Midterms will be returned in class on Friday. Problem set 4 (long) is on web, due February 13 (Monday)

Previously in Math 103a:

Subgroups!

2-step subgroup test. G group

nonempty subset $H \subset G$ is a subgroup of G if

Inverses: $a \in H \Rightarrow a^{-1} \in H$, and

Products: $a, b \in H \Rightarrow ab \in H$.

In today's episode we'll study cyclic groups & their subgroups.

Cyclic groups

Recall: a group G is cyclic if $\exists a \in G$ s.t. $G = \{a^n : n \in \mathbb{Z}\} = \langle a \rangle$.

Def: if $\langle a \rangle = G$, then a is called a generator of G. Generators are not unique.

Ex 1. $\mathbb{Z}$ is cyclic: take $a = 1$ or -1

Recall that 1^n means $\underbrace{1+1+\cdots+1}_{n}$

Ex 2. $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ (addition mod n) is cyclic with $a = 1$ or $a = n-1$, usually other generators exist.

e.g. $n = 4$ $\quad G = \{0, 1, 2, 3\}$

$a = 1$ ✓ $\quad \langle 1 \rangle = \langle 1, 2, 3, 0 \rangle$

since $(1+1+1+1) \bmod 4 = 0$

$a = 2$ ✗ $\quad \langle 2 \rangle = \langle 2, 0 \rangle$ $\quad 2+2 \bmod 4 = 0$

$a = 3$ ✓ $\quad (3+3) \bmod 4 = 2$

$(3+3+3) \bmod 4 = 1$

$(3+3+3+3) \bmod 4 = 0$

$\therefore \langle 3 \rangle = \{3, 2, 1, 0\} = \mathbb{Z}_4$.

$\langle 0 \rangle = \{0\}$ trivial subgroup

generators of $\mathbb{Z}_4$ are $1 \& 3$

Ex 3. $U(n)$ This is tricky, Sometimes cyclic, sometimes not

e.g. $U(9) = \{1, 2, 4, 5, 7, 8\}$ cyclic

$\langle 2 \rangle = U(9)$ $\{2, 4, 8, 7, 5, 1\}$

2^1 2^2 2^3 2^4 2^5 2^6

Claim $U(8) = \{1, 3, 5, 7\}$ is not cyclic!

Easy to check:

$\langle 1 \rangle = \{1\}$

$\langle 3 \rangle = \{3, 1\}$ $3^2 = 9$

$\langle 5 \rangle = \{5, 1\}$ $5^2 = 25$

$\langle 7 \rangle = \{7, 1\}$ $7^2 = 49$

$|1| = 1$, $|a| = 2$ $a \neq 1$. No generator.

what happened is that $3^0 = 3^2$ in $U(8)$

$= 3^4$

same for 5 & 7

$5^2 = 1 = 5^0$ in $U(8)$

Q: For $a \in G$, when does $a^i = a^j$

Thm. (Criterion for $a^i = a^j$) $a \in G$ group.

(1) If $|a| = \infty$, then $a^i \neq a^j$ for $i \neq j$

(2) If $|a| = n < \infty$, then $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ and $a^i = a^j \iff n \mid i-j$.

Pf. In either case, note that

$$a^i = a^j \iff a^{i-j} = e$$

WLOG assume $i \geq j$

(1) Assume $|a| = \infty$. If $a^{i-j} = e$, $i-j \geq 0$, then $i-j = 0$. (Why?) This proves (1).

(2) Assume $|a| = n$ and $a^{i-j} = e$.

If $i-j \neq 0$, then $i-j \geq n$, so $a^i \neq a^j$ for both i, j between 0 & $n-1$

i.e. $|\{e, a, a^2, \ldots, a^{n-1}\}| = n$

(all powers are different)

$\therefore \{e, a, a^2, \ldots, a^{n-1}\} \subset \langle a \rangle$ & $|\langle a \rangle| \geq n$

If $k \geq n$, use division algorithm to check higher powers of a

(*) $k = qn + r \quad 0 \le r < n$

Then $a^k = (a^n)^q a^r = e\, a^r = a^r$

$\therefore\ a^k \in \{e, a, a^2, \ldots, a^{n-1}\}$

$\therefore\ \langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$

In particular

$$|\langle a \rangle| = |a| = n$$

Finally, if $a^{i-j} = e$, $i - j \ge n$, then let $h = i - j$, and use (*)

$e = a^h = (a^n)^q a^r = a^r$. Since $r < n$ must have $r = 0$.

$\therefore\ i - j = qn$, which means

$n \mid i - j$. //

Cor 1 $|\langle a \rangle| = |a| \quad \forall\ a \in G$.

Cor 2. $a^n = e \Longrightarrow k = 0$ or $n \mid k$

Note that $\langle a \rangle$ is abelian, so operation in $\langle a \rangle$ can be viewed as addition.

Q: What are other generators for $\langle a^k \rangle$? what is smallest possible power of a?

Check some examples.

Suppose $|a| = 30 = 2 \times 3 \times 5$. What is $\langle a^7 \rangle$?

$\gcd(7, 30) = 1$ so $\exists\ s, t$ s.t.

$$7s + 30t = 1$$

$$(a^7)^s (a^{30})^t = a^1 = a$$

$$\therefore\ a^{7s} = a$$

Since $\langle a^7 \rangle \subset \langle a \rangle = \langle a^{7s} \rangle \subset \langle a^7 \rangle$

$$\therefore\ \langle a^7 \rangle = \langle a \rangle = \{e, a, a^2, \ldots, a^{29}\}$$

This works because $\gcd(7, 30) = 1$

Similarly, $\langle a^{26} \rangle = \langle a^2 \rangle$

$\gcd(30, 26) = 2$ so $\exists\ s, t$ $26s + 30t = 2$

$$\Longrightarrow (a^{26})^s = a^2$$

General case:

Thm. If $|a| = n$, $k > 0$, then

(1) $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$

(2) $|a^k| = n / \gcd(n, k)$.

Cor 1 $|a^k| \mid n$

Cor 2. $|a^i| = |a^j| \iff \langle a^i \rangle = \langle a^j \rangle \iff$

$\gcd(i,n) = \gcd(j,n)$

Pf of Thm. Division algorithm

$k = qn + d$ $\quad d = \gcd(n,k)$

$\therefore a^k = a^d$ $\quad 0 \le d < n$

$\Rightarrow \langle a^k \rangle = \langle a^d \rangle$

and $|a^k| = |a^d|$ This proves (1).

For (2), $(a^d)^{n/d} = a^n = e$

so $|a^d| \le n/d$.

If $0 < i < n/d$, then

$(a^d)^i = a^{di} \neq e$, since $di < n$

$\therefore |a^d| \ge n/d$.

It follows that $|a^d| = n/d$, which proves (2). //

Observation: all cyclic groups G with $|G| = n$ "look alike."

Reason: Suppose $\langle a \rangle = G$. Then

$G = \{e, a, a^2, \ldots, a^{n-1}\}$

and Cayley table is determined!