MATH H113: Honors Introduction to Abstract Algebra

2016-03-07

- Even and odd permutations

$\exists$ a handout

Theorem 1: Let $n \geq 2$. Then there is a *unique* homomorphism $\epsilon : S_n \to \{\pm 1\}$ (under multiplication) such that $\epsilon((a, b)) = -1$ $\forall$distinct $a, b \in \{1, 2, \dots, n\}$.
It is surjective.
We'll do this differently from the book (see handout).
For today, let $n \geq 2$ and let $A = \{1, 2, \dots, n\}$. We'll use the action of S_n on A given by $\sigma \cdot a = \sigma(a)$ ($\sigma \in S_n, a \in A$).
Ex. 18 in Sect. 17 (p. 45) says:
Let a group H act on a set A. Define a relation $\sim$ by $a \sim b$ if $a = h \cdot b$ for some $h \in H$. Then $\sim$ is an equivalence relation. The equivalence class $\bar{a}$ of an element $a \in A$ is called the *orbit* of a under the action of H.

Definition: Let $\sigma \in S_n$ and $a \in A$. Let $\sim$ be the above equivalence relation for the action of $H = \langle \sigma \rangle$ on A. Then the equivalence class $\bar{a}$ of a is called the *orbit* of a for σ.

Proposition: Let $\sigma \in S_n$ and $a \in A$. Let d be the smallest positive integerfor which $\sigma^d(a) = a$. Then the elements $\sigma^i(a)$, $i = 0, 1, \dots, d-1$, are distinct, and the orbit of a under σ $\{a, \sigma(a), \sigma^2(a), \dots, \sigma^{d-1}(a)\}$.
Proof: Let d be as above (this exists because if $m = |\sigma|$ then $m < \infty$ and $\sigma^m = 1$, so $\sigma^m(a) = a$. In general, though, d can be unequal to $|\sigma|$). The elements $\sigma^i(a)$, $i = 0, 1, \dots, d-1$ are distinct because if $\sigma^i(a) = \sigma^j(a)$ for some $O \leq i < j < d$, then (cancelling σ^i) $\sigma^{j-i}(a) = a$ with $0 < j - i < d$, contradicting the choice of d. Then $O = \{a, \sigma(a), \sigma^2(a) \dots, \sigma^{d-1}(a)\}$; the orbit ecause:

i. $O \in$ the orbit (clear, since $1, \sigma, \sigma^2 m \dots, \sigma^{d-1} \in \langle \sigma \rangle$).
ii. if $b \in$ the orbit then $b = \tau(a)$ with $\tau \in \langle \sigma \rangle$.

Write $\tau = \sigma^i$ for some $i \in \mathbb{Z}$.
Write $i = qd + j$ with $q, j \in \mathbb{Z}$ and $0 \leq j < d$.
Then $b = \sigma^i(a) = \sigma^{qd+j}(a) = \sigma^j(\sigma^{qd}(a)) = a = \sigma^j(a) \in O$.
$\therefore$ the orbit $\subseteq O$, so they're equal.

Corollary: Let σ, a, d be as above, and let $\tau = (a\ \sigma(a)\ \sigma^2(a)\ \dots\ \sigma^{d-1}(a))$. Then $\tau(b) = \sigma(b)$ $\forall b \in O$ and $\tau(b) = b$ $\forall (b) \notin O$.

Example: $\sigma = (1\ 2\ 3)(4\ 6)(5\ 7) \in S_8$.
Orbits are $\{1, 2, 3\}, \{4, 6\}, \{5, 7\}, \{8\}$.

Theorem 2: Every permutation in S_n can be written as a product of disjoint cycles. Such a representation is unique up to:

1. adding or removing 1-cycles,
2. permuting the disjoint cycles (which all commute with each other), and
3. choosing a different starting point for (some of) the cycles.

Proof: **Existence**: Given $\sigma \in S_n$, choose one element in each orbit of σ, and multiply the cycles as in the corollary for all such elements. The cycles are disjoint because the orbits are disjoint. Their product is σ because $\forall a \in A$, only on eof the cycles affects a or $\sigma(a)$, and that cycle maps a to $\sigma(a)$.
Uniqueness: Suppose $\sigma = \tau_1, \tau_2, \ldots, \tau_k$ where $\tau_1, \ldots, \tau_k$ are disjoint cycles. Include extra 1-cycles so that each element of A occurs in exactly one of the cycles of τ. Then you have an equivalence relation $\sim$ on A given by $a \sim b$ if they occur in the same cycle τ_i. This is the same equivalence relation as the one giving the orbits of σ. Then each τ_i is as in the corollary; if you choose a different "a", you just end starting the cycle at a different point.

Now we can prove Thm. 1 (about existence and uniqueness of $\epsilon : S_n \to \{\pm 1\}$).
Definition: A *transposition* is a 2-cycle.
Proposition: Every element of S_n can be written as a product of transpositions (not uniquely).
Proof: For any d-cycle, you have: $(a_1\ a_2\ \ldots\ a_d) = (a_1\ a_2)(a_2\ a_3)\ldots(a_1\ a_d)$ $(\forall d \in \mathbb{Z}_{>0})$. So a d-cycle is a product of $d-1$ transpositions.
For any $\sigma \in S_n$, write it as a product of (disjoint) cycles and apply the above to each cycle.
So if $\sigma = \tau_i\ \tau_2\ \ldots \tau_k$, where $\tau_1, \ldots, \tau_k$ are disjoint cycles and every element of a occurs in some τ: ($\therefore$ in exactly one τ_i, how many transpositions do we get?
Say τ_i has length d_i for each i. Then the number of transpositions is:
$\sum\limits_{i=1}^{k}(d_i - 1) = (\sum\limits_{i=1}^{k} d_i) - (\sum\limits_{i=1}^{k} 1) = n - k,$
where k is the number of orbits of σ.
If ϵ exists, then it has to equal $(-1)^{n-k}$ because it's a homomorphism, and ϵ of each transpositions is -1.

Definition: Define $\epsilon : S_n \to \{\pm 1\}$ by $\epsilon(\sigma) = (-1)^{n-k}$, where k is the number of orbits of σ. This is well defined (but we need to prove it's a homomorphism).

Lemma: Let $a_1, a_2, \ldots, a_r, b_1, b_2, \ldots, b_s$ be distinct elements of A, with $r, s \in \mathbb{Z}_{>0}$. Then:

a. $(a_1\ a_2\ \ldots\ a_r)(b_1\ b_2\ \ldots b_s)(a_r\ b_s) = (a_1\ a_2\ \ldots\ a_r\ b_1\ b_2\ ldots\ b_s)$ and
b. $(a_1\ a_2\ \ldots\ a_r\ b_1\ b_2\ \ldots b_s)(a_r\ b_s) = (a_1\ a_2\ \ldots\ a_r)(b_1\ b_2\ ldots\ b_s)$

Proof:

a. Compute both sides and see that they're equal (see handout).
b. Multiply both sides of (a) on the right by (a_r b_s).

Corollary: Multiplying an element of S_n by a transposition changes its number of orbits by ± 1.

Proposition: If $\sigma \in S_n$ can be written as a product of m transpositions, then $\epsilon(\sigma) = (-1)^m$.
Proof: We showed that if $\rho, \tau \in S_n$ and τ is a transposition then $\epsilon(\rho\tau) = -\epsilon(\rho)$.
Also $\epsilon(1) = 1$ (because 1 has n orbits).
Apply this m times, starting with $\epsilon(1) = 1$ to get $\epsilon(\sigma) = (-1)^m$.

Then $\epsilon(\tau) = -1$ $\forall$ transpositions τ (take $m = 1$), and ϵ is a homomorphism (if σ is a product of m transpositions and ρ is a product of k transpositions then $\sigma\rho$ is a product of $m + k$ transpositions and $\therefore$ $\epsilon(\sigma\rho) = (-1)^{m+k} = (-1)^m(-1)^k = \epsilon(\sigma)\epsilon(\rho)$. So ϵ exists.
And ϵ is unique because we said what it has to be.