Algebra (Winter) Notes

Camila Restrepo

Last updated January 26, 2024

Note: Theorem numbers come from the order they are presented in lecture, and do not correspond to any textbook or written course material.

Week 2

Cyclic Subgroups

Definition of a cyclic group:
A group G is called **cyclic** if there is an element $a \in G$ such that $G = \left\{a^j : j \in \mathbb{Z}\right\}$. a is called a **generator** of G. We indicate that G is a cyclic group generated by a with the notation $G =< a >$.

Theorem 2.1
Suppose $a \in G$. Then $< a >$ is a subgroup of G.

Proof. Suppose $a^m, a^n \in < a >$ where $m, n \in \mathbb{Z}$. Then $a^m a^n = a^{m+n} \in < a >$ since $m + n \in \mathbb{Z}$. Also $a^{-m} \in < a >$ for all m since $-m \in \mathbb{Z}$, and $a^m a^{-m} = a^0 = e = a^0 = a^{-m} a^m$.
By the 2-step subgroup test $< a >$ is a subgroup. □

Definition of a cyclic subgroup:
The subgroup $< a >\subseteq G$ is called the **cyclic subgroup** generated by $a \in G$.

Example of generators:
Take $G = \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ together with addition mod 6.
$\mathbb{Z}_6 =< 1 >$ since $n(1) = n \mod 6$. Note that we also have $\mathbb{Z}_6 =< 5 >$.

Remark: In general, $\mathbb{Z}_n$ is cyclic and generated by $< -1 >$. All finite cyclic are isomorphic to Z_n for some n.
Remark: For $a \in G$, $< a >=< a^{-1} >$.

Example of the integers:
Take $G = \mathbb{Z}$.

$< 1 >= \{j1 : j \in \mathbb{Z}\} = \mathbb{Z}$.
$< 2 >= \{j2 : j \in \mathbb{Z}\} =$ even numbers $\subset \mathbb{Z}$.
$< m >= \{jm : j \in \mathbb{Z}\} =$ integers divisible by m for $m \neq 0$.
$< 0 >= \{0\}$.

Remark: Infinite cyclic groups are all isomorphic to $\mathbb{Z}$.

Definition of the centre of a group:
The **centre** of G is the subset

$$Z(G) = \{x \in G : xa = ax \forall a \in G\}$$

i.e., the elements that commute with everything in G.

Theorem 2.2
$Z(G)$ is a subgroup of G.

Proof. Suppose $x, y \in Z(G) and a \in G$. Then $(xy)a = x(ya) = xay = axy = a(xy)$. Therefore $xy \in Z(G)$.
Moreover, $xa = ax \implies x^{-1}xa = x^{-1}ax \implies a = x^{-1}ax \implies ax^{-1} = x^{-1}axx^{-1} \implies ax^{-1} = x^{-1}a \implies x^{-1} \in Z(G)$.
By the 2-step subgroup test, $Z(G)$ is a subgroup of G. □

Remark:

1. G is abelian $\iff Z(G) = G$
2. $Z(G)$ is abelian (even when G is not)
3. $Z(D_3) = \{e\}$ (brute force)
4. $x \in Z(G) \iff xax^{-1} = a$ for all $a \in G \iff axa^{-1} = x$ for all $a \in G$

Example of a non-trivial center:
$Z(GL(2, \mathbb{R})) = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} : a \in \mathbb{R}^{\times} \right\}$

Definition of the centralizer:
Fix $b \in G$. The **centralizer** of b in G is

$$\begin{aligned} C_G(b) = C(b) &= \{a \in G : ab = ba\} \\ &= \left\{a \in G : aba^{-1} = b\right\} \end{aligned}$$

Theorem 2.3
For any $b \in G$, $C_G(b)$ is a subgroup.

Proof. Subgroup test. $\square$

Remark:

1. $C_G(e) = G$
2. $C_G(b) = G \iff b \in Z(G)$
3. $e \in C_G(b)$, $< b > \subseteq C_G(b)$

Example of a centralizer:
$C_{GL(2,\mathbb{R})}\left(\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\right) = \left\{\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} : a, b \in \mathbb{R}^{\times}\right\}$

Recall: G is cyclic if $G =< a >= \left\{a^j : j \in \mathbb{Z}\right\}$ for some $a \in G$.

Theorem 2.4
Suppose $a \in G$. Then

1. If $|a| = \infty$, then $a^k = a^j \iff j = k$
2. If $|a| = n$, then $a^k = a^j \iff n$ divides $k - j$

Proof.

1. Suppose $|a| = \infty$. This means $a^n \neq e$ for any $n \geq 1$. Suppose now $a^k = a^j$ with $k \geq j$. Then $a^k a^{-j} = aja^{-j} = e \implies a^{k-j}$ for $k - j \geq 0$. Since $a^n \neq e \forall n \geq 1$, we have $k - j = 0 \implies k = j$.
2. Suppose $|a| = n$. This means $a^n = e$ and n is the least positive number satisfying this equation. Suppose $a^k = a^j$ with $k \geq j$. Then $a^{k-j} = e$ where $k - j \geq 0$. By definition of n, $n \leq k - j$. By the division algorithm, $k - j = qn + r$ where $q, r \in \mathbb{Z}$ are unique and $0 \leq r \leq n - 1$.
   $e = a^{k-j} = a^{qn+r} = a^{qn}a^r = (a^n)^q a^r = e^q a^r = ea^r = a^r$, so $r = 0$ by the minimality of n, and so $k - j = qn \implies \frac{k-j}{n} = q \in Z \implies n$ divides $k - j$.
   Conversely if $qn = k - j$, then $a^{k-j} = (a^n)^q = e^q = e \implies a^k = a^j$.

$\square$

Remark: In part 2., n divides $k - j \iff (k - j) \mod n = 0 \iff k \mod n = j \mod n$

Corollary 2.5
Suppose $|a|\, n$. Then $a^k = e$ for some $k \in \mathbb{Z} \iff$ k is a multiple of $|a|$

Proof. Suppose $a^k = e$. Then $a^k = a^0$, so n divides $k - 0 = k$. $\square$

Corollary 2.6
Suppose $a \in G$. Then

1. If $|a| = n$ then $< a >= \left\{e, a^1, a^2, \ldots, a^{n-1}\right\}$ and $|< a >| = |a|$.
2. If $|a| = \infty$, then $< a >$ is infinite and $|< a >| = |a| = \infty$

Proof. Didn't take notes for this one. $\square$

Corollary 2.7
Suppose G is a finite group and $a, b \in G$. Then

1. $|a|\,, |b|$ are finite
2. If $ab = ba$ then $|ab|$ divides $|a|\,|b|$

Proof.
1. Suppose by way of contradiction that $|a|$ is infinite. Then $< a > \subseteq G$ is infinite. But G is finite so $|< a >| \leq |G|$ is a contradiction.
2. $(ab)^{|a||b|} = a^{|a||b|}b^{|a||b|} = (a^{|a|})^{|b|}(b^{|b|})^{|a|} = e^{|b|}e^{|a|} = e$

$\square$

2 examples omitted. Sorry, I'm prepping for my tutorial later!

Theorem 2.8
Suppose $a \in G$ and $|a| = n$. Then for any $k \geq 1$, $< a^k >=< a^{\gcd(n,k)} >$ and $\left|a^k\right| = \frac{n}{\gcd(n,k)}$

Theorem 2.9 Fundamental Theorem of Cyclic Groups
Suppose $G =< a >$ is cyclic and $|G| = n$. Then

1. Every subgroup of H is cyclic and $k = |H|$ divides $n = |G|$, i.e., k is a divisor of n
2. For every divisor k of n, there is a unique subgroup of G of order k and it is equal to $< a^{\frac{n}{k}} >$

Proof. 1. Suppose H is a subgroup of G and $H \neq < e >$. Let $m \geq 1$ be the least power of a such that $a^m \in H$. Since H is closed under multiplication and inversion, $< a^m > \subseteq H$. Suppose $a^j \in H$. By the division algorithm, $j = qm + r$ with $0 \leq r \leq m \implies a^j = (a^m)^q a^r \implies a^j (a^m)^{-q} = a^r$, so since $a^j, (a^m)^{-q} \in H$, $a^r \in H \implies r = 0$ by the minimality of m.

2. Suppose k divides n, i.e. $\frac{n}{k}$ is an integer. Recall that $\left|< a^{\frac{n}{k}} >\right| = \left|a^{\frac{n}{k}}\right| = k$. It follows that $\left|< a^{\frac{n}{k}} >\right| = k$.

   Suppose $H \subseteq < a >$ is a subgroup and $|H| = k$. By part 1, $H = a^m$ for some $m \geq 1$. By Theorem 2.8, $k = |H| = |< a^m >| = |a^m| = \frac{n}{\gcd(m,n)} \implies \gcd(m, n) = \frac{n}{k}$.

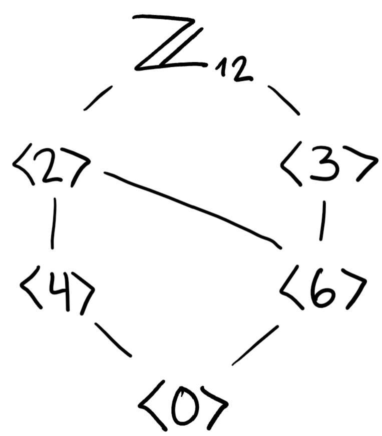
   By Theorem 2.8 again, $H =< a^m >=< a^{\gcd(m,n)} >=< a^{\frac{n}{k}} >$.

∎

Example of the subgroups of $\mathbb{Z}_{12}$:
The divisors of $n = 12$ are $1, 2, 3, 4, 6, 12$

- $k = 1$: $< 0 >$
- $k = 2$: $< 6 >= \{0, 6\}$
- $k = 3$: $< 4 >= \{0, 4, 8\}$
- $k = 4$: $< 3 >= \{0, 3, 6, 9\}$
- $k = 6$: $< 2 >= \{0, 2, 4, 6, 8, 10\}$
- $k = 12$: $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

Note: The lattice of subgroups of $\mathbb{Z}_{12}$ illustrates the containment relationships.



Remark: In $\mathbb{Z}_n$, clearly $< m > \subseteq < k > \iff m \in < k > \iff ka = m \iff$ k divides m.

Example of subgroups of $\mathbb{Z}_p$:
Consider $\mathbb{Z}_p$ where p is prime. The only subgroup of $\mathbb{Z}_p$ is $< 0 >$.