Group Theory

Lecture 3, Sunday November 6, 2022
Ari Feiglin

Note:

I was not present at this lecture, and so this summary was written based off of someone else's who was.

3.1 Abelian and Cyclic Groups

From now on, instead of writing $a \circ b$, I will simply write ab for a group's operation.

Definition 3.1.1:

G is an **abelian group** (or G is abelian) if G is a group and for every $a, b \in G$, $ab = ba$.

Thus $\mathbb{Z}$, $\mathbb{Z}_n$, and Euler (n) are all examples of abelian groups.
We will further define exponentiation in groups. For $a \in G$, we define $a^0 = e$ (where $e \in G$ is the identity) and for $n \in \mathbb{N}$: $a^{n+1} = a^n a$. Thus $a^n = \underbrace{a \cdots a}_{n \text{ times}}$. We further define $a^{-n} = \left(a^{-1}\right)^n$. The ordinary rules for exponentiation hold here:

$$(a^n)^m = a^{nm} \qquad a^n a^m = a^{n+m}$$

Moreso, in an abelian group $(ab)^n = a^n b^n$.

Proposition 3.1.2:

Let G be a group then for every $a, b \in G$, $(ab)^2 = a^2 b^2$ if and only if G is abelian.

Proof:

If G is abelian, then this is trivial. Let's show the converse. Let $a, b \in G$ then $(ab)^2 = abab$ and so:

$$abab = a^2 b^2$$

So multiplying the left by a^{-1} and the right by b^{-1} gives

$$ba = ab$$

As required.

■

Definition 3.1.3:

The **order** of an element $a \in G$ is the minimum integer $n > 0$ such that $a^n = e$. If such a number does not exist, then the order is defined to be ∞. The order of a is denoted by $o(a)$, and sometimes $|a|$.

For example:

- $o(7) = \infty$ in $\mathbb{Z}$.
- $o(7) = 2$ in Euler (8) (since $7^2 = 49 \equiv 1 \pmod 8$)
- $o(1) = n$ in $\mathbb{Z}_n$ (since $1 + \cdots + 1 = n$)

Proposition 3.1.4:

Suppose $g \in G$ is of finite order, then $g^m = e$ if and only if $o(g) \mid m$.

Proof:

Let $o = o(g)$. Suppose $g^m = e$, then by the quotient rule $m = qo + r$ for some q and $0 \leq r < o$, then:

$$g^m = (g^o)^q g^r = e^q g^r = g^r$$

Since $0 \leq r < o$, and o is the minimum number such that $g^o = e$, this can equal e only if $r = 0$, and thus o divides m. To prove the converse, suppose $o \mid m$, so $m = qo$. And so:

$$g^m = g^{qo} = (g^o)^q = e$$

As required.

■

Definition 3.1.5:

A group G is **cyclic** (or G is a cyclic group) if there exists some $a \in G$ such that:

$$G = \left\{a^k \mid k \in \mathbb{Z}\right\}$$

a is called the **generator** of G.

For example, 1 generates $\mathbb{Z}$ and $\mathbb{Z}_n$. And a cyclic group can have multiple generators, for example 2 is another generator of $\mathbb{Z}_3$ (since $1 \equiv 2 + 2 \pmod 3$). Also notice that every cyclic group is also abelian: $a^n a^m = a^{n+m} = a^{m+n} = a^m a^n$.

Lemma 3.1.6:

If G is a cyclic group generated by g then every element in G can be written uniquely as g^k for $0 \leq k < o(g)$. Therefore $|G| = o(g)$.

Proof:

Let $o = o(g)$. Notice then that if $k \in \mathbb{Z}$ then there exists a q and $0 \leq r < o$ such that $k = qo + r$, so $g^k = g^{qo+r} = g^{qo} g^r = g^r$. So every element in G can be written as g^r for $0 \leq r < o$, and so the size of G is at most o. And if $0 \leq n \leq m < o$ such that $g^n = g^m$ then $g^{m-n} = e$ and since $m - n < o$ and o is the minimum number such that $g^o = e$, it must be that $n = m$. So every element in G has a *unique* representation as g^r, and thus G has a size of o.

■

Theorem 3.1.7:

Every cyclic group is isomorphic either to $\mathbb{Z}$ or some $\mathbb{Z}_n$.

Proof:

Suppose g generates G. If the order of g is infinite, we will show that $G \cong \mathbb{Z}$. We define an isomorphism as follows:

$$f \colon \mathbb{Z} \longrightarrow G \quad n \mapsto g^n$$

This is obviously surjective by the definition of a cyclic group. It is injective since $g^n = g^m$ if and only if $g^{n-m} = e$, which can happen only if $n = m$ since g is of infinite order. It satisfies the homomorphic property since

$$f(n + m) = g^{n+m} = g^n g^m = f(n) f(m)$$

And if g is of finite order, let $o = o(g)$, we will show that $G \cong \mathbb{Z}_o$. We define an isomorphism as follows:

$$f \colon \mathbb{Z}_o \longrightarrow G \quad [n] \mapsto g^n$$

This is well defined since if $m \in [n]$ then $m = n + qo$ so $g^m = g^{n+qo} = g^{qo} g^n = g^n$. This is surjective since we showed that every element can be written as g^n for $0 \leq n < o$, and it is injective since this representation is unique. This function is homomorphic since:

$$f([n] + [m]) = f([n + m]) = g^{n+m} = g^n g^m = f([n]) f([m])$$

■

Notice that for $g \in G$, $o(g) \leq |G|$. This is trivial for infinite Gs, otherwise then since if $n \neq m < o(g)$ then $g^n \neq g^m$ so mapping $\{0, \ldots, o(g) - 1\}$ to G by $n \mapsto g^n$ is injective and therefore $o(g) \leq |G|$.

Proposition 3.1.8:

Suppose G is a finite group, then in order for $\varnothing \neq H \subseteq G$ to be a subgroup, it is sufficient for it to be closed under multiplication.

We know that in order for H to be a subgroup, we must show that it contains e and is closed under inverses as well. What this proposition is saying is that these are implied by closure under multiplication.

Proof:

Since G is closed under multiplication $g^n \in G$ for every n. Since $o(g) \leq |G| < \infty$, $g^{o(g)} = e$, $e \in G$. And since $o(g) \geq 1$ then $g^{o(g)-1} = g^{-1} \in G$, so G is closed under inversion as well.

■

Proposition 3.1.9:

The intersection of subgroups is itself a subgroup.

Proof:

Suppose $\{H_\lambda\}_{\lambda \in \Lambda}$ are subgroups of G. Then we know that e is in every H_λ, so it is in their intersection. And if:

$$a, b \in \bigcap_{\lambda \in \Lambda} H_\lambda$$

Then $a, b \in H_\lambda$ for every $\lambda \in \Lambda$ and since H_λ is a subgroup, $ab \in H_\lambda$, so ab is in the intersection. And if a is in the intersection, it is in every H_λ so a^{-1} is in every H_λ, so it is in the intersection as well.

■

Definition 3.1.10:

Suppose G is a group and $S \subseteq G$, then we define $\langle S \rangle$ to be the smallest subgroup of G which contains S.

Since we showed the intersection of subgroups is a subgroup:

$$\langle S \rangle = \bigcap_{S \subseteq H \leq G} H$$

It is trivial to see that:

$$\langle S \rangle = \left\{ s_1^{k_1} \cdots s_n^{k_n} \;\middle|\; n \in \mathbb{N}, k_i \in \mathbb{Z} \right\}$$

Since this trivially contains S and is a subgroup. And every group containing S must contain elements of the form $s_1^{k_1} \cdots s_n^{k_n}$.
And therefore:

- If g generates the cyclic group G, $\langle g \rangle = G$ ($\langle g \rangle$ is another way of writing $\langle \{g\} \rangle$).
- $\langle 1 \rangle = \mathbb{Z}$
- $\langle 0 \rangle = \{0\} \subseteq \mathbb{Z}$
- $\langle 3 \rangle = \langle 5 \rangle = \text{Euler}(7)$

Theorem 3.1.11:

Every subgroup of a finite cyclic group is itself cyclic, and for every number which divides the size of the group, there is exactly one subgroup of that size, and these are the only subgroups it has.

Proof:

Suppose $G = \langle g \rangle$. Then notice that $\langle g^a, g^b \rangle = \langle g^{\gcd(a,b)} \rangle$. This is because since there exists α, β such that $\gcd(a, b) =$

$\alpha a + \beta b$ so:

$$g^{\gcd(a,b)} = g^{\alpha a} g^{\beta b} \in \left\langle g^a, g^b \right\rangle$$

And so $\left\langle g^{\gcd(a,b)} \right\rangle \subseteq \left\langle g^a, g^b \right\rangle$.
And $g^{\alpha a} g^{\beta b} = g^{\alpha a + \beta b}$, and since $\gcd(a,b)$ divides every linear combination of a and b, it divides this one. And so this linear combination is a multiple of $\gcd(a,b)$ and therefore this element is in $\left\langle g^{\gcd(a,b)} \right\rangle$.
And so every finitely generated subgroup of G is cyclic (we showed this where the subgroup is generated by two elements, and so this can be shown inductively), and since every subgroup can be generated (by itself) and since G is finite, this means that every subgroup is cyclic.
If $o(g) = n$, then:

$$\langle g^a \rangle = \langle g^a, e \rangle = \langle g^a, g^n \rangle = \left\langle g^{\gcd(a,n)} \right\rangle$$

And thus every subgroup of G is generated by a element g^d such that $d \mid n$, and since:

$$\left\langle g^d \right\rangle = \left\{ e, g^d, g^{2d}, \ldots, g^{n-d} \right\}$$

which has size $\frac{n}{d}$, so for every number which divides n there is a subgroup of that size. So if $\langle g^a \rangle$ and $\left\langle g^b \right\rangle$ both have the same size, then there must be a' and b' which divide n such that $\left\langle g^{a'} \right\rangle = \langle g^a \rangle$ and $\left\langle g^{b'} \right\rangle = \langle g^b \rangle$. So $\frac{n}{a'} = \frac{n}{b'}$ and therefore $a' = b'$, so these cyclic groups are the same. And so cyclic subgroups of the same size are equal.

■

Theorem 3.1.12:

Subgroups of infinite cyclic groups are also cyclic.

Proof:

We will show this for $\mathbb{Z}$, since it is isomorphic to every infinite cyclic group. Suppose H is a subgroup of $\mathbb{Z}$, then let a be the minimum positive number in H, then $\langle a \rangle \subseteq H$. Suppose $x \in H$ then $x = qa + r$ for $0 \leq r < a$. Since $\langle a \rangle \subseteq H$, $x - qa = r \in H$. If $r \neq 0$ then this contradicts the minimumness of a, so $r = 0$. And therefore $x \in \langle a \rangle$, so $H = \langle a \rangle$ and H is therefore cyclic.

■