Lecture 1

Algebra consists, generally speaking, of Groups, Rings, and Fields. These are covered, respectively, in 220A, 220B, and 220C.
We will begin with the minimal possible axioms, and go on to more extensive axioms. If you start with very few axioms, there are too many examples. If you go too far with axioms, you have too many examples. Group theory is all about binary operations.

Definition 0.1. Let S be a set. A binary operation on S is a function $f : S \times S \to S$. The image of $(a, b) \in S \times S$ under f is often denoted by $a * b$, or simply ab.

Definition 0.2. A binary operation is called associative if, for each $a, b, c \in S$, we have

$$(ab)c = a(bc)$$

Definition 0.3. An element $e \in S$ is an identity if $ex = xe = x$ for all $x \in S$

Definition 0.4. A monoid is a set S equipped with a binary operation which is associative, and which admits an identity.

Lecture 2

Given $x_1, \ldots, x_n \in M$, with M a monoid, we may inductively define

$$\prod_{i=1}^{n} x_i \stackrel{\text{def}}{=} (\prod_{i=1}^{n-1} x_i)x_n$$

Fact: In a commutative monoid, given any bijection $\psi : \{1, \ldots, n\} \to \{1, \ldots, n\}$,

$$\prod_{i=1}^{n} x_{\psi(i)} = \prod_{i=1}^{n} x_i$$

Definition 0.5. A group G is a monoid such that $\forall x \in G$, $\exists y \in G$ such that $xy = yx = e$. Here, y is called an inverse of x. Note, we have not yet proved that y is unique.

Claim. *For any $x \in G$, for G a group, x^{-1} is unique.*

Proof. Let y, y' be inverses to x. Then

$$y = ey = (y'x)y = y'(xy) = y'e = y'$$

■

Example 0.1. Let G be a group. Let S be a nonempty set.
The set of maps from S to G, denoted $M(S, G)$, is a group as follows.
Given $f, g \in M(S, G)$, define $fg(x) = f(x)g(x)$.
Identity: $e(x) = e \forall x \in S$.
Inverses: For an $f \in M(S, G)$, f^{-1} is the function such that $(f^{-1})(x) = f(x)^{-1}$.

Example 0.2. Given a nonempty set S, define Perm_S as the set of all bijective maps from S to S. This forms a group under composition.
When $|S|$ is a finite set of size n, we identify Perm_S with S_n.

Example 0.3. Let k be a field, and V a vector space over k. Then $GL(V)$ and $GL(n, k)$ are groups.

Example 0.4. $\mathbb{Q}$ is a group. $\mathbb{Q}^\times$, which is $\mathbb{Q}\backslash\{0\}$, is a group under multiplication. This works for any field.

Example 0.5. $\mathbb{Z}$ is an additive group. $\{1, -1\}$ forms a multiplicative group.

Definition 0.6. A group G is called cyclic if $\exists a \in G$ such that every $x \in G$ is of the form a^n for some $n \in \mathbb{Z}$. Such an a is called a generator.
So $\mathbb{Z}$ is (additively) cyclic with generators ± 1.

Definition 0.7. The order of G is $|G|$ if G is finite, and ∞ otherwise.

Definition 0.8. Let $N \in \mathbb{N}$. Then the Nth roots of unity form a multiplicative subgroup of $\mathbb{C}$. It is cyclic, and generated by $e^{\frac{2\pi i k}{N}}$.
An element $e^{\frac{2\pi i k}{N}}$ is called a primitive if it is a generator.
For example, for $N = 4$, our group would be $\{\pm 1, \pm i\}$. The primitives would be $\pm i$.
$\{e^{\frac{2\pi i k}{N}}\}$ is a generator of the Nth roots of unity if and only if k is coprime to N.

Let P be a regular polygon with N sides. Let $\text{Aut}(P) = \{$ automorphisms of $P\}$.
The automorphisms of P form a group, and it is generated by a reflection and a rotation.

Definition 0.9. A subset $S \subseteq G$ generates G if every $x \in G$ can be written $x = s_1^{a_1} \cdots s_n^{a_n}$ with $s_i \in S$ for each i.
Let $\sigma, \tau \in \text{Aut}(P)$. We can see that $\tau\sigma\tau^{-1} = \tau\sigma\tau = \sigma^{-1} = \sigma^{n-1}$.
If G is generated by S, any expression of the form $s_1^{a_1} \cdots s_n^{a_n}$, with $s_i \in S$ and $a_i \in \mathbb{Z}$ is called a word in the generators.
If W is a set of words in S, then

$$\langle S \mid \rangle$$

is the free group on S quotiented by the normal subgroup generated by all elements of W. This is called a group presentation of the resulting group.
So $\text{Aut}(P) = \langle \sigma, \tau, \sigma^n = \tau^2 = (\tau\sigma)^n = e \rangle$

Lecture 3

Definition 0.10. A monoid M is called commutative/abelian if for all $x, y \in M$, $xy = yx$.
$N \subset M$ is called a submonoid iff $x, y \in N \implies xy \in N$, and $e \in N$.
A function $f : M \to N$ is a homomorphism of monoids if $f(xy) = f(x)f(y)$ for all $x, y \in M$.

Definition 0.11. A commutative/abelian group and a homomorphism of groups are defined exactly as above. A subgroup is defined similarly as above, but with the added requirement that $x \in N$ implies $x^{-1} \in N$.

Example 0.6. Let μ_N denote the Nth roots of unity, generated by $e^{\frac{2\pi i}{N}}$. We have a morphism $f : \mathbb{Z} \to \mu_N$ given by $f(k) = e^{\frac{2\pi ik}{N}}$.

Example 0.7. We have a $\pi : D_n \to \mu_N$ given by $\pi(\sigma) = -\pi(\tau) = -1$, $\pi(e) = e$.

Definition 0.12. Given $\phi : G \to H$ a homomorphism of groups, the kernel of ϕ, denoted $\ker(\phi)$, is defined by

$$\ker(\phi) \stackrel{\text{def}}{=} \{g \in G \mid \phi(g) = e\}$$

Similarly, we define the image, $\mathrm{Im}(\phi)$, by

$$\mathrm{Im}(\phi) = \{h \in H \mid \exists g \in G, \phi(g) = h\}$$

Definition 0.13. If N is a subgroup of G, then we say that N is normal if for all $g \in G$ and $n \in N$, we have $gng^{-1} \in N$.

Lemma 1. *Given a morphism $\pi : G \to H$, then*

1. *π is injective if and only if $\ker(\pi) = \{e\}$. In this case, we say $\pi : G \hookrightarrow H$.*

2. *π is surjective if and only if $\mathrm{Im}(a) = H$. In this case, we say $\pi : G \Rightarrow H$.*

Proof. The second assertion is obvious, but we shall prove the first. Suppose that π is injective. Then clearly $\ker(\pi) = \{e\}$. Now, suppose that $\ker(\pi)$ is trivial. Suppose that $\pi(a) = \pi(b)$. Then $\pi(a)\pi(b)^{-1} = e = \pi(ab^{-1})$, so $ab^{-1} = e$, so $a = b$. ■

Proposition 1. *Given a group homomorphism $\pi : G \to H$, the kernel of π is a normal subgroup of G.*

Proof. Choose $x \in G, y \in \ker(\pi)$. Then

$$\pi(xyx^{-1}) = \pi(x)e\pi(x)^{-1} = e$$

So $xyx^{-1} \in \ker(\pi)$.

Definition 0.14. Given $H \trianglelefteq G$, we define the quotient group as follows.
For any $g \in G$, we denote the left coset of H containing g as gH. The set of left cosets forms a group, with the group operation given by

$$(gh)(g'H) = (gg')H$$

This is not, a priori, well defined, so we will prove that now. That is,

Lemma 2. *$gH = g'H$ if and only if $g(g'^{-1}) \in H$.*

Proof. First, assume $gH = g'H$. Then $g \in g'H$, i.e there is some $h \in H$ such that $g = g'h$. Thus, $gg'^{-1} = h \in H$. Now, assume $g(g'^{-1}) \in H$. Then choose $x \in gH$. There is an $h \in H$ such that $g = g'h$.
Then $g'g^{-1}x = g'g^{-1}gh = g'h$, and so $x = g'h\underbrace{(g'g^{-1})}_{\in H} \in g'H$.
This is one inclusion, and the other follows similarly.

Claim. *If H is normal, then G/H, the set of left cosets of H, inherits a group structure from G as follows: $(gH)(g'H) \overset{\text{def}}{=} gg'H$*

Proof. For well-definedness, assume that $gH = ghH$. Note that $(ghg')(gg')^{-1} = ghg'^{-1} \in H$. So by a previous claim, $gH = ghH$.

Lecture 4

Definition 0.15. Let G be a group. The automorphism group $\mathrm{Aut}(G)$ of G is defined as the group of bijective homomorphisms $f : G \to G$, with the group operation defined as function compositions.
For a given $x \in G$, there is an automorphism given by $g \mapsto x^{-1}gx$, which is conjugation by x. Any automorphism which can be given by conjugation is called an inner automorphism, and they form a normal subgroup of $\mathrm{Aut}(G)$.

Claim. *Consider $f : G \to \mathrm{Aut}(G)$ defined by $x \mapsto (g \mapsto x^{-1}gx)$. This is a group homomorphism.*

Proof. For any $g_1, g_2 \in G$, and any $x \in G$, we have

$$f_x(g_1g_2) = x^{-1}g_1g_2x = x^{-1}g_1xx^{-1}g_2x = f_x(g_1)f_x(g_2)$$

So, $f_x \in \mathrm{Aut}(G)$. Now, let $x, y \in G$ and $g \in G$. Then

$$f_{xy}(g) = (xy)^{-1}gxy = y^{-1}x^{-1}gxy = y^{-1}(x^{-1}gx)y = (f_x \circ f_y)(g)$$

■

Definition 0.16. The opposite group of a group G has the same underlying set as G, whose group operation (denoted $*_{op}$) is defined by

$$(x *_{op} y) \stackrel{\text{def}}{=} yx$$

Claim. *This is associative*

Proof. We have

$$(x *_{op} y) *_{op} z = (yx) *_{op} z = zyx = x *_{op} (zy) = x *_{op} (y *_{op} z)$$

■

Fact: H normal is equivalent to every left coset of H is a right coset.
Notation: $H \trianglelefteq G$ means H is a subgroup of G.
$H \triangleleft G$ means H is a normal subgroup of G.

Lemma 3. *Let $K \trianglelefteq H \trianglelefteq Q$. Let $\{x_i\}$ be a set of left coset representatives for $H \trianglelefteq G$, i.e. $\{x_i H\}$ is a complete, non-repeating set of left cosets.*
Let $\{y_i\}$ be a set of left coset representatives for $K \trianglelefteq H$.
Then $\{y_i x_i\}$ is a set of left coset representatives for $K \trianglelefteq G$.

Corollary 0.1. *If $(G : H)$ denotes the number of left cosets of H in G, then*

$$(G : K) = (G : H)(H : K)$$

Proof. We will prove the lemma, and the corollary will follow.
First, why is it a complete list of cosets? First, if $g \in G$, then $\exists! x_i$ such that $g \in x_i H$, i.e. $g = x_i h$ for some $h \in H$. Further, for $h \in H$, $\exists! y_j$ such that $h \in y_j K$. Then $g = x_i h \in x_i y_j K$.
Why is it unique? Exercise

■

Definition 0.17. $|G| = (G : \{e\})$.

Corollary 0.2. *For normal subgroups, $|G| = |G/N| \cdot |N|$*

Definition 0.18. If $g \in G$, then the order of the element g is defined as the smallest integer k such that $g^k = e$. If there is no such k, then we say the order is ∞.

Lecture 5

Recall: $(G : H)$ is the index of H in G, which is the number of left cosets of H in G.
We know that

$$\frac{|G|}{|H|} = \frac{(G : e)}{(H : e)}$$

Corollary 0.3. *If $g \in G$, $o(g) < \infty$, $|G| < \infty$, then $o(g) \mid |G|$.*

Corollary 0.4. *If G is a group with $|G| = p$, a prime number, then $o(g) = 1$ or p for all $g \in G$.*

Lemma 4. *There are exactly 1 element of order 1 in any group.*

Proof. We know $o(e) = 1$. If e, e' are both units in G, then $e = ee' = e'$.

Corollary 0.5. *If $|G| = p$, then G is cyclic.*

Proof. Choose $g \neq e$. Then $o(g) = p$, so $\{g^0, g^1, \ldots, g^{p-1}\}$ is p distinct elements in G, so g must generate G.
Classification of groups of order n.

$n = 1$	$G = \{e\}$
$n = 2$	prime
$n = 3$	prime
?	

We will classify all groups of order 4 by force, without the proper tools (eg semidirect products, sylow theorems).
If there exists a g such that $o(g) = 4$, then G is cyclic. Otherwise, all $g \neq e$ have order 2. Let $G = \{e, a, b, c\}$. If $ab = a$, then $b = c$, and similarly if $ab = b$. So $ab = c$. Thus, we know every group of order 4.

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

The above is the *Cayley table of the group.*

Claim. *The G above, the Klein 4-group, is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

Definition 0.19. For H, K groups, we define their direct product $H \times K$ by

$$H \times K = \{(h, k) \mid (h, k)(h', k') = (hh', kk')\}$$

Continuing with the classification, 5 is prime, so we move on to $n = 6$. If it's non-cyclic, then $o(g) \in \{1, 2, 3\}$ for all $g \in G$.
We can classify them by setting up a semidirect product...
Let H, K be groups, and let $\psi : H \to \mathrm{Aut}(N)$. We define the semidirecN product by $H \ltimes N$. The underlying set is $H \times N$, and the group operation is given by

$$(x_1, h_1)(x_2, h_2) = (x_1 \psi(h_2)(x_2), h_1 h_2)$$

⋮

7 is prime. Consider $n = 8$.

The abelian groups of this order are $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

If it isn't abelian, it could be D_4 or Q_8. Q_8 is the quaternion group, consisting of $\{\pm 1, \pm i, \pm j, \pm k\}$, with $i^2 = j^2 = k^2 = ijk = -1$.

It is called this because it is the group of units of $\mathbb{H}$, the quaternions. H is for William Rowe Hamilton, who first wrote this down, and whose name scans exactly the same as "Alexander Hamilton."

Let's move on to $n = 9$. It could be cyclic, and if it is cyclic but non-ableian, then it could be $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. It could be that there exists a different group such that $g \neq e \implies o(g) = 3$. This turns out not to be the case, but proving it with only what we have now would be tough.

If $|G| = 10$, then G is either cyclic, a product of cyclics, or dihedral.

Basic Constructions

1. Theorem about finitely generated abelian groups
2. Semidirect product constructions: If $N \lhd G$, then G acts on N by conjugation: $\psi : G \to \mathrm{Aut}(N)$, $x \mapsto (g \mapsto xgx^{-1})$.

   For a semidirect product, we need $H \lhd G$ such that $|G| = |N||H|$.
3. Special constructions.

One of the big steps for the class project will be finding normal subgroups.

Definition 0.20. A group G is simple if it has no nontrivial normal subgroups.

Strategy to understand all finite groups:

1. Find simple ones. This one has been achieved through work starting in the 1960s through the 1980s, and 10000 journal pages.
2. Assemble them into more complicated ones

There are a few big classes of finite simple groups:

- Alternating group A_n, for $n \geq 3$
- Finite groups of Lie type, groups of matrices over finite fields.

There are also the sporadic groups, of which there are 26, which don't fit into any other category. They include the monster group, the largest simple group, and the baby monster group, the second largest simple group.

Lecture 5

Correction to a statement made last time:
There is something called the J-invariant of elliptic curves. An elliptic curve is a torus with a complex structure. This is $\mathbb{C}/\Lambda$, where Λ is a free $\mathbb{Z}$-module of rank 2. Let τ be one of the generators. We want all things of the form $\Lambda_\tau = \{m + n\tau\}$.
For a change of basis in Λ, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. I don't really know what the heck he's talking about lol, I'm gonna go fiddle with the preamble.
Groups can be represented on vector spaces. We want to define "multiplication by elements of G" on elements of V, such that $g \cdot (v_1 + v_2) = g \cdot v_1 + g \cdot v_2$, nad $(g \cdot (cv)) = c(g \cdot v)$, where $c \in k$, the ground field of V.
This gives a homomoprhism $G \to \mathrm{GL}(V)$.
More generally, groups can "act" on sets (ignoring any other structure). Recall that for a set S, we define $\mathrm{Perm}(S)$ as the set of all bijective $f : S \to S$.

Definition 0.21. A group action on the set S is a group homomorphism $\pi : G \to \mathrm{Perm}(S)$. We denote for $g \in G$, $s \in S$, we denote $\pi(g)(s)$ by $g{\cdot}s$. Note that $(g_1{\cdot}g_2){\cdot}s = g_1 \cdot (g_2 \cdot s)$.

Definition 0.22. If $G \to \mathrm{Perm}(S)$ is a group action, the orbit of the action containing $s \in S$ is

$$\{g \cdot s \mid g \in G\}$$

Note that $S = S_1 \coprod S_2 \coprod \cdots$ is a decomposition of S into disjoint orbits. We can then obtain $G \to \mathrm{Perm}(S_i)$.
Consider $n \times n$ matrices that are invertible and have a single 1 and all the rest 0 in each row and each column. This is a subset of $\mathrm{GL}(n, \mathbb{F})$. We can represent a group as matrices by constructing a basis indexed by the group elements $\{v_{g_1}, v_{g_2}, \ldots, v_{g_d}\}$, and define $\pi(g)(v_{g_i}) = v_{gg_i}$.
In this way we can identify S_3 with the set of 3×3 matrices which act on the basis $\{v_{s_1}, v_{s_2}, v_{s_3}\}$ according to the permutation of the indices.
So, given $\sigma \in jS_3$, there is a $\pi(\sigma) \in \mathrm{GL}(3, \mathbb{F})$, and $(6, \operatorname{char} \mathbb{F})$.
Any element of S_n can be decomposed into cycles, like so

$$\begin{aligned} S_n = &\{1, \sigma(1), \sigma^2(1), \ldots, \sigma^n(1)\} \\ &\cup \{i, \sigma(i), \ldots\} \\ &\cup \vdots \end{aligned}$$

Lecture 6

Recall: $S_n \overset{\text{def}}{=} \text{Perm}\{1, 2, \ldots, n\}$.
For $\sigma \in S_n$, $\langle\sigma\rangle$ denotes the cyclic subgroup of S_n generated by σ.
We arrange elements such that $\sigma(i_k^{(j)}) = \begin{cases} i_{k+1}^{(j)} & k < n_j \\ i_1^{(j)} & k = n_j \end{cases}$

$$\{1, 2, \ldots, n\} = \coprod_j \{i_1^{(j)}, \ldots, i_{n_j}^{(j)}\}$$

So $\sigma = [i_1^{(1)}, \ldots, i_{n_1}^{(1)}] \cdots [i_1^{k)}, \ldots, i_{n_k}^{(k)}]$
Let $G \subset S_4$, with $G = \{e, [12][34], [13][24], [14][25]\}$. We can see $G \cong V_4$, the Klein 4-group.

Claim. *G is normal in S_4.*

Proof. Let $\sigma = [i_1^{(1)}, \ldots, i_{n_1}^{(j)}] \cdots$. Then

$$\tau^{-1}\sigma\tau = [\tau(i_1^{(1)}), \ldots, \tau(i_{n_1}^{(j)})] \cdots$$

for $\tau \in S_4$. Indeed, $\tau^{-1}([12][34])\tau = [\tau(1)\tau(2)][\tau(3)\tau(4)] \in G$

■

Let S_n act on the K, the functions from $\mathbb{Z}^n$ to $\mathbb{Z}$. So this is $\pi : S_n \to \text{Perm}\,\text{Hom}_{Set}(\mathbb{Z}^n, \mathbb{Z})$.
Define $\pi(\sigma)f(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$. It is clear that $\pi(\tau)\pi(\sigma)f = \pi(\tau\sigma)f$.
$\coprod_j \{1_i^{(j)}, \ldots, i_{n_j}^{(j)}\}$,
Here is Quinn's explanation of how this cycle/orbit nonsense notation works.

$$\tau(\sigma(\tau^{-1}(x)))$$

$$\tau^{-1}(x) = i_k^{(j)} \implies x = \tau(i_k^{(j)})$$

$$\sigma(\tau^{-1}(x)) = i_{k+1}^{(j)}$$

$$\tau(\sigma(\tau^{-1}(x))) = \tau(i_{k+1}^{(j)})$$

Let $f(x_1, \ldots, x_n) = \prod_{1 \le i < j \le n}(x_i - x_j)$.
Define $\varepsilon : S_n \to \{\pm 1\}$ by $\pi(\sigma)f(x_1, \ldots, x_n) = \varepsilon(\sigma)f(x_1, \ldots, x_n)$.

Proposition 2. *First, every σ is a product of simple transpositions. Second,* $\text{sgn}(\varepsilon) \overset{\text{def}}{=} (-1)^{\textit{number of transpositions}}$

Proof. ■
$\ker \text{sgn} = A_n$, the alternating group.
We see $G \lhd A_4$, with $|A_4/G| = 3$. So $A_4/G \cong Z_3$.

Theorem 0.6. *For later: A_n is simple for $n \geq 5$.*

Definition 0.23. A tower of subgroups is a collection of subgroups

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_m = \{e\}$$

A tower is normal if $G_{i+1} \lhd G_i$.
A normal tower is ableian (cyclic) if G_i/G_{i+1} is abelian (cyclic) for all i.
A group G is solvable if it has an abelian tower with $G_m = \{e\}$.
A refinement of a tower is a new tower into which some groups have been inserted.

Proposition 3. *Any abelian tower has a cyclic refinement.*

Lecture 7

Lemma 5. *Let G be a finite abelian group. Then G admits a cyclic tower ending in $\{e\}$.*

Proof. We will induct on $|G|$. If $G = \{e\}$ it's true. This is our base case.
Otherwise, let $x \in G$ be a non-identity element of G. Let $X =< x > \lhd G$.
Consider $G' = G/X$. $|G/X| < |G|$, so

$$G/X = G'_0 \supseteq G'_1 \supseteq \cdots \supseteq \{e\}$$

Let $G_j = \pi_X^{-1}(G'_j) \lhd G$, where $\pi_X : G \to G/X$ is the projection map.
Then

$$G \supseteq G_0 \supseteq \cdots \supseteq X$$

This is a cyclic tower, because $G_j/G_{j+1} = G'/G'_{j+1}$. We can add $\{e\}$ to the end of this tower, because X is cyclic.

Proposition 4. *Any abelian tower admits a cyclic refinedment.*

Proof. Consider

$$\Gamma = \Gamma_0 \supseteq \Gamma_1 \supseteq \cdots \supseteq \Gamma_i \supseteq \cdots$$

We know $\Gamma_{i+1} \lhd \Gamma_i$ such that Γ_i/Γ_{i+1} is abelian.
Γ_i/Γ_{i+1} has a cyclic tower by the lemma; so the inverse image of Γ_{i+1} in Γ_i under the projection map has a cyclic tower, so

$$\Gamma_i \underbrace{\supseteq \cdots \supseteq}_{\text{new cyclic tower}} \Gamma_{i+1}$$

Example 0.8. Let $G = \mathrm{GL}(n, \mathbb{F})$.
Let N be the strictly upper triangular matrices, i.e. upper triangular matrices with 0 on the diagonal.

$$\begin{pmatrix} 0 & a_1 & a_2 & \cdots & a_{1n} \\ 0 & 0 & \cdots & \cdots & a_{2n} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 & a_{nn} \end{pmatrix}$$

N^{r-1} has the form

$$\begin{pmatrix} 0 & 0 & a_{12} & \cdots & a_{1n} \\ 0 & 0 & \cdots & \cdots & a_{2n} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & 0 \end{pmatrix}$$

Let $U_r = \{I + A \mid A \in N_r\}$. This is a subgroup of $\mathrm{GL}(n, \mathbb{F})$.
We have a tower

$$U_1 \supseteq U_2 \supseteq \cdots \supseteq U_k$$

It turns out that U_{i+1} is normal in U_i, but this is not obvious. We have that $U_i/U_{i+1} = \mathbb{F}^{n-i}$.
Let's review some things we know. S_1 is trivial, S_2 is cyclic, $S_3 \trianglelefteq A_4 \cong \mathbb{Z}/3\mathbb{Z}$. $S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$, so S_3 is solvable.
$S_4 \trianglelefteq A_4 \trianglelefteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. We know $A_4/(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/3\mathbb{Z}$, and $S_4/A_4 \cong \mathbb{Z}/2\mathbb{Z}$, so S_4 is solvable.
For all n, $S_n \trianglelefteq A_n$ and $S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$. But for $n \geq 5$, A_n is simple, and so S_n is not solvable.

Group actions

Ways of making a group act on itself:

1. Conjugation: For $x \in G$, there is a map $c_x : G \to G$ defined by $c_x(y) = xyx^{-1}$.

2. G acts on subgroups which are conjugate to the subgroup H: $c_x(H) = xHx^{-1}$.

3. Left translation: Given $x \in G$, we can define $T_x \in \mathrm{Perm}(G)$. This is defined by $T_x(y) = xy$. We can define right-translation similarly.

If G acts on S, meaning we have a homomorphism $G \to \mathrm{Perm}(S)$. This is sometimes written ${}^{G} \circlearrowright S$.

Definition 0.24. Suppose $G \circlearrowright S$. Then, for $s \in S$, $Gs = \{gs \mid g \in G\}$ is the orbit containing s.
Similarly, $G_s = \{g \in G \mid gs = s\}$ is the stabilizer of s.

Claim. *G/Gs and Gs are in 1-1 correspondence.*

Proof. If $x, y \in G$, then $xG_s = yG_s$ is equivalent to $y^{-1}xG_s = G_s$, which is equivalent to $y^{-1}x \in G_s$, which is equivalent to $yxs = s$, which is equivalent to $xs = ys$, which is equivalent to x, y in the same orbit.

Example 0.9. S_3 acts on $S = \{1, 2, 3\}$.

$$G_1 = \{e, (23)\}$$
$$G/G_1 = \{eG_1, (12)G_1, (123)G_1, (132)G_1\}$$

Lecture 8

Theorem 0.7. *A_n is simple for $n \geq 5$.*

Lemma 6. *(a) A_n is generated by 3-cycles*

(b) If $n \geq 5$, all 3-cycles are conjugate in A_n

Proof. (a) We want to consider the product $[ij][rs]$. If i, j, r, s are not all distinct, then either

- $[ij][rs] = \text{Id}$ if $i = r$ or $j = s$, or vice versa
- $[ij][rs]$ is a 3-cycle
- $[ij][rs] = [isj]$

Or, $[ij][rs] = [ijr][rs]$ if they are all distinct.

(b) Let $\gamma \in S_n$. We have

$$\gamma[i_1 \cdots i_m]\gamma^{-1} = [\gamma(i_1) \cdots \gamma(i_m)]$$

Given $[ijk]$ and $[i'j'k']$, let $\gamma(i) = i'$, $\gamma(j) = j'$, and $\gamma(k) = k'$. Then $\gamma[ijk]\gamma^{-1} = [i'j'k']$. If γ is even we are done. If γ is odd, then there exist distinct r, s distinct from all of i, j, k ($n \geq 5$), then $\gamma' = \gamma[rs]$.

Proof. of theorem.
Let $N \neq \{e\}$ be a normal subgroup of A_n. Let $\sigma \in N$, $\sigma \neq e$, have the maximum number of fixed points among all such σs. So some orbit of σ has > 1 element.
Suppose all orbits of σ have 1 or 2 elements. Then there must be at least 2 orbits with two elements each. Otherwise, $\sigma = [ij] \notin A_n$
So $\{1, \dots, n\} = \mathcal{O}_1 \coprod \mathcal{O}_2 \coprod \cdots \coprod \mathcal{O}_k$.
On two such orbits, σ acts as $\sigma = [ij][rs]$ on $\{i, j, r, s\}$. Let $k \neq i, j, r, s$ (again we use the assumption $n \geq 5$). Let $\tau = [rsk]$, and $\sigma' = \tau\sigma\tau^{-1}\sigma^{-1} = [\tau, \sigma] \in A_n$. Now, $\sigma' = \tau\sigma\tau^{-1}\sigma^{-1} \in N$.

$$\begin{aligned}\sigma'(i) &= \tau\sigma\tau^{-1}\sigma^{-1}(i)\\ &= \tau\sigma\tau^{-1}(j)\\ &= \tau\sigma(j)\\ &= \tau(i)\\ &= i\end{aligned}$$

So

$$\begin{aligned}\sigma'(j) &= \tau\sigma\tau^{-1}\sigma^{-1}(j)\\ &= \tau\sigma\tau^{-1}(i)\\ &= \tau\sigma(j)\\ &= \tau(j)\\ &= j\end{aligned}$$

So if $\sigma(x) = x$, and $x \neq i, j, r, s$, then $\sigma'(x) = x$, so σ' has more fixed points than σ.
Hence, σ is an orbit with at least 3 elements, $i, j, k, \dots$.
If $\sigma \neq [ijk]$, then σ must move at least 2 other numbers r, s. Let $\tau = [krs]$, and again define $\sigma' = [\tau, \sigma] \in N$. $\sigma'(i) = i$ if $\sigma(x) = x$, but $x \in \{k, r, s\}$. Then $\sigma(x') = x'$.
So σ' again has more fixed points than σ, contradicting our assumption that $\sigma \neq [ijk]$.
Hence $[ijk] \in N$.
So all 3-cycles are in N, because $N \lhd A_n$. Because A_n is generated by 3-cycles, we must conclude $N = A_n$. ■
Enough horrible cycle garbo.

Back to group actions

Example 0.10. Let $G = \mathrm{SL}_2(\mathbb{R})$, $S = \mathscr{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$.

Define

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}$$

These are the "fractional linear transformations"
If $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$, then

$$\begin{aligned} \operatorname{Im}\left(\frac{az+b}{cz+d}\right) &= \operatorname{Im}\left(\frac{(az+b)(c\overline{z}+d)}{|cz+d|^2}\right) \\ &= \frac{1}{|cz+d|^2}\operatorname{Im}(\cdots) \end{aligned}$$

So

$$\frac{(ad-bc)\operatorname{Im}(z)}{|cz+d|^2} = \frac{\operatorname{Im}(z)}{|cz+d|^2}$$

We want $ai+b = i(ci+a) = -ci+d$.
So the stabilizer of i is $\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}) \mid \frac{ai+b}{ci+d} = i\}$.
Let $K = \{\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}\}$. G/K is in bijection with $\mathscr{H}$.

Orbits of group actions

Suppose $^G \circlearrowleft S$. Then of course $S = \coprod_{i\in I} G_{s_i}$, where we have chosen exactly one s_i from each orbit. If S is finite, then

$$|S| = \sum_{i\in I} |G_{s_i}| = \sum_{i\in I} (G : G_{s_i})$$

Definition 0.25. If G acts on itself by conjugation, $G_x = \{g \in G \mid gxg^{-1} = x\}$, and is referred to as the normalizer of x.
Then

$$(G : I) = \sum_{x\in C} (G : G_x)$$

Where C is a set of representations of conjugacy classes. This is often called the "class equation."
This can be written

$$(G : 1) = |Z| + \sum_{x\in C, x\notin Z} (G : G_x)$$

Lecture 8

Lecture 9

Direct Product

Consider the sequence of sets $\{S_i\}_{i\in I}$. Define

$$\bigtimes_{i\in I} S_i \stackrel{\text{def}}{=} \{(x_i)_{i\in I}\}$$

The direct product can be defined in general in any abelian category.

Direct Sum

Let $\{G_i\}_{i\in I}$ to be a sequence of abelian groups. Then define

$$\begin{aligned}\bigoplus_{i\in I} G_i &\stackrel{\text{def}}{=} \{(x_i)_{i\in I} \mid x_i \in G, \text{ all but finitely many } x_i = 0\} \\ &\subseteq \prod_{i\in I} G_i\end{aligned}$$

Define $\lambda_j(x) = \begin{cases} x_j & i = j \\ 0 & \text{otherwise} \end{cases}$

Proposition 5. *Let A_j, B be abelian groups. Suppose $f_j : A_j \to B$ is a group homomorphism for all j. Then there exists a unique $f : \bigoplus A_j \to B$ such that $f \circ \lambda_j = f_j$ for all j.*

Proof. Define $f((x_i)_{i\in I}) = \sum_{i\in I} f_i(x_i)$, a finite sum. Note such an f being well defined requires the hypothesis that only finitely many x_i are not the identity.

Definition 0.26. A basis for an abelian group A is a collection of elements $e_i \in A$ such that every $x \in A$ admits a unique representation in the form

$$x = \sum_i (x_i \cdot e_i)$$

where the x_i are integers. If $Z_i \cong \mathbb{Z}$, then $A \cong \oplus_{i\in I} Z_i$.
We call this the free abelian group with basis $\{e_i\}$
More generally, let S be a set. We can define $\mathbb{Z}\langle S\rangle$ as the free abelian group generated by S, defined as

$$\mathbb{Z}\langle S\rangle \stackrel{\text{def}}{=} \{\phi : S \to \mathbb{Z} \mid \phi(x) = 0 \text{ for all but finitely many } x\}$$

Lemma 7. *Let* $A \xrightarrow{f} A'$ *be a surjective homomorphism of finite abelian groups, with* A' *free, and let* $B \subseteq A$ *be a subgroup.*
Then there exists a $C \subseteq A$ *such that* $f|_C : C \to A'$ *is an isomorphism, and* $A \cong B \oplus C$.

Proof. Let $\{e_i\}_{i \in I}$ be a basis of A'. f is surjective by hypothesis, so we may choose $a_i \in A$ such that $f(a_i) = e_i$ for all i. Note $\ker f|_B = B$. The rest of the proof is in lang. lol.

Theorem 0.8. *Let* A *be a finitely generated free abelian group with* n *generated. Let* $B \lhd A$ *be any subgroup. The* B *is free with* $\leq n$ *generators.* ‘

Proof. We will prove this by induction on n.
If $n = 1$, then $A \cong \mathbb{Z}$. We know all of the subgroups of $\mathbb{Z}$: if $B \subseteq A$, then $B = N\mathbb{Z}$ is free, generated by N.
Now for the inductive step:
$f : A \to \mathbb{Z}\langle x_i \rangle$ be projection. Let B_1 be the kernel of $f|_B$. Then $B_1 \subset \mathbb{Z}\langle x_1, \ldots, x_{n-1} \rangle$ is a free group on $\leq n-1$ generators. Let $C \subset A$ be such that $C \oplus \mathbb{Z}\langle x_i, \ldots, x_n \rangle \cong \langle x_1, \ldots, x_n \rangle$. Then $B \cong (B \cap C) \oplus B_1$.
Let A be an abelian group generated by a finite set $S = \{x_1, \ldots, x_n\}$.
Define $\mathbb{Z}\langle S \rangle \xrightarrow{hom} A$ by $\phi \mapsto \sum \phi(x_i) x_i$ for $x_i \in A$.
Let $K = \ker(\mathbb{Z}\langle S \rangle \to A)$ be a subgroup of a free group on $\leq n$ generators. So it is also free on $\leq n$ generators.

Definition 0.27. Let $f : A \to B$ be a homomorphism of Abelian groups. Then define

$$\begin{aligned} \ker(f) &= \{a in A \mid f(a) = 0\} \\ \operatorname{im}(f) &= \{b \in B \mid b = f(a) \text{ for some } a \in A\} \\ \operatorname{coker}(f) &= B / \operatorname{im}(f) \end{aligned}$$

So we have $\mathbb{Z}[T] \to K$ with cokernel $\mathbb{Z}\langle S \rangle / K \cong A$.

Conclusion?

Any finitely generated abelian group is the cokernel of a homomorphism $\mathbb{Z}[T] \to \mathbb{Z}[S]$ between finitely generated free abelian groups.

Definition 0.28. (Smith normal form for integer matrices)
Let A be a $p \times n$ matrix with entries in $\mathbb{Z}$. We say A is in Smith Normal Form if there exist nonzero integers $a_1, \ldots, a_n$ such that $a_i \mid a_{i+1}$, and $a_{ij} = \begin{cases} a_i & \text{if } j = i \leq m \\ 0 & \text{if } j = i > m \\ 0 & \text{if } j \neq i \end{cases}$. In

other words, the only nonzero entries are on the diagonal, and satisfy this criterion.

Theorem 0.9. *If A is a $p \times n$ integer matrix, there exist invertible integer matrices P, Q, such that PAQ is in Smith Normal Form.*

Proof. We will use a modification of Gaussian elimination. Consider the matrix

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \end{pmatrix}$$

Normally, we would take the 2nd row minus $\frac{a_{11}}{a_{21}}$ times the first. We aren't in a field, we are in $\mathbb{Z}$, so we can't do that.

Instead, consider the 2×2 integer matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Let $e = \gcd(a, c)$. We know $e = ax + cy$, for some $x, y \in \mathbb{Z}$. Now $a = e\alpha, c = e\beta$, then $1 = \alpha x + \beta y$. Then we have the invertible matrix

$$\begin{pmatrix} x & y \\ -\beta & \alpha \end{pmatrix}$$

Multiplying this matrix by $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ yields a matrix with a 0 in the bottom left. So, on the first column, we acted by

$$\begin{pmatrix} a \\ c \end{pmatrix} \mapsto \begin{pmatrix} e \\ 0 \end{pmatrix}$$

We combine this with column operations, which will be the same as the above row operations but transposed, and we can multiply $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ by some matrix to yield a 2×2 matrix with a 0 in the upper right.

We can upscale this algorithm, and use row and column operations, and we can do the thing we said we can do. In particular, at the end a_{11} will be the gcd all matrix entries in the first row and column, etc.

■

Corollary 0.10. *Any finitely generated ableian group is isomorphic to*

$$\mathbb{Z}/a_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_m\mathbb{Z} \oplus \mathbb{Z} \underbrace{\oplus \cdots \oplus}_{t} \mathbb{Z}$$

■

Lecture 10

See handout on Gauchospace about Smith Normal Form. Sorry am bad
Apparently you can use Smith Normal Form to show that there are only 3 abelian groups of order 8...?

Groups of order pq, $p \neq q$ prime

Let G have order pq. We know it has to contain a p-Sylow subgroup and a q-Sylow subgroup, both cyclic.

Lemma 8. *If $(G : H)$ is the smallest prime dividing $|G|$, then $H \lhd G$.*

Proof. If $H = \mathbb{Z}/q\mathbb{Z} \subset G$, then $G/H \cong \mathbb{Z}/p\mathbb{Z}$.
Consider $\{x \in G \mid xH \text{ has order } p\}$. What is $o(x)$? Either p or pq. If there is an x with $o(x) = pq$, then $G \cong \mathbb{Z}/pq\mathbb{Q}$. Then we have an x with $o(x) = p$, and y with $o(y) = q$. Then $x^{-1}yx \in \langle y \rangle$. Then $x^{-1}yx = y^k$ for some k. So $x^{-p}yx^p = y^{kp}$. But x^p is the identity.
We need $kp \equiv 1 \pmod{q}$.
$\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong (\mathbb{Z}/q\mathbb{Z})^\times$ is cyclic of order $\phi(q) = q - 1$. So $q \mid (kp - 1)$, so $kp - 1 \equiv 0 \pmod{q}$, so $kp \equiv 1 \pmod{p}$
Done? Maybe?

■

The point is $\mathbb{Z}/(pq)\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$.
Let $G = \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/q\mathbb{Z}$. We're gonna do "the Smith Normal Form" thing, I guess. This group has generators $e_1 = (1, 0), e_2 = (0, 1)$. We have $pe_1 = qe_2 = e$, and $e_1e_2 = e_2e_1$. We want to do Smith Normal Form to the matrix $\begin{pmatrix} p & 0 \\ 0 & q \end{pmatrix}$. We get $\begin{pmatrix} 1 & 0 \\ 0 & pq \end{pmatrix}$. So there's only one generator...?
So we know what happens if $|G| = p$, $|G| = 4$, $|G| = pq$ with $p < q$.
What if $|G| = 8, 9, 12, 16,$, etc.?

Lemma 9. *If G is a p-group, then $G \supset \mathbb{Z}/p\mathbb{Z}$.*

■

So if $|G| = 8$, then G contains a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z}$. By the lemma we proved earlier, this subgroup has to be normal.