Math 128A, Mon Sep 28

HW revisions: Submitted in a separate Gradescope assignment
Please only submit the problems you want to change.

- 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. 6. Reading for Wed: Ch. 7.
- PS04 due tonight. Outline for PS05 due Wed.
- Problem session Oct 02, 10:00–noon on Zoom.

If you want to discuss exam, please come to office hours:
M 2-3, W 1-2

Even and odd permutations

$= (15)(14)(13)(12)$

Recall:

$(12345) = (12)(23)(34)(45)$

$1 \leftarrow 2 \leftarrow 3 \leftarrow 4 \leftarrow 5$

Theorem

Every $\alpha \in S_n$ is a product of 2-cycles.

Lemma (Fact)

If $\epsilon = \beta_1 \beta_2 \ldots \beta_r$, where each β_i is a 2-cycle, then r is even.

Theorem

For $\alpha \in S_n$, exactly one of the following is true:

- *α is a product of an* **even** *number of 2-cycles; or*
- *α is a product of an* **odd** *number of 2-cycles.*

Proof: Suppose

$$\alpha = \beta_1 \ldots \beta_k = \gamma_1 \ldots \gamma_m,$$

(8)

socks and shoes

where each β_i and γ_j is a 2-cycle.

$$(\gamma_1 \cdots \gamma_m)^{-1} = \gamma_m^{-1} \cdots \gamma_1^{-1}$$

So mult both on L by $(\sigma_1 \cdots \sigma_m)^{-1}$: of (1)

π'l on one

$$\sigma_m^{-1} \cdots \sigma_1^{-1} \beta_1 \cdots \beta_k = \epsilon$$

inverse of n-cycle

But remember, the inverse of a 2-cycle is a 2-cycle. So the LHS is a product of m+k 2-cycles that is equal to the identity, so by the Lemma, m+k is even.

Therefore, m and k are either both even or both odd, which is what we wanted to prove.

Ex:

$$(1\,2\,3\,4\,5)^{-1} = (5\,4\,3\,2\,1)$$
$$= (1\,5\,4\,3\,2)$$

The alternating group

Definition

If α is product of an even number of 2-cycles, we say α is **even**; if α is product of an odd number of 2-cycles, we say α is **odd**.

Prev thm says that a permutation is either odd or even, but not both. $(n \geq 2)$

Fact (Thm)/Defn: Even permutations in S_n form a subgroup of S_n called the **alternating group** of degree n, written A_n.

Why is A_n a subgroup?

0. $\epsilon = (12)(12)$, so $\epsilon \in A_n$.

$\boxed{\exists}$ something in A_n

1. A $\alpha, \beta \in A_n$

key!

So $\alpha = \sigma_1 \sigma_2 \cdots \sigma_k$, k even

σ_i, τ_j 2-cycles

$\beta = \tau_1 \tau_2 \cdots \tau_m$, m even

So $\alpha\beta = \sigma_1 \sigma_2 \cdots \sigma_k \tau_1 \tau_2 \cdots \tau_m$

is prod of $k+m$ 2-cycles

$k+m$ is even, since k, m even

So $\alpha\beta$ is prod of even # 2-cycles

$\subset$ $\alpha\beta \in A_n$

key!

2. (inverse) similar

$$A_3 = \{\epsilon, (123), (132)\}$$

$$A_4 = \{\epsilon, (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243)\}$$

$$A_5 = \{\epsilon, (12)(34), \text{14 other } (ab)(cd), (123), \text{19 other } (abc), (12345), \text{23 other } (abcde)\}$$

$(1)(2)(12345)$

$(1)(2345)$

Size of A_n

Foreshadowing of Ch 7!

$(1\,2\,3) = (1\,2)(2\,3)$

Theorem

For $n \geq 2$, A_n is exactly half the size of S_n, i.e., $|A_n| = \dfrac{n!}{2}$.

Proof: Consider the set

$$O = (1\ 2)A_n = \{(1\,2)\sigma \mid \sigma \in A_n\} \quad (n \geq 3)$$

2-cycle * two 2-cycles

$$= \{(1\,2)\epsilon, (1\,2)(1\,2\,3), (1\,2)(1\,3\,2), \ldots\}$$

= three 2-cycles

Since every permutation of A_n is even, and we multiply each permutation in A_n by the 2-cycle (1 2) to get an element of O, every permutation in O is odd. So O is contained in the set of odd permutations of S_n.

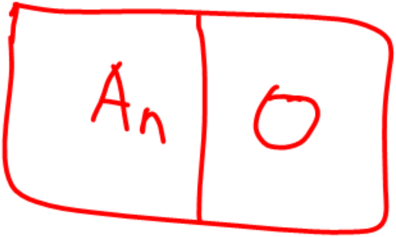
Conversely, suppose alpha is an odd permutation. Then:

$\beta = (1\,2)\alpha$ is even

But $(12)\beta = (12)(12)\alpha = \alpha$,

so $\alpha \in O$.

It follows that O is precisely the set of all odd permutations in S_n.



Partition of S_n

Sketch of the rest of the proof: Remains to show that A_n and O have same number of elements. One way to prove that is to prove that there is a bijection from A_n to O, such as:

$f: A_n \to O$ by $f(\sigma) = (12)\sigma$.

Try at home: Prove that f is one-to-one and onto.

Cycles as odd and even permutations

don't change odd/even
status of a product

- Cycles of odd length are even

Ex $(1\,2\,3\,4\,5) = (12)(23)(34)(45)$

- Cycles of even length are odd

Ex $(1\,2\,3\,4) = (12)(23)(34)$

- So if α is a product of disjoint cycles, α is an even permutation $\Leftrightarrow$

The disjoint cycle form of alpha contains an *even* number of cycles of *even* length.

See: PS04 #7(b).

Isomorphisms

You've seen (PS04 #1) that $\mathbf{Z}_{60}$ is "the same" as a multiplicative cyclic group $\langle a \rangle$ of order 60. What do we mean by "the same?"

Definition

A **isomorphism** from G to $\overline{G}$ is $\varphi : G \to \overline{G}$ such that

opn pres

1. For all $a, b \in G$,

$$\varphi(ab) = \varphi(a)\varphi(b)$$

and

2. φ is a bijection (one-to-one and onto).

(or if op'n in G is $*$, $\varphi(a * b) = \varphi(a)\varphi(b)$)

To say that G and $\overline{G}$ are **isomorphic** means that there exists an isomorphism $\varphi : G \to \overline{G}$.

We will see that we can think of isomorphic groups as being "the same" in terms of group theory.

Example

$\mathbb{Z}_{60} = \{0, \ldots, 59\}, + \pmod{60}$

Suppose $\overline{G} = \langle a \rangle$ is a cyclic group of order 60 (i.e., $\text{ord}(a) = 60$).
Define $\varphi : \mathbf{Z}_{60} \to \overline{G}$ by

$$\varphi(i) = a^i.$$

Thm: φ is an isomorphism.
Well-defined:

One-to-one: Meaning different inputs give different outputs.

(A) $a, b \in G$, $\varphi(a) = \varphi(b)$

$\vdots$

(C) $a = b$

Onto:

(A) $\bar{a} \in \bar{G}$

$\vdots$

(C) $\exists\, a \in \mathbb{Z}_{60}$ s.t. $\varphi(a) = \bar{a}$

Operation-preserving:

(A) $a, b \in G = \mathbb{Z}_{60}$

(C) $\varphi(\overbrace{a+b}^{\text{op'n in } \mathbb{Z}_{60}}) = \overbrace{\varphi(a)\varphi(b)}^{\text{op'n in } \bar{G}}$

Example

Let $\overline{G} = \{3n \mid n \in \mathbf{Z}\}$, operation $+$.
Define $\varphi : \mathbf{Z} \to \overline{G}$ by $\varphi(n) = 3n$.

Example?

$\mathbf{R}^*$ is nonzero reals, operation $\times$.

Define $\varphi : \mathbf{R}^* \to \mathbf{R}^*$ by $\varphi(x) = 3x$. Is φ an isomorphism?

Cayley's Theorem

Theorem

Every group G is isomorphic to a permutation group on the set G.

Sketch of proof: Define $T_g : G \to G$ by

$$T_g(x) = gx.$$

Let $\overline{G} = \{T_g \mid g \in G\}$, operation composition. Can show that each T_g is a permutation and that $\overline{G}$ is a group.
Now define $\varphi : G \to \overline{G}$ by

$$\varphi(g) = T_g.$$

To prove φ is an isomorphism, we need to:

How and why are isomorphic groups the same?

Theorem

$\varphi : G \to \overline{G}$ an isomorphism, $a, b \in G$. Then

1. $\varphi(e) = \overline{e}$.
2. $\varphi(a^n) = \varphi(a)^n$.
3. *a and b commute $\Leftrightarrow$ $\varphi(a)$ and $\varphi(b)$ commute.*
4. $G = \langle a \rangle \Leftrightarrow \overline{G} = \langle \varphi(a) \rangle$
5. $\mathrm{ord}(a) = \mathrm{ord}(\varphi(a))$.
6. *$x^k = b$ and $\overline{x}^k = \varphi(b)$ have the same number of solutions.*
7. *$\varphi^{-1} : \overline{G} \to G$ is also an isomorphism.*
8. *G and $\overline{G}$ have same number of elements of each order.*
9. *G abelian $\Leftrightarrow$ $\overline{G}$ abelian*
10. *φ sends subgroups of G to subgroups of $\overline{G}$, and vice versa.*
11. *φ sends the center of G to the center of $\overline{G}$.*

Proving that groups are **not** isomorphic

Not enough to pick some $\varphi : G \to \overline{G}$ and show φ isn't an isomorphism — maybe there's a different map that is!

But just as two people with different eye colors can't be genetic twins, two groups with different characteristics can't be isomorphic.

Example: Two groups of order 10 that aren't isomorphic?

Example: Prove that D_6 and A_4 aren't isomorphic.