Abstract Algebra

Week 3 Notes (a)

shaozewxy

September 2022

2.3 Cyclic Groups and Cyclic Subgroups

Definition of cyclic group

A group H is **cyclic** if H can be generated by a single element, i.e., $\exists x \in H$ such that $H = \{x^n | n \in \mathbb{Z}\}$

In this case we can write $H = \langle x \rangle$.

A cyclic group might have more than 1 generators:

Given cyclic group $H = \langle x \rangle$, then $H = \langle x^{-1} \rangle$ since $\forall x^n, x^n = (x^{-1})^{-n}$.

Examples

1. Given $G = D_{2n} = \langle r, s | r^n = s^2 = 1, rs = sr^{-1} \rangle, n \geq 3$. And let H be the subgroup of all rotations.

   Then $H = \langle r \rangle = \{1, r, r^2, ..., r^{n-1}\}, |H| = |r| = n$.

   Therefore we can write any r^t as r^k where

   $$t = nq + k \qquad\qquad 0 \leq k \leq n$$

   For example in $D_8, r^4 = 1 \to r^{105} = r, r^{-42} = r^{4(-11)+2} = r^2$.

2. Given $H = \mathbb{Z}$, then $H = \langle 1 \rangle$ with operation $+$.

Properties of cyclic groups

Composition of cyclic groups

Given $H = \langle x \rangle$, then $|H| = \langle x \rangle$ where if one side is infinite, then the other is also infinite.

1. If $|H| = n < \infty \to x^n = 1, H = \{1, x, x^2, ..., x^{n-1}\}$.

2. If $|H| = \infty \to \forall n \neq 0, x^n \neq 1$ and $\forall a \neq b \in \mathbb{Z}, x^a \neq x^b$.

Proof:

For 1, let $|x| = n$, then clearly $1, x, x^2, ..., x^{n-1}$ are distinct since if $\exists a, b < n, x^a = x^b \to x^{b-a} = 1$ contrary to the fact that n is the smallest integer such that $x^n = 1$.

Thus H has at least n elements, then only NTS $|H| = n$. Suppose $x^t \in H$ then $\exists 0 \leq k < n, x^t = x^{nq+k}$ so $x^t = x^k \in H$.

2 is trivially true.

The proof above shows how to reduce x^t into x^k where $0 \leq k < |x|$.

Cyclic groups and gcd

Given $x \in G, m, n \in \mathbb{Z}$. If $x^n = x^m = 1$, then denote $d = gcd(m, n), x^d = 1$. In particular $x^m = 1 \to |x||m$.

Proof:

By the Euclidean Algorithm, $\exists r, s$ such that $mr + ns = d$, therefore $x^d = x^{mr+ns} = 1$.

Then when $x^m = 1$, we have that $x^{|n|} = x^m = 1$, therefore $x^{(|x|,m)} = 1$, but since $|x|$ is the smallest such positive integer, $(|x|, m) = |x|$. Therefore $|x||m$.

Cyclic groups isomorphic to $\mathbb{Z}/\mathbb{Z}n$

1. Given $n \in \mathbb{Z}^+, |\langle x \rangle| = |\langle y \rangle| = n$, then the map

$$\phi : \langle x \rangle \to \langle y \rangle$$
$$x^k \to y^k$$

   is well-defined and isomorphic.

2. Given $\langle x \rangle$ is infinite, then the map

$$\phi : \mathbb{Z} \to \langle x \rangle$$
$$k \to x^k$$

   is well-defined and isomorphic

Proof:

For 1, first we NTS that the definition is well-defined:

Given $x^r = x^s$, WTS $\phi(x^r) = \phi(x^s)$:

Since $x^r = x^s \to x^{r-s} = 1 \to n|(r-s)$

Therefore $x^s = x^{nk+r}$ for some k, and therefore $\phi(x^s) = \phi(x^{nk+r}) = \phi(x^{nk}\phi(x^r)) = \phi(x^r)$.

Therefore the mapping is well-defined.

Then it is easy to prove that ϕ is a homomorphism and since $|\langle x \rangle| = |\langle y \rangle|$, we only NTS ϕ is surjective, which is also obvious since $\forall y^k, \exists x^k, \phi(x^k) = y^k$.

Therefore ϕ is an isomorphism.

For 2, first we NTS that ϕ is injective:

Given $r, s \in \mathbb{Z}$ such that $\phi(r) = \phi(s)$, we have that $x^r = \phi(r) = \phi(s) = x^s$.

Therefore since $|\langle x \rangle| = \infty, x^r = x^s \to r = s$.

Therefore ϕ is injective.

It is obvious that ϕ is surjective.

Therefore ϕ is isomorphic.

We use Z_n to denote the cyclic groups of order n.

Structure of cyclic groups

We discuss which powers of x generates $\langle x \rangle$:

Order of powers of x

Let G be a group, let $x \in G, a \in \mathbb{Z} - \{0\}$.

1. If $|x| = \infty$, then $|x^a| = \infty$.
2. If $|x| = n < \infty$, then $|x^a| = \frac{n}{(n,a)}$.
3. In particular, if $|x| = n < \infty$ and a is a positive integer dividing n, then $|x^a| = \frac{n}{a}$.

Proof:

For 1, suppose $|x^a| = k < \infty$, then $(x^a)^k = x^{ak} = 0 \to |x| < ak < \infty$. Contradiction.

For 2, we denote $|x^a| = k, (n, a) = d, n = db, a = dc$. Then we only NTS that $|x^a| = k|\frac{n}{(n,a)} = b$ and $b|k$:

Since $(x^a)^k = 0 \to n = db|ak = dck \to b|ck$.

Since $(n, a) = d \to b, c$ coprime.

Therefore $b|k$.

We also know that $(x^a)^d = x^{ad} = x^{nc} = 0 \to k|b$.

Therefore $b = k$.

For 3, this is just a special case of 2 where $(n, a) = a$.

Powers of x that generate $\langle x \rangle$

1. Given $|x| = \infty, H = \langle x^a \rangle \iff a = \pm 1$.

2. Given $|x| = n < \infty, H = \langle x \rangle \iff (a, n) = 1$.

Proof:

For 1, suppose $\langle x^a \rangle = \langle x \rangle$, then $\exists k \neq 0$ such that $(x^a)^k = x$.

Therefore $x^{ak-1} = 0 \to a = \pm 1$.

For 2, this is just using the above result.

Structure of cyclic group

Given $H = \langle x \rangle$ a cyclic group,

1. Every subgroup of H is cyclic. If $K \leq H$ then either $K = 1$ or $K = \langle x^d \rangle$ where d is the smallest positive integer such that $x^d \in K$.

2. If $|H| = \infty, \forall a \neq b \in \mathbb{Z}, \langle x^a \rangle \neq \langle x^b \rangle$. And $\forall m \in \mathbb{Z}, \langle x^m \rangle = \langle x^{|m|} \rangle$.

3. If $|H| = n < \infty$, then for each positive integer a that divides $n, \exists! K \leq H, |K| = a$. This subgroup K is defined as $\langle x^d \rangle, d = \frac{n}{a}$. Furthermore for every integer $m, \langle x^m \rangle = \langle x^{(m,n)} \rangle$, i.e. the subgroups form a bijection with the positive divisors of n.

Proof:

For 1, suppose $K \neq 1$, then $\exists x^a \in K$.

Therefore there must $\exists x^d$ where d is the smallest such positive integer.

We WTS that $K = \langle x^d \rangle$. Suppose $\exists x^a \in K, d \nmid a$, then $a = dq + r$ with $r < d, a^r \in K$, contradiction, therfore $\nexists$ such x^a.

Therefore $K = \langle x^d \rangle$.

For 2 this is obvious.

For 3, first it is obvious that $|\langle x^d \rangle| = \frac{n}{(n,d)} = a$.

Then we NTS that suppose $\exists \langle x^b \rangle$ such that $|\langle x^b \rangle| = a$, then $\langle x^b \rangle = \langle x^d \rangle$:

Since $\langle x \rangle = \{1, x^b, x^{2b}, ..., x^{(a-1)b}\}$, we know that $x^{ab} = 1 \to n | ab$.

Since $a | n, n | ab \to d | b$. Therfore $x^b \in \langle x^d \rangle$, i.e. $\langle x^b \rangle \subseteq \langle x^d \rangle$.

Since $|\langle x^b \rangle| = |\langle x^d \rangle|$ and $\langle x^b \rangle \subseteq \langle x^d \rangle \rightarrow \langle x^b \rangle = \langle x^d \rangle$.

Then the fact that $\langle x^m \rangle = \langle x^{(n,m)} \rangle$ naturally follows.