Math 128A, Wed Sep 16

- Use a laptop or desktop with a large screen so you can read these words clearly.
- In general, please turn off your camera and mute yourself.
- Exception: When we do groupwork, please turn both your camera and mic on. (Groupwork will not be recorded.)
- Please always have the chat window open to ask questions.
- Reading for today: Ch. 5.
- Exam review Fri Sep 18, 10:00–noon on Zoom. 128A 10am, 131B 11am, session will be recorded.
- **Exam 1 Mon Sep 21**, on Chs. 1–4 and PS01–03.
- Outline for PS04 due Wed Sep 23.

Exam procedure for Mon Sep 21

1. Please have a clear workspace ready where you can write.
2. Please have some kind of camera ready. First position the camera so I can see your face, and later so I can see your workspace.
3. Please have the Gradescope assignment page “Exam 1” open and ready to go.
4. Exam will be handed out via chat, or by email if necessary.

Questions?

What is $\langle a^k \rangle$ like?

G a group, $a, b \in G$, $\mathrm{ord}(a) = n < \infty$.

Theorem

We have

$$\left\langle a^k \right\rangle = \left\langle a^{\gcd(n,k)} \right\rangle, \qquad \mathrm{ord}(a^k) = \frac{n}{\gcd(n,k)}.$$

Corollary

$\left\langle a^k \right\rangle = \left\langle a^j \right\rangle$ *if and only if* $\gcd(n,k) = \gcd(n,j)$.

Corollary

a^k *generates* $\langle a \rangle$ *if and only if* $\gcd(n,k) = 1$.

Example: Suppose $\mathrm{ord}(a) =$ 12 $\boxed{1}, \cancel{2}, \cancel{3}, \cancel{4}, \boxed{5}, \cancel{6}, \boxed{7}, \cancel{8}, \cancel{9}, \cancel{10}, \boxed{11}$

The generators of $\langle a \rangle$ are:

$\to a^1, a^5, a^7, a^{11}$

$\mathrm{ord}(a)=12$, so $a^{12}=e$

$\langle a^5\rangle = \{a^5, a^{10}, a^{15}=a^3, a^8,$
$a^{13}=a, a^6, a^{11}, a^{16}=a^4,$
$a^9, a^{14}=a^2, a^7, a^{12}=e\}$

Same elements as <a>, but in different order.

Fundamental Theorem of Cyclic Groups

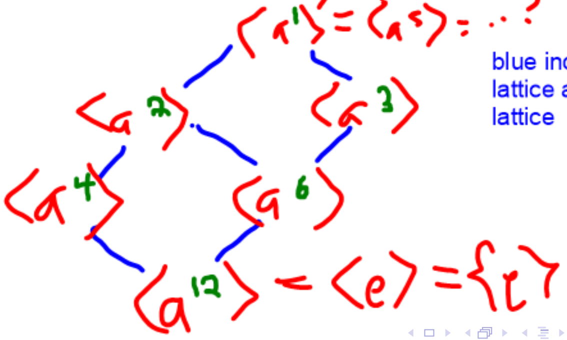
Theorem

Every subgroup of a cyclic group is cyclic. Also, if $\mathrm{ord}(a) = n$*, then the subgroups of* $\langle a \rangle$ *are precisely the subgroups* $\langle a^d \rangle$*, where* d *is some divisor of* n*.*

Example: Let $\mathrm{ord}(a) = n = 12$
Subgroups of $\langle a \rangle$:

Divs of 12: 1, 2, 3, 4, 6, 12

Subgp lattice



blue indicates divisor lattice and also subgp lattice

Why is $\langle a^2 \rangle \supseteq \langle a^6 \rangle$?

$$\langle a^2 \rangle = \{a^2, a^4, a^6, a^8, a^{10}, e\}$$

$$\langle a^6 \rangle = \{a^6, e\}$$

$$\langle a^3 \rangle = \{a^3, a^6, a^9, e\}$$

$$\langle a^4 \rangle = \{a^4, a^8, e\}$$

Neither set contains the other.

Elements of order d in a finite group

Definition

$\varphi(d)$ = number of elements of $\{1, \ldots, d\}$ that are relatively prime to d.

$\varphi(12) = 4$ b/c $1, 5, 7, 11$

Theorem

If $G = \langle a \rangle$ is cyclic of order $n = \operatorname{ord}(a)$, d divides n, then G has exactly $\varphi(d)$ elements of order d.

Because G has exactly one cyclic subgroup of order d, which has exactly $\varphi(d)$ generators. More generally:

Theorem

G a finite group. The number of elements of G of order d is a multiple of $\varphi(d)$.

This will be very useful! See PS04.

Ex: In *any* finite group, the number of elements of order 12 is a multiple of 4 (taking d=12, noting phi(12)=4).

Reminder:

f: A -> B means f is function with domain A, codomain B

domain A means possible inputs to f are from A
codmain B means possible outputs from f are all in B, though we don't assume that everything in B is actually achieved as an output.

f one-to-one: Never hit the same output twice.

f onto: Every possible output (i.e., every element of the codomain) is an actual output of the function.

f bijection: f one-to-one and onto.

See Ch. 0 pp 21-23.

See my proof notes for how to prove f 1-to-1, onto (A/C outline).

$f: \{1,2\} \to \{1,2\}$

$f(1) = 1$, $f(2) = 1$

Then f is not onto b/c 2 isn't hit (isn't an output of f).

Ch. 5: Permutations

Definition

A **permutation** of a set A is a bijection (one-to-one and onto) $\alpha : A \to A$.

Example: $A = \{1, 2, 3, 4, 5, 6, 7\}$, one possible α is:

So $\alpha(5) = 1$

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 6 & 3 & 5 & 1 & 7 & 4 \end{pmatrix} \begin{array}{l} \leftarrow \text{inputs} \\ \leftarrow \text{outputs} \end{array}$$

Permutations are multiplied by function composition. E.g., take also

on same set

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 6 & 4 & 2 & 5 & 7 \end{pmatrix}$$

Then compute $\alpha\beta$ (which is β, then α) by:

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 6 & 4 & 2 & 5 & 7 \\ 3 & 2 & 7 & 5 & 6 & 1 & 4 \end{pmatrix} \begin{array}{l} \}\beta \\ \}\alpha \end{array}$$

$\alpha \circ \beta$

So $\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 7 & 5 & 6 & 1 & 4 \end{pmatrix}$

Faster way to compute alpha*beta:

1 goes thru 3 to 3
2 goes thru 1 to 2
3 goes thru 6 to 7
4 goes thru 4 to 5
5 thru 2 to 6
6 thru 5 to 1
7 thru 7 to 4

$$(\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1}$$

$$= \begin{pmatrix} 3 & 2 & 7 & 5 & 6 & 1 & 4 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 2 & 1 & 7 & 4 & 5 & 3 \end{pmatrix}$$

Check $(\alpha\beta)(\alpha\beta)^{-1} = e = \varepsilon$

Permutation groups

Definition

Sym(A) is the group of **all** permutations of A. If $A = \{1, \ldots, n\}$, we abbreviate Sym(A) as S_n, the **symmetric group of degree** n.

Example: In S_7, α as before:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 6 & 3 & 5 & 1 & 7 & 4 \end{pmatrix}$$

Identity and α^{-1} are:

$$\varepsilon = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}$$

$$\alpha^{-1} = \begin{pmatrix} 2 & 6 & 3 & 5 & 1 & 7 & 4 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 1 & 3 & 7 & 4 & 2 & 6 \end{pmatrix}$$

Definition

A **permutation group** is a subgroup of Sym(A), i.e., a set of permutations that itself forms a group.

You try

Given:

Next

Compute $\alpha\beta$.

time.

Cycle notation for permutations

In S_7, the cycle $(1\ 4\ 7\ 3)$ (for example) represents the perm

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 1 & 7 & 5 & 6 & 3 \end{pmatrix} = (1\,4\,7\,3)\,(2)(5)(6)$$

Theorem

Every permutation is a product of disjoint cycles.

Proof by (an example of) algorithm: In ~~S_{12}~~ S_9, take

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 7 & 5 & 4 & 1 & 2 & 9 & 8 \end{pmatrix} \in S_9$$

Then

$$\alpha = (1\,3\,7\,2\,6)(4\,5)(8\,9)$$

Permutations in cycle form

Definition

The **cycle form** of a permutation α is α expressed as a product of disjoint cycles.

Theorem

Disjoint cycles commute.

Proof by playing cards!

Order of a permutation in cycle form

Theorem

The order of a permutation written in cycle form is the LCM of its cycle lengths.

Proof: Suppose $\alpha = \alpha_1 \cdots \alpha_k$ in cycle form (i.e., α_i and α_j are disjoint for $i \neq j$). Then because disjoint cycles commute:

$$\alpha^n = \alpha_1^n \cdots \alpha_k^n.$$

Because disjoint cycles permute disjoint sets, to get $\alpha^n = \epsilon$, need to have **every** $\alpha_i^n = \epsilon$. So n must be a common multiple of cycle lengths, and smallest such n is the least common multiple of cycle lengths.

You try

Given:

Find $\mathrm{ord}(\alpha)$ and compute $\alpha\beta$ in cycle form.