^{-1}\bar{x}\bar{y} = 1$ for all $x, y \in H$.

Equivalent to $x^{-1}y^{-1}xy = [x, y] \in [H, H]$.

True by definition!

<u>Proposition</u>. Let $G \xrightarrow{\varphi} K$ be a surjective homomorphism with $H \leq G$. Then:

(1) $H^{(i)} \leq G^{(i)}$ for all $i \geq 0$.
So if G is solvable, H is also. } note: there's no K here!

(2) $\varphi(G^{(i)}) = K^{(i)}$.

(3) If $N \lhd G$, and N and G/N are solvable, so is G.

24.4
Proofs.

(1) is obvious if you work from the top;

$$H' \subseteq H \Rightarrow [H', H'] \subseteq [H, H].$$

(2) Commutators commute w/ homomorphisms.

i.e. $\varphi([x,y]) = [\varphi(x), \varphi(y)]$

so $\varphi(G^{(i)}) \subseteq K^{(i)}$.

But since φ is surjective, every commutator in K is the image of a commutator, so get equality (by induction).

(3) ~~apply~~

$$1 = \underbrace{N^{(0)} \triangleleft N^{(1)} \triangleleft \cdots \triangleleft}_{n \text{ is solvable}} N^{(k)} \underbrace{\triangleleft \cdots\cdots \triangleleft G}$$

Here, we pull back a derived series

$$1 = H^{(0)} \triangleleft \cdots \triangleleft H^{(r)} = G/N$$

for G/N to G.

~~We know the images~~

Alternatively, apply 2:

If G/N and N are solvable, apply (2) to

$$G \to G/N.$$

Eventually, for large enough n, $\varphi(G^{(n)}) = 1$ because G/N is solvable. So $G^{(n)} \subseteq N$, and now apply 1. We eventually get down to the trivial group.

24.5. Some cool theorems:

Let G be a finite group. In each of the following situations, G is solvable:

(1. Burnside) $|G| = p^a q^b$ for primes p, q.

(2. Hall) If $|G| = p^a m$ and G has a subgroup of index m.

(3. Feit - Thompson) $|G|$ is odd.

(4. Thompson) If for all $x, y \in G$, $\langle x, y \rangle$ is a solvable group.

But plenty of groups aren't solvable (e.g. A_5 which is simple)

So there are no non-abelian finite simple groups of odd order!