Lecture 4

SOME RECAPS OF NOTATIONS

Additive notation for abelian groups

Sometimes, if G is an abelian group, we write for $a, b \in G$ $a+b$ instead of $a \cdot b$

Example: $\mathbb{Z}$, $\mathbb{Z}_n$, $\mathbb{R}$

Additive	Multiplicative
$a+b$	ab
na	a^n
$-a$	a^{-1}
0	e

In general groups, we write a^n to mean if $n>0$, then $a^n = \underbrace{a \cdots a}_{n \text{ times}}$

$n=0$, then $a^0 = e$

$n<0$, then $a^n = \underbrace{a^{-1} \cdots a^{-1}}_{n \text{ times}}$

So if $a \in G$, then $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$

In additive notation, we won't write a^n instead, we write na

So if $n>0$, $na = \underbrace{a+a+\cdots+a}_{n \text{ times}}$

if $n=0$, then $0 \cdot a =$ identity of the group $= 0 = e$

if $n<0$, then $na = a^{-1}+a^{-1}+\cdots+a^{-1} = \underbrace{(-a)+\cdots+(-a)}_{n \text{ times}}$

Add

$na+ma=(n+m)a$

$d(na)=(nd)a$

Mult.

$a^n a^m = a^{n+m}$

$(a^n)^d = a^{nd}$

addition

multiplication – shorthand for repeated addition

multiplication

exponentiation – short hand for repeated multiplication

Why Cyclic groups?

① Cyclic groups are the 'simplest' groups. Generated by 1 element. Cyclic groups are always abelian.

② Cyclic groups will form the simplest subgroups.

Let G be a group, and let $a \in G$. Then the smallest subgroup of G containing a is $\langle a \rangle$.

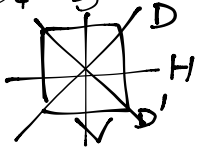
That is, if $H \leq G$, and $a \in H$, then $\langle a \rangle \leq H$.

Pf: Sps $a \in G$, and $H \leq G$, s.t. $a \in H$.

Then $a^{-1} \in H$ b/c H is a subgroup. Also, $e \in H$.

So $\{a^n \mid n \in \mathbb{Z}\} \leq H$ ∎

D_4 = symmetries of a square $= \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$



NOT a cyclic group.

Fact: Cyclic groups are abelian.

Pf: Let $G=\langle a\rangle$ be a cyclic group generated by $a\in G$. Then all elements of G are of the form a^n for some n. And the elements clearly commute.

Cyclic subgroup of D_4

$\langle R_0\rangle = \{R_0\}$

$\{R_0, R_{90}, R_{180}, R_{270}\} \leq G$

$\langle R_{90}\rangle = \langle R_{270}\rangle$

$\langle R_{180}\rangle = \{R_0, R_{180}\}$

$\langle D\rangle = \{R_0, D\}$

$\langle D'\rangle = \{R_0, D'\}$

$\langle V\rangle = \{R_0, V\}$

$\langle H\rangle = \{R_0, H\}$

Thm: Sps $a\in G$, and a has finite order, then $|a| = |\langle a\rangle|$.

$U(8)$ is not cyclic but it is abelian

$U(8) = \{k\in \mathbb{Z}_8 \mid \gcd(k,8)=1\} = \{1,3,5,7\}$

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

$\langle 3\rangle = \{3, 1\}$

$\langle 5\rangle = \{1, 5\}$

$\langle 7\rangle = \{1, 7\}$

What're the cyclic subgroups of $\mathbb{Z}_8 = \{0,1,2,3,4,5,6,7\} \bmod 8$.

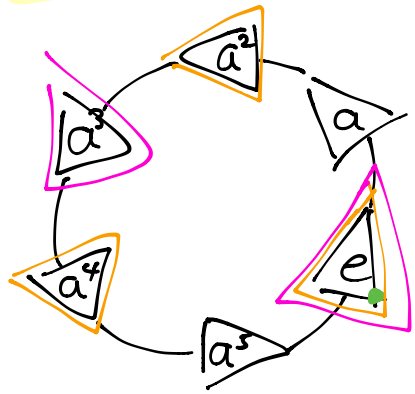
$\langle 0\rangle = \{0\}$

$\langle 1\rangle = \{1^n\} = \{n\cdot 1\} = \{0,1,\cdots,7\}$

$\langle 2\rangle = \{2^n\} = \{n\cdot 2\} = \{0,2,4,6\}$

$\langle 5\rangle = \{n\cdot 5\} = \{0,1,\cdots,7\}$ b/c $\gcd(5,8)=1$ *

Graph of a Cyclic Group



All symmetries are of the form "shift k beads counterclockwise"

Let a = shift 1 bead counterclockwise

What is $|a|$?

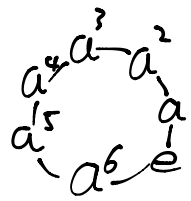
Let G = the group symmetries of this necklace. Then $G=\langle a\rangle$. G is a cyclic group of order 6.

$G=\langle a\rangle$
But $\langle a^2\rangle \neq G$
$|\langle a^3\rangle| = 8$ $\langle a^2\rangle$ is also cyclic
$|\langle a^3\rangle| = 2$, $\langle a^4\rangle = \langle a^2\rangle$

Thm: Sps $G=\langle a\rangle$, and $|\langle a\rangle| = n$.
Then $\langle a^k\rangle = \langle a^d\rangle$, where $d = \gcd(k,n)$
Moreover, every subgroups of this form is

Note: $6 = 2\cdot 3$
divisors of 6: 1, 2, 3, 6

Thm: Let $G=\langle a\rangle$, & sps $|\langle a\rangle| = n$. Then for each k/n, $\exists$ exactly one subgroup of order k, namely $\langle a^{n/k}\rangle$

Now 

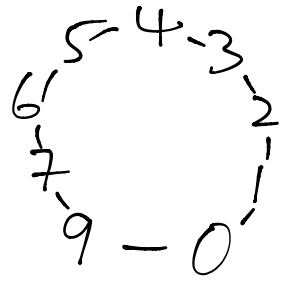
a = shift 1 cclkw
Let H = symmetries of this necklace

The generators of H are: a, a^3, a^5, a^7

What are the generators of $\langle a^2\rangle$?
all elements a^k where $\gcd(k,8) = \gcd(2,8)$
• Generators of $\langle a^2\rangle$ are a^2 & a^6.

What are the generators of a^4? Only a^4 as $\gcd(4,8) = \gcd(4,8) = 4$

Now for Z_{10}

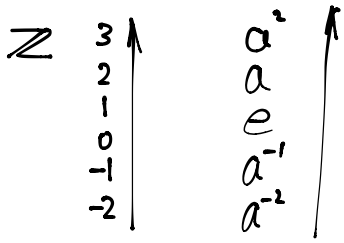


$= "1^{2}"$

generator: 1

0–3–6–9–2–5–8–1–4–7
0–4–8–2–6

Let G = symmetries of this infinitely long necklace.
Let a = shift up by 1 bead



Thm (0.2)
$\forall a,b \in \mathbb{Z}, a,b \neq 0, \exists s,t \in \mathbb{Z}$ s.t. $\gcd(a,b) = as+bt$
Moreover, $\gcd(a,b)$ is the smallest positive integer of the form $as+bt$.

Pf: Let $S = \{am+bn \mid m,n \in \mathbb{Z},\ am+bn > 0\}$
Clearly $S \neq 0$ (For example $a \cdot a + b \cdot b \in S$
Let d = the least element of S.

First, we'll see that $d \mid a$.
To see this, we write $a = dq + r$ where $0 \leq r < r$

want to show $r = 0$
Sps $r \neq 0$, then $r = a - dq = a - (as+bt)q$ for some s,t.
$= a(1-sq) + b(-qt)$
So $r \in S$, but $r < d$, which is a contradiction.
So $r = 0$, thus $d \mid a$.

In fact, we see similarly, that $d \mid b$. So d is a common divisor of a & b.
So, suppose $d' > 0$, is another common divisor. Then $d'h = a$
$d'k = b$
for some h & k.
Then $d = as+bt = d'hs + d'kt = d'(hs+kt)$
So $d' \mid d$. In particular, $d' \leq d$.
So $d = \gcd(a,b)$

∎

Homework / Practice problem Review.

Ch3 (26/?)
A group with 2 elements that commute must have a subgroup of order 4.

Pf. Let G be a group, $a,b \in G$ s.t. $|a| = |b| = 2$, $ab = ba$, $a \neq b$.
We guess that $\{e, a, b, ab\}$ form a subgroup
Let $H = \{e, a, b, ab\}$, we want to check H is a subgroup.
Since $H \neq 0$, and H is a finite set, it suffices to check that H is closed under multiplication.

Drawing this's multiplication table:

·	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e