Math 113, Fall 2019
Lecture 10, Thursday, 10/1/2019

1 Clicker Questions

1. Write

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 1 & 6 & 2 & 4 & 7 & 3 \end{pmatrix} \in S_7$$

as a product of disjoint cycles.
Answer: One product is $(4, 2, 1, 5)(6, 7, 3)$ and another is $(1, 5, 4, 2)(3, 6, 7)$.

2. Which of the following are odd permutations?

$$\alpha = (1, 2)(2, 3)(3, 4) \in S_4$$
$$\beta = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10) \in S_{10}$$
$$\gamma = (1, 2, 3)(2, 4)(1, 3, 5) \in S_6.$$

Answer: All of them are odd permutations. We can write

$$\beta = (1, 2)(2, 3)(3, 4)(4, 5)(5, 6)(6, 7)(7, 8)(8, 9)(9, 10).$$

2 Even and Odd Permutations

Theorem 2.1. Every permutation of a finite set can be written as a product of disjoint cycles.
In addition, this is **unique** up to:
(1) Writing the cycles in a different order (disjoint cycles commute), and
(2) choosing a (possibly) different starting point for each cycle.

One particular kind of cycle is:

Definition: transposition -

A **transposition** is a cycle of length 2.
(This is only defined for some (a, b) where $a, b \in A$ and $a \neq b$.)

Vojta notes that these have the following central role:

Proposition 2.1.1. Every permutation of a finite set can be written as a product of transpositions.

Notice that we leave out the word 'disjoint' here because that would be false.

Proof. Use Thm 9.8 and the identity

$$(a_1, a_2, \ldots, a_n) = (a_1, a_2)(a_2, a_3) \cdots (a_{n-1}, a_n).$$

□

Then we have the following theorem:

Theorem 2.2. No permutation in (any finite set which would then be isomorphic to) S_n can be expressed both as a product of an even number of transpositions and as a product of an odd number of transpositions.

We'll sketch the book's second proof (as the first proof uses linear algebra's concept of the determinant, where many linear algebra texts rely on this theorem to develop the theory of determinants). The book shows that if $\sigma \in S_n$ is a permutation and $\tau \in S_n$ is a transposition, then:

$$(\#\text{ of orbits of } \sigma\tau) = (\#\text{ of orbits of } \sigma) \pm 1.$$

This rules out the possibility that the odd and even possibilities are concurrent. Vojta gives that the book thereafter is a bit sketchy, so we add a few more points.
We show that if σ is a product of m transpositions, then

$$m \equiv n - (\#\text{ of orbits of } \sigma) \pmod 2$$

To prove this, we use induction on m. Base case is $m = 0$ with $m = 0$ implies that σ is the identity, which implies that it has n orbits, with both sides of the congruence simply equals 0. Then the inductive step is easy.
Then, suppose σ is a product of m transpositions and is also a product of m' transpositions. Then notice

$$m = \underbrace{n - (\#\text{ orbits of } \sigma)}_{} \equiv m' \pmod 2,$$

where the underbraced portion depends only on σ. So $m \cong m' \pmod 2$.
This then allows us to define even and odd permutations, where any permutation is either one or the other (and not both).

Definition: Alternating Group -

The set $A_n = \{\sigma \in S_n \mid \sigma \text{ is even}\}$ is a subgroup of S_n, called the **alternating group**.

Vojta comments that the inverse of an even permutation is also even. Let's look at some examples.

2.1 Examples

Example:
Recall:

$$S_3 = \{\underbrace{\rho_0 = (1), \rho_1 = (1,2,3), \rho_2 = (1,3,2)}_{A_3,\text{ even}}, \underbrace{\mu_1 = (2,3), \mu_2 = (1,3), \mu_3 = (1,2)}_{\text{odd}}\}$$

If $n = 0$ or 1 then S_n is trivial, and so is A_n. Hence $|S_n| = |A_n| = 1$.
If $n \geq 2$, then $\sigma \mapsto \sigma \circ (1,2)$ maps $A_n \to S_n \setminus A_n$, and this is bijective. Hence

$$|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}.$$

Example: Recall at the beginning of the semester, we brought up the 15-puzzle. We teased that the solution of the 15-puzzle cannot be found if any two adjacent squares are interchanged.

3 More Clicker Questions

3. Let G be a finite cyclic group (order n) generated by element a, and let $b = a^s$. Then the **index** of the cyclic subgroup $\langle b \rangle$ of G is?

Answer: The index of $\langle b \rangle$ is

$$\frac{n}{\frac{n}{\gcd(s,n)}} = \gcd(s,n)$$

because the order of $\langle b \rangle$ is $\frac{n}{\gcd(s,n)}$. In Vojta's words, recall from before that

$$\langle b \rangle = \left\langle a^{\gcd(s,n)} \right\rangle$$

has $\frac{n}{\gcd(s,n)}$ elements, so as above, we have $\gcd(s,n)$.

4. How many of the following statements are true?

(T) A subgroup of a group is a left coset of itself; true by taking the identity $eH = H$
(F) Every finite group G contains an element of every order that divides the order of G; false via S_3, because if this were true, every group would be cyclic (order 6, but has no element of order 6, otherwise it would be cyclic)
(T) Every group of prime order is abelian; true because such groups are cyclic and hence abelian
(T) A_n is of index 2 is $S_n, \forall_{n>1}$.

4 Cosets and Lagrange's Theorem

Definition: Cosets -

Let H be a subgroup of a group G. Then a **left coset** of H in G is a sub**set** of G of the form

$$aH = \{ah : h \in H\}$$

for some $a \in G$.

In additive notation, this is

$$a + H = \{a + h : h \in H\}.$$

4.1 Facts about cosets

(Fact 1) $|aH| = |H|$ because $h \mapsto ah$ is a bijection $H \to aH$.

(Fact 2) $a \in aH, \forall_{a \in G}$. In particular, $aH \neq \emptyset, \forall_{a \in G}$, and $\cup_{a \in G} aH = G$.

(Fact 3) $b \in aH \implies bH = aH$.

Proof. Notice $b \in aH \implies b = ah$, for some $h \in H$. Then $bH = (ah)H = a(hH) = aH$. Recall that for every subset S of G and all $a \in G$, we defined $aS = \{as : s \in S\}$ as before. Then for all $a, b \in G, S \subseteq G$, we have

$$(ab)S = a(bS),$$

where $\{(ab)s : s \in S\} = \{a(bs) : s \in S\}$.
Finally, $hH = H, \forall_{h \in G}$, which Vojta leaves as an exercise. □

(Fact 4) If $aH \cap bH \neq \emptyset$, then $aH = bH$.

Proof. Pick $c \in aH \cap bH$. Then $aH = cH = bH$, by fact (3) above. □

Then facts (2) and (4) together imply the following theorem:

Theorem 4.1. Let H be a subgroup of a group G. Then the left cosets of H form a partition of G.

Vojta notes that the book presents this in a different way, constructing the corresponding equivalence relation. That is, $aH = bH \iff b^{-1}a \in H$.
We'll look at some examples.

Example: Let $H = \langle \mu_3 \rangle = \{\rho_0, \mu_3\} \in S_3$, where $\mu_3 = (1, 2)$.
Its left cosets are

$$\begin{aligned} \rho_0 H &= H = \{\rho_0, \mu_3\} \\ \rho_1 H &= \{\rho_1\rho_0, \rho_1, \mu_3\} = \{\rho_1, \mu_1\} \\ \rho_2 H &= \{\rho_2\rho_0, \rho_2\mu_3\} = \{\rho_2, \mu_2\}, \end{aligned}$$

via the table on page 79.
Then its right cosets are $\{\rho_0, \mu_3\}, \{\rho_1, \mu_1\}$, and $\{\rho_2, \mu_2\}$.
Notice that $H\rho_1 \neq \rho_1 H$.

Definition: $(G : H)$**, left coset -**

If $H < G$, then $(G : H)$ is the number (or cardinality) of left cosets of H in G.

On our homework, we prove that this is the same as the cardinality of **right** cosets of H in G.
This brings us to an important theorem, where we deviate a little from the book:

Theorem 4.2. (**Lagrange's Theorem**) Let G be a finite group and let H be a subgroup of G. Then

$$|G| = (G : H)|H|.$$

In particular, $|H|$ divides $|G|$.

Proof.

$$\begin{aligned} G &= \sum_{\text{cosets } aH} |aH| \\ &= \text{sum of } |H| \text{ added } (G:H) \text{ times} \\ &= (G:H)|H| \end{aligned}$$

□

4.2 Corollaries of Lagrange's Theorem

Corollary 4.2.1. If G is finite, then

$$(G:H) = \frac{|G|}{|H|}.$$

Corollary 4.2.2. Every group of prime order is cyclic.

Corollary 4.2.3. If G is a finite group with order n, then $a^n = e$, for all $a \in G$.

Proof. Let $m = |a|$. Then $m = |\langle a \rangle|$ divides n, so $a^n = (a^m)^{n/m} = e^{n/m} = e$. □

Now a fact:

S_3 is the smallest non-abelian group.

Proof. If $|G| = n < 6$, then

$$|G| = 2, 3, 5$$

imply n is prime, so G is cyclic, and hence abelian. Then if $|G| = 4$ (had an element of order 4), then it's cyclic and hence abelian. Otherwise, all $a \in G$ have order 1 or 2. Then this implies that $a^2 = e, \forall_{a \in G}$, which implies $a = a^{-1}, \forall_{a \in G}$, and hence

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba, \forall_{a,b \in G},$$

which is close to exercise 4.36 in the text. □

5 Introduction: Products of Groups

The groups we've developed so far are:

- cyclic
- permutation
- dihedral
- numbers: $(\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}^*, \ldots, U)$
- matrices
- Klein V

We can use groups we know about as building blocks to create other groups.

Recall that if $S_1, \ldots, S_n$ are sets, then their product

$$\prod_{i=1}^{n} S_i = S_1 \times \cdots \times S_n$$

is defined to be the set of all ordered n-tuplies $(s_1, \ldots, s_n)$, such that $s_i \in S_i$, for all i. A canonical example is $\mathbb{R}^n = \mathbb{R} \times \cdots \times \mathbb{R}$ (n times).

Then we can make the following definition:

Definition: Group product -

Let $G_1, \ldots, G_n$ be groups. Then their **product**

$$\prod_{i=1}^{n} G_i = G_1 \times \cdots \times G_n$$

is the set $\prod_{i=1}^{n} G_i$, with group operation defined component-wise.

So if $n = 2$, then $(a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2)$, and $(a_1, a_2)^{-1} = (a_1^{-1}, a_2^{-1})$, the identity element is (e_1, e_2) where e_i is the identity of G_i, for all i.

Remark: If all G_i are abelian, then so are their products.

This is easy to see, and we may refer to their product as their **direct sum**:

$$\bigoplus_{i=1}^{n} G_i = G_1 \oplus G_2 \oplus \cdots \oplus G_n.$$

Lecture ends here.