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

$$\prod_{i=1}^{n} x_i := (\prod_{i=1}^{n-1} x_i)x_n$$

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

$$\ker(\phi) := \{g \in G \mid \phi(g) = e\}$$

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: $(gH)(g'H) := gg'H$*

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

$$(x *_{op} y) := yx$$

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 4

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

$$(x_1, h_1)(x_2, h_2) = (x_1\psi(h_2)(x_2), h_1h_2)$$

⋮

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 orbits, like so

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