MAT301H1S Lec5101 Burbulla

Week 3 Lecture Notes

Winter 2020

Chapter 4: Cyclic Groups

What Is A Cyclic Group?

Definition: a group $(G, \cdot)$ is called **cyclic** if there is an element $a \in G$ such that

$$G = \{a^n \mid n \in \mathbb{Z}\} = \{\ldots, a^{-2}, a^{-1}, a^0 = e, a, a^2, \ldots\}.$$

For a group $(G, +)$ with additive notation this looks like

$$G = \{n \cdot a \mid n \in \mathbb{Z}\} = \{\ldots, -2a, -a, 0, a, 2a, \ldots\}.$$

Such an element is called a **generator** of G, and we write $G = \langle a \rangle$.

Examples:

1. $\mathbb{Z} = \langle 1 \rangle$ or $\langle -1 \rangle$
2. In $\mathbb{Z}_8 : \langle 3 \rangle = \{0, 3, 6, 9, 12, 15, 18, 21, \ldots\} = \{0, 3, 6, 1, 4, 7, 2, 5\} = Z_8$, so $\mathbb{Z}_8 = \langle 3 \rangle$. But $\langle 2 \rangle = \{0, 2, 4, 6\} \neq \mathbb{Z}_8$.
3. $U(8) = \{1, 3, 5, 7\}$ is not cyclic since $\langle 1 \rangle = \{1\}, \langle 3 \rangle = \{1, 3\}, \langle 5 \rangle = \{1, 5\}$ and $\langle 7 \rangle = \{1, 7\}$.

Theorem 4.1: Criterion for $a^i = a^j$

Let $G = \langle a \rangle$ be a cyclic group. For which values of i and j does $a^i = a^j$? The answer depends on whether G is finite or infinite:

1. If $a^n \neq e$ for $n \neq 0$, then $G = \langle a \rangle$ is an infinite cyclic group and $a^i = a^j \Leftrightarrow a^{i-j} = e = a^0 \Leftrightarrow i - j = 0 \Leftrightarrow i = j$.
2. If G is finite and $|a| = n$, then $a^i = a^j \Leftrightarrow i \equiv j \pmod{n}$.
   Proof: assume $i \geq j$. Since $a^{i-j} = e$ and $|a| = n$, by definition of order, $n \leq i - j$. By the division algorithm, $i - j = qn + r$, for some positive q and some r with $0 \leq r \leq n - 1$. Then $e = a^{i-j} = a^{qn+r} = (a^n)^q\, a^r = e\, a^r = a^r$, implying $r = 0$, since $r < n$. Thus n divides $i - j$; or in modular arithmetic:

   $$i \equiv j \pmod{n}.$$

   As a corollary, $|G| = |\langle a \rangle| = |a|$, and $a^k = e \Rightarrow |a| \mid k$.

The Order of ab if $ab = ba$

Theorem: suppose a and b are any two elements in a group G such that $ab = ba$. Then $|ab| \mid |a||b|$, that is, $|ab|$ divides $|a||b|$.

Proof: let $|a| = m, |b| = n$. In the cyclic subgroup $\langle ab \rangle$ of G, we have

$$\begin{aligned}
(ab)^{mn} &= \underbrace{ab \cdot ab \cdot \cdots \cdot ab}_{mn\ times} \\
(\text{since } ab = ba) &= \underbrace{a \cdot a \cdot \cdots \cdot a}_{mn\ times} \cdot \underbrace{b \cdot b \cdot \cdots \cdot b}_{mn\ times} \\
&= a^{mn}\ b^{mn} \\
&= (a^m)^n\ (b^n)^m \\
&= e^n e^m = e,
\end{aligned}$$

so by the previous slide, $|ab|$ must divide $mn = |a||b|$.

Example 1

In $U(42) = \{1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41\}$, check that $|25| = 3, |13| = 2$. Thus $|25 \cdot 13|$ must be 1, 2, 3 or 6. In fact, $25 \cdot 13 = 325 \equiv 31 \pmod{42}$, and $|31| = 6$, as you can check. Similarly, $|25 \cdot 25|$ must divide 3^2 so it must be 1, 3 or 9. In fact, $25^2 = 625 \equiv 37 \ (\text{mod} 42)$ and $|37| = 3$, as you can check.

In D_6 : every reflection has order 2, and the product of any two reflections is a rotation. So if a product of reflections does not have order 1, 2 or 4, then the reflections do not commute. For example:

$$[F_{180}][F_{60}] = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 & \sqrt{3} \\ \sqrt{3} & -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} -1 & -\sqrt{3} \\ \sqrt{3} & -1 \end{bmatrix} = [R_{240}],$$

which has oder 3. Thus F_{180} and F_{60} cannot commute: in fact, $[F_{60}][F_{180}] = [R_{120}] \neq [R_{240}]$.

Example 2

Suppose $|a| = 12$ and

$$G = \langle a \rangle = \{1, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, a^{10}, a^{11}\}.$$

What is the order of each element in G? Since $|\langle a^k \rangle| = |a^k|$, you can approach this question two different ways. For example

1. $\langle a^9 \rangle = \{a^9, a^{18} = a^6, a^{27} = a^3, a^{36} = 1\}$, so $|a^9| = |\langle a^9 \rangle| = 4$.
2. If $m = |a^9|$, then m is the *least* positive integer such that

$$(a^9)^m = 1 \Rightarrow a^{9m} = 1 \Rightarrow 12 \mid 9m \Rightarrow m = 4.$$

The complete list of orders of the elements in G is:
$|a| = 12, |a^2| = 6, |a^3| = 4, |a^4| = 3, |a^5| = 12, |a^6| = 2, |a^7| = 12,$
$|a^8| = 3, |a^9| = 4, |a^{10}| = 6$, and $|a^{11}| = 12$.

Theorem 4.2

The results of the previous example can be generalized to:
Theorem: let $|a| = n$, let k be a positive integer. Then

$$|a^k| = \frac{n}{\gcd(n,k)} \text{ and } \langle a^k \rangle = \left\langle a^{\gcd(n,k)} \right\rangle.$$

Proof: see book.

Example 2, continued: with $G = \langle a \rangle$ and $|a| = 12$,

$$\langle a^5 \rangle = \langle a^7 \rangle = \langle a^{11} \rangle = \langle a \rangle = G;$$
$$\langle a^{10} \rangle = \langle a^2 \rangle;$$
$$\langle a^9 \rangle = \langle a^3 \rangle;$$
$$\langle a^8 \rangle = \langle a^4 \rangle.$$

The two remaining subgroups are $\langle 1 \rangle = \{1\}$, and $\langle a^6 \rangle = \{1, a^6\}$.

Corollaries of Theorem 4.2

1. In a finite cyclic group, the order of an element divides the order of the group.
2. If $|a| = n$, then $\langle a^i \rangle = \langle a^j \rangle$ if and only if $\gcd(n, i) = \gcd(n, j)$, and $|a^i| = |a^j|$ if and only if $\gcd(n, i) = \gcd(n, j)$.
3. $\langle a \rangle = \langle a^j \rangle$ if and only if $\gcd(n, j) = 1$, and $|a| = |a^j|$ if and only if $\gcd(n, j) = 1$.
4. $\mathbb{Z}_n = \langle k \rangle$ if and only if $\gcd(n, k) = 1$. That is, the complete list of generators of $\mathbb{Z}_n$ is $U(n) = \{k \in \mathbb{Z}_n \mid \gcd(n, k) = 1\}$.

Example 3

1. In $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ the complete list of generators is $U(12) = \{1, 5, 7, 11\}$. So for example,

$$\begin{aligned} \langle 5 \rangle &= \{0, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55\} \\ &= \{0, 5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7\}. \end{aligned}$$

2. Consider $U(50)$: its order is $\phi(50) = 20$, and it elements are $\{1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39, 41, 43, 47, 49\}$. Given that $U(50) = \langle 3 \rangle$, (check this!) find all generators of $U(50)$.

Solution: $\langle 3^k \rangle = \langle 3 \rangle \Leftrightarrow \gcd(20, k) = 1 \Leftrightarrow k \in U(20)$. Since $U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$, the generators of $U(50)$ are

$$\{3, 3^3, 3^7, 3^9, 3^{11}, 3^{13}, 3^{17}, 3^{19}\} \text{ or } \{3, 27, 37, 33, 47, 23, 13, 17\}.$$

The Fundamental Theorem of Cyclic Groups

Theorem 4.3: let $G = \langle a \rangle$ be a cyclic group with order n. Then:

1. every subgroup of G is cyclic.
2. if $H \leq G$ then $|H|$ is a divisor of n.
3. for each divisor k of n, G has exactly one subgroup of order k, namely $\langle a^{n/k} \rangle$, generated by $\left(a^{n/k}\right)^j$ such that $j \in U(k)$.

Proof: see the book. It's not difficult, just tedious.

From Example 2: the only subgroups of $G = \langle a \rangle$ with $|a| = 12$ have orders 1, 2, 3, 4, 6 or 12, and are, respectively,

$$\langle a^{12/1} \rangle = \langle a^{12} \rangle = \{1\}, \langle a^{12/2} \rangle = \langle a^6 \rangle = \{1, \mathbf{a^6}\},$$
$$\langle a^{12/3} \rangle = \langle a^4 \rangle = \{1, \mathbf{a^4}, \mathbf{a^8}\}, \langle a^{12/4} \rangle = \langle a^3 \rangle = \{1, \mathbf{a^3}, a^6, \mathbf{a^9}\},$$
$$\langle a^{12/6} \rangle = \langle a^2 \rangle = \{1, \mathbf{a^2}, a^4, a^6, a^8, \mathbf{a^{10}}\},$$
$$\langle a^{12/12} \rangle = \langle a \rangle = \{1, \mathbf{a}, a^2, a^3, a^4, \mathbf{a^5}, a^6, \mathbf{a^7}, a^8, a^9, a^{10}, \mathbf{a^{11}}\}.$$

Example 4: All The Subgroups of $\mathbb{Z}_{42} = \langle 1 \rangle$

k	$42/k$	subgroup of order k, $\langle (42/k) \cdot 1 \rangle$, with $k \mid 42$
1	42	$\langle 42 \rangle = \{0\}$
2	21	$\langle 21 \rangle = \{0, \mathbf{21}\}$
3	14	$\langle 14 \rangle = \{0, \mathbf{14}, \mathbf{28}\}$
6	7	$\langle 7 \rangle = \{0, \mathbf{7}, 14, 21, 28, \mathbf{35}\}$
7	6	$\langle 6 \rangle = \{0, \mathbf{6}, \mathbf{12}, \mathbf{18}, \mathbf{24}, \mathbf{30}, \mathbf{36}\}$
14	3	$\langle 3 \rangle = \{0, \mathbf{3}, 6, \mathbf{9}, 12, \mathbf{15}, 18, 21, 24, \mathbf{27}, 30, \mathbf{33}, 36, \mathbf{39}\}$
21	2	$\langle 2 \rangle$ is set of all even numbers in $\mathbb{Z}_{42}$
42	1	$\langle 1 \rangle = \mathbb{Z}_{42}$

Note: the entries in boldface, in the above table and in the previous slide, are generators for the given subgroups.

Theorem 4.4

Theorem: if G is a cyclic group of order n and d is a positive divisor of n, then the number of elements of order d in G is $\phi(d)$.

Proof: suppose $d \mid n$. Then the number of elements of order d in $G = \langle a \rangle$ are all the generators of the subgroup $\langle a^{n/d} \rangle$ of order d. The number of generators of $\langle a^{n/d} \rangle$ is given by Theorem 4.3.3: namely $|U(d)| = \phi(d)$.

Example 4, Continued: the number of elements of order 2 in $\mathbb{Z}_{42}$ is $\phi(2) = 1$; the number of elements in $\mathbb{Z}_{42}$ with order 3 is $\phi(3) = 2$; the number of element in $\mathbb{Z}_{42}$ with order 6 is $\phi(6) = 2$; the number of elements in $\mathbb{Z}_{42}$ with order 7 is $\phi(7) = 6$; the number of elements in $\mathbb{Z}_{42}$ with order 14 is $\phi(14) = 6$; the number of elements in $\mathbb{Z}_{42}$ with order 21 is $\phi(21) = 12$; and the number of elements in $\mathbb{Z}_{42}$ with order 42 is $\phi(42) = 12$. (Total: 41.)

Example 5

In D_8 consider the cyclic subgroup of rotations

$$C_8 = \langle R \rangle = \{1, R, R^2, R^3, R^4, R^5, R^6, R^7\},$$

with $R = R_{\pi/4}$.
It has $\phi(2) = 1$ element of oder 2, namely $R^4 = R_\pi$;
it has $\phi(4) = 2$ elements of order 4, namely $R^2 = R_{\pi/2}$ and $R^6 = R_{3\pi/2}$;
and it has $\phi(8) = 4$ elements of order 8, namely $R = R_{\pi/4}$, $R^3 = R_{3\pi/4}$, $R^5 = R_{5\pi/4}$, and $R^7 = R_{7\pi/4}$.

How Many Elements of Order d Are In a Group G?

If G is cyclic, the answer is: $\phi(d)$. But what if G is an arbitrary finite group? The best we can say is that the number of elements of order d in G is a *multiple* of $\phi(d)$.

Proof: if G has no elements of order d then the theorem is trivially true, since 0 is a multiple of $\phi(d)$; $0 = 0 \cdot \phi(d)$.

If a is one element of order d in G, then the subgroup of G generated by a, $\langle a \rangle$, contains $\phi(d)$ elements of order d. If there are no other elements of order d in G, we are done. If b is another element of order d in G but $b \notin \langle a \rangle$, then $\langle b \rangle$ also contains $\phi(d)$ elements of order d. This gives $2 \cdot \phi(d)$ elements of order d ...unless there is one element of order d that is common to both $\langle a \rangle$ and $\langle b \rangle$. But if c has order d and $c \in \langle a \rangle \cap \langle b \rangle$ then $\langle a \rangle = \langle c \rangle$ and $\langle b \rangle = \langle c \rangle$. Thus $\langle a \rangle = \langle b \rangle$, contradicting our assumption that b is *not* in $\langle a \rangle$. And so on ....

Subgroup Lattices

In the following diagram all the subgroups of $\mathbb{Z}_{42}$ are displayed in a lattice: the order of the subgroups increases, bottom to top; the lines join a group H to a group K if $H < K$. (Ref. Example 4)