Math 541 Notes

Mar 25, 2011

Theorem: $\exists!$ homomorphism $\varphi : S_n \to \{\pm 1\}$, which is onto.

Proof. Uniqueness: Suppose φ satisfies the conditions of the theorem, we are then led to the following discussion:
Claim 1: $\varphi(\tau) = -1$, $\forall \tau$ transpositions.
Remark: Every $\sigma \in S_n$ can be written (with parity unchanged, i.e. If $\sigma = \tau_1 ... \tau_k = \tau'_1 ... \tau'_r$, then $k - r$ is even.)
$\sigma = \tau_1 ... \tau_n$
where τ_i are transpositions.

Proof. (proof of Claim 1) If $\varphi(\tau) = 1$, $\forall \tau$ transpositions,
then $\varphi(\sigma) \overset{hom}{=} \varphi(\tau_l) \circ ... \circ \varphi(\tau_l) = 1...1 = 1$
so φ is not onto,
so $\exists \tau$ such that $\tau = (ab)$ such that $\varphi(\tau) = -1$ ☐

Claim 2: Any τ, τ' transpositions are conjugated. i.e., $\exists \sigma \in S_n$ such that $\sigma \tau \sigma^{-1} = \tau'$.
In particular $\forall \tau, \tau'$,

$$\varphi(\tau') = \varphi(\sigma \cdot \tau \cdot \sigma^{-1}) = \varphi(\sigma)\varphi(\tau)\varphi(\sigma)^{-1} \overset{\varphi(\sigma) \in \{\pm 1\}}{=} \varphi(\tau)$$

Proof. (proof of Claim 2) $\tau = (ab)$
$\tau' = (cd)$
computation: $(bc)(ab)(bc)^{-1} = (ac)$
$(ad)(ac)(ad)^{-1} = (cd)$
thus we conclude $\sigma(ab)\sigma^{-1} = (cd)$,
where $\sigma = (ad)(bc)$. ☐

The above discussion implies the uniqueness because if φ, φ' satisfies conditions of theorem, then $\forall \sigma \in S_n$, we have
$\varphi(\sigma) \overset{\varphi hom}{=} \varphi(\tau_l) \circ ... \circ \varphi(\tau_n) = \varphi'(\tau_l) \circ ... \circ \varphi'(\tau_n) \overset{\varphi' hom}{=} \varphi'(\sigma)$, where the second equality is because $\varphi(\tau_i) = -1 = \varphi'(\tau_i), \forall \tau_i$ transpositions.

Existence: we have constructed before the homomorphism

$$sgn : S_n \to \{\pm 1\}$$

and it is onto, since $sgn(\tau) = -1, \forall \tau$ transpositions. ☐

Corollary: If $\sigma = \tau_l ... \tau_1$ and $\sigma = \alpha_{l'} ... \alpha_1$ are two decompositions of σ into transpositions, then $l' - l$ is even (always both odd or both even).

Proof. $sgn(\sigma) = sgn(\tau_l \circ ... \circ \tau_n) \overset{hom}{=} sgn(\tau_l) \circ ... \circ sgn(\tau_l) = (-1)^l$
$sgn(\sigma) = sgn(\alpha_{l'}...\alpha_{l'}) = (-1)^{l'}$
$(-1)^{l'-l} = 1$ □

Lemma: Every permutation $\sigma \in S_n$ can be written uniquely as $\sigma = c_l...c_1$ up to order, where each c_i is a permutation which is a cycle
$c_i = (\vec{a_{1i}}\vec{a_{2i}} \; ... \; \vec{a_{ni}})$, $|c_i| \cap |c_j| \neq 0, i \neq j$
(Example: In S_3 (123) is a cycle)
such that interseptions between $c_i, |c_i| = \emptyset$ is empty.

Proof. by induction on n

$$n = 1$$

$$n = 2$$

both satisfy.
General n, suppose claim is true in $S_k, \forall k < n$.
Take $id \neq \sigma \in S_n$. Take the element 1, without loss of generality, $\sigma(1) = 2$.
Continue, $\sigma(2) = 1$ or $\sigma(2) = 3 \neq 1$
In the first case, $\sigma = (12) \circ \underbrace{(3...)}_{\tau}$
τ can be considered as an element in $S_k, k \equiv h - 2$
(*) by induction,
$\tau = (...) \circ (...) \circ (...)$
In the second case, $\sigma = (12...m) \circ \underbrace{(...)}_{\tau}$
If $m = n, \sigma = (12...n)$
If $m < n$, we are back in argument like (*). □

Math 541 Notes

Mar 28, 2011

Let $\varphi : G \to H$ be a homomorphism.

Claim: (a) Denote $\ker(\varphi) = \{g \in G | \varphi(g) = 1_G\}$. Then $ker(\varphi) < G$.

(b) $\{\varphi(g) | g \in G\} = Im(\varphi) < H(b)$

Proof. a)(i) Closure. $g_1, g_2 \in \ker(\varphi)$

$\varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2) = 1 \cdot 1 = 1 \Rightarrow g_1, g_2 \in ker(\varphi)$

(ii) Identity.

$\varphi(1_G \cdot 1_G) = \varphi(1_G) = \varphi(1_G) \cdot \varphi(1_G)$

Multiply both sides by $\varphi(1_G)^{-1}$, get

$1_H = \varphi(1_G)$,

so $\varphi(1_G) = 1_H$.

(iii) Show that for $g \in \ker(\varphi)$ also

$g^{-1} \in \ker(\varphi)$

but $\varphi(g^{-1}) = \varphi(g)^{-1} = 1^{-1} = 1$.

b) $Im(\varphi) < H$

(i) Closure. $h_1 = \varphi(g_1), h_2 = \varphi(g_2)$

$h_1 \cdot h_2 = \varphi(g_1) \cdot \varphi(g_2) \overset{hom}{=} \varphi(g_1 \cdot g_2)$

(ii) $1_H \in Im(\varphi)$, because $\varphi(1_G) = 1_H$.

(iii) If $h = \varphi(g) \in Im(\varphi)$

then $h^{-1} = \varphi(g)^{-1} = \varphi(g^{-1})$

so $h^{-1} \in Im(\varphi)$. □

Examples:

(1) Let $GL_2(\mathbb{R})$ denote the general linear group of order 2 over $\mathbb{R}$,

$det : GL_2(\mathbb{R}) \to \mathbb{R}^*$

$\ker(det) = SL_2(\mathbb{R})$, called special linear group.

(2) $n \geq 1, sgn : S_n \to \{\pm 1\}$,

$\ker(sgn) = A_n$,

It is called alternating group of order n, and has $\#A_n = n!/2$ groups of even permutations.

For instance, let's consider $\ker(sgn)$ of the following map:

sgn:$S_3 \to \{\pm 1\}$

In this case the solution is $\ker(sgn) = \{(id), (123), (132)\}$.

(3) $det : O(2) \to \{\pm 1\}$ Hw4

$ker(det) = SO(2) = R$ =rotations of $\mathbb{R}^2$.

It is a special O group.

(4) m,n with no common divisor.

A good example is $m = 2, n = 3$.

In addition to the above, consider $\mathbb{Z}_m = \{0, ..., m-1\}$, $\mathbb{Z}_n = \{0, ..., n-1\}$, and $\mathbb{Z}_{mn} = \{0, ..., mn-1\}$.

Definition: Let G, H be groups. Define the product of G and H to be the triple

⊙G×H– Cartesian product,

⊙operation (g,h)·$(g', h') = (gg', hh')$,

⊙Id=$(1_G, 1_H)$.

Theorem(Chinese Reminder Theorem) The map $\varphi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$

$$x \mapsto (x \bmod m,\ x \bmod n)$$

is an isomorphism of groups.

Proof. (i) hom. HW

(ii) Bijection enough to show $1-1$ compute $\ker(\varphi)$.

Suppose $x \in \ker(\varphi)$ $0 \leq x < mn$. This means

$x \bmod m = 0 \Rightarrow m|x$

$x \bmod n = 0 \Rightarrow n|x$

Recall if N is an integer ≥ 1

then $\exists!$ factorization?

$N = P_1^{k_1} ... P_r^{k_r}$ prime number

Now $m|x$, $m = P_1^{k_1} ... P_r^{k_r}$

$n|x$, $n = P_1'^{k_1'} ... P_r'^{k_r'}$

$P_i s$ and $P_i' s$ are different

so $mn|x \Rightarrow x \equiv 0$ in $\mathbb{Z}_{mn}$ ∎