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 (1)**.** Binary Operation
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 (2)**.** Associative
A binary operation is associative if, for each $a, b, c \in S$, we have

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

Definition 0.3 (3)**.** Identity
An element $e \in S$ is an identity if $ex = xe = x$ for all $x \in S$

Definition 0.4 (4)**.** Monoid 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 (5)**.** Group
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 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 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 3

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

Example 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 5

$\mathbb{Z}$ is an additive group. $\{1, -1\}$ forms a multiplicative group.
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 0.6 (6)**.** Order
The order of G is $|G|$ if G is finite, and ∞ otherwise.

Definition 0.7 (7)**.** Roots of unity
Let $N \in \mathbb{N}$. Then the Nth roots of unity is a multiplicative subgroup of $\mathbb{C}$. It is cyclic, and generated by $e^{\frac{2\pi ik}{N}}$.
An element $e^{\frac{2\pi ik}{N}}$ 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 0.8 (8)**.** Generating Set
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 $\text{Aut}(P) = \langle \sigma, \tau, \sigma^n = \tau^2 = (\tau\sigma)^n = e \rangle$