Math 113, Fall 2019
Lecture 9, Thursday, 9/26/2019

1 Clicker Questions

1. Consider the following statements:

- α - The symmetric group S_{10} has 10 elements
- β - The symmetric group S_3 is cyclic
- γ - S_n is not cyclic for any n

Which of these are true?

It turns out, all cyclic groups are abelian, so none of the above is true.

2. Let G be a be a **finite** group.
Cayley's theorem constructs an isomorphism of G with a subgroup H of S_G.
We have $H = S_G$ if and only if:
(a) G is trivial
(b) $|G| \leq 2$
(c) $0 = 1$ (never)
(d) $G \cong S_n$ (for some $n \in \mathbb{N}$)
(e) None of the above
Vojta says this boils down to counting, and $|S_n| = n!$, so this is true precisely for $n = 1, 2$.

2 Permutation Groups

Theorem 2.1. Let A be a set. Then S_A (the set of permutations of A) is a group under composition of functions.

Proof. Composition is a well defined operation on S_A. Let $f, g \in S_A$. Then $f \circ g$ is a function from A to A, and it is bijective because it's a composition of bijections. Hence $f \circ g \in S_A$.
We check the three requirements (axioms). Associativity is proved already for composition of functions. The identity function $\mathrm{id_A : A \to A}$ is bijective, so it's in S_A. Also,

$$\mathrm{id_A \circ f = f \circ id_A = f, \forall_{f \in S_A}}.$$

Finally, to check the existence of the inverse element, consider that for all $f \in S_A$, because f is a bijection, it has a (unique) inverse function $f^{-1} A \to A$ characterized by

$$f \circ f^{-1} = f^{-1} \circ f = \mathrm{id_A},$$

so f^{-1} is an inverse **element** of f in S_A, the set of permutations (bijections). $\square$

Vojta reminds us that we've seen this in a Clicker question, but:

Definition: Permutation group $S_{\{1,2,\ldots,n\}}$ -

For all $n \in \mathbb{N}$, S_n is the permutation group $S_{\{1,2,\ldots,n\}}$.

Notice that $|S_n| = n!$ for all $n \in \mathbb{N}$ because choosing $\sigma \in S_n$ involves n choices for $\sigma(1)$, $n-1$ choices for $\sigma(2)$, and so on until 2 choices for $\sigma(n-1)$, and 1 choice for $\sigma(n)$, where these can be in any order.

Example: One such example is to consider permutations (shuffling orders) of a deck of cards: S_{52}. So S_{52} is the set of possible rearrangements of a 52-card deck.

Example: A simpler example is S_3, which we can write as:

$$S_3 = \{\rho_0, \rho_1, \rho_2, \sigma_1, \sigma_2, \sigma_3\},$$

where $\sigma_1 := \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ and $\rho_1 := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. Vojta reminds that there's a full group table on page 79 of our text.
From this table, we see that $\rho_i = \rho_1^i, \forall_{i=0,1,2}$ and $\mu_1 = \mu_1\rho_{i-1}$ (where $\mu = \sigma$).
Hence $S_3 = \langle \rho_1, \mu_1 \rangle$.
Permutations tell us something about all finite groups due to the following theorem:

Theorem 2.2. If the sets A and B have the same cardinality, then $S_A \cong S_B$.

Proof. Because they have the same cardinality, that means there exists some bijection $f : A \to B$. The idea for the rest of the proof is to use f to relabel the elements of A.
Define $\varphi : S_a \to S_B$ by $\varphi(\sigma) = f \circ \sigma \circ f^{-1}$. This maps B to B

$$\begin{tikzcd} B \arrow[r, "f^{-1}"] \arrow[rrr, bend right, "f\circ\sigma\circ f^{-1}"'] & A \arrow[r, "\sigma"] & A \arrow[r, "f"] & B \end{tikzcd}$$

and it is bijective because it's a composition of bijections. Similarly, define $\phi : S_B \to S_A$ by $\psi(\tau) = f^{-1} \circ \tau \circ f$ for all $\tau \in S_B$. Then

$$\psi \circ \varphi : S_A \to S_A = \mathrm{id}_{\mathrm{S_A}},$$

because

$$\begin{aligned} \psi(\varphi(\sigma)) &= f^{-1} \circ (f \circ \sigma \circ f^{-1}) \circ f \\ &= \cancel{f^{-1} \circ f} \circ \sigma \circ \cancel{f^{-1} \circ f} \\ &= \sigma \\ &= \mathrm{id}_{\mathrm{S_A}}(\sigma), \forall_{\sigma \in \mathrm{S_A}}. \end{aligned}$$

Similarly, $\varphi \circ \psi = \mathrm{id}_{\mathrm{S_B}}$. Therefore, φ is bijective, because it has an inverse, namely ψ.
Now to exhibit the homomorphism property, consider:

$$\begin{aligned} \varphi(\sigma_1) \circ \varphi(\sigma_2) &= f \circ \sigma^1 \circ f^{-1} \circ f \circ \sigma_2 \circ f^{-1} \\ &= f \circ \sigma_1 \circ \sigma_2 \circ f^{-1} \\ &= \varphi(\sigma_1 \circ \sigma_2), \forall_{\sigma_1, \sigma_2 \in S_A}. \end{aligned}$$

Then $\varphi : S_A \xrightarrow{\sim} S_B$, as required.

□

Definition: Dihedral group D_n -

For an integer $n \geq 3$, the **dihedral group** D_n is the group of symmetries (rigid motions) of a regular n-gon.
Moreover,

$$|D_n| = 2n$$

Notice that D_n has a subgroup $\cong \mathbb{Z}_n$, namely the rotations in the plane of the polygon. Moreover,

$$\underbrace{\mathbb{Z}_n}_{|\mathbb{Z}_n|=n} < \underbrace{D_n}_{|D_n|=2n} \leq \underbrace{S_n}_{|S_n|=n!},$$

where for all $n \geq 4$, the right 'inequality' is strict (it is a proper subgroup), and the left inequality is strict for all $n \leq 2$.

Theorem 2.3. (Cayley's Theorem) Every group G is isomorphic to a subgroup of S_A for some set A.

In fact, we'll show it's true with $A = G$. Keep in mind the following example:

$$\begin{array}{cccc} +_3 & 0 & 1 & 2 \\ 0 & 0 & 1 & 2 \\ 1 & 1 & 2 & 0 \\ 2 & 2 & 0 & 1 \end{array}.$$

Proof. In fact, we'll show it's true with $A = G$. We'll construct an isomorphism $\varphi : G \to H$ for some $H \leq S_G$.
To do this, define

$$\lambda_x : G \to G$$
$$\lambda_x(g) = xg, \forall_{g \in G}.$$

Note $\lambda_x = S_G$ because every element of G occurs exactly once in each row of the group table. Hence λ_x is bijective. Therefore we have $\varphi : G \to S_G$ is well defined.
Now φ is injective because all of the rows in the group are different (actually, $\lambda_x = \lambda_y \implies \lambda_x(e) = \lambda_y(e) \implies x = y$ because $\lambda_x(e) = xe = x$ and $\lambda_y = y$ similarly).
Now for the homomorphism property, consider:

$$\begin{aligned} \varphi(x) \circ \varphi(y) &= \lambda_x \circ \lambda_y \\ &= (g \mapsto \lambda_x(\lambda_y(g)) = x(yg) = (xy)g = \lambda_{xy}(g)) \\ &= \varphi(xy). \end{aligned}$$

Then by Lemma 8.15, φ is a group isomorphism (isomorphism of groups) with a subgroup of S_G. $\square$

3 Clicker Questions

3. Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 3 & 1 & 4 & 2 \end{pmatrix} \in S_6$.
Then all of the orbits of σ are:
$\{1,4,5\}, \{2,6\}, \{3\}$.

4. How many of the following are true, for the same σ as before?

$$\sigma = (1,5,4)(2,6)(3)$$
$$\sigma = (1,5,4)(2,6)$$
$$\sigma = (1,5,4)(6,2)$$
$$\sigma = (1,4,5)(2,6) \text{ this is false}$$
$$\sigma = (5,4,1)(2,6)$$

All but the fourth one are true.

4 Orbits and Cycles

Given a set A and permutation $\sigma \in S_A$, we define a relation on A by $a \sim b$ if

$$\sigma^n(a) = b,$$

for some $n \in \mathbb{Z}$. This is an equivalence relation, where:

$$\begin{aligned} \text{reflexivity} : \sigma^p(a) = a, \forall_{a \in A} \\ \text{symmetry} : \sigma^n(a) = b \implies \sigma^{-n}(b) = a \\ \text{transitivity} : \sigma^n(a) = b, \sigma^m(b) = c \implies \sigma^{n+m}(a) = c. \end{aligned}$$

Now because this is an equivalence relation, the cells of the corresponding partition are called "orbits" of σ.

Definition: Cycle -

We introduce **cycle notation**:

$$\sigma := (a_1, a_2, \dots, a_n), \text{ with } a_1, \dots, a_n \in A \text{ mutually distinct}$$

which means $\sigma(a_i) = a_{i+1}, \forall_{i=1,\dots,n-1}, \sigma(a_n) = a_1$, and $\sigma(a) = a, \forall_{a \notin \{a_1,\dots,a_n\}}$.
If σ is of this form, then we say it's a **cycle**.

Definition: Disjoint Cycles -

The cycles σ and τ are **disjoint** if

$$\{a \in A : \sigma(a) : \sigma(a) \neq a\} \cap \{a \in A : \tau(a) \neq a\} = \{\}$$

Vojta notes that the identity element is always a cycle (even in $S_\emptyset$ by definition).

Lecture ends here.