MATH 171 FALL 2008: LECTURE 19

DAGAN KARP

1. Group actions continued

Remark 1. Recall that group actions $G \circlearrowright A$ give rise to equivalence relations

$$[a] = \{x \cdot a : x \in G\}$$

for $a \in A$. The equivalence class $[a]$ of a is called the *orbit* of a.

In particular, any group G acts on itself via conjugation. The map

$$G \times G \to G$$

is given by

$$(x, y) \mapsto x \cdot y = c_x(y) = xyx^{-1}.$$

The equivalence classes under this action are called *conjugacy classes*. For $y \in G$, the conjugacy class of y, denoted C_y is

$$C_y = [y] = \{xyx^{-1} : x \in G\}.$$

Proposition 2. *The stabilizer G_a of a is a subgroup of G. There is a one to one correspondence between the left cosets of G_a and the elements of the orbit of a; hence the order of the orbit of a equals the index of G_a.*

Proof. If $x, y \in G_a$, then $a = y \cdot a$, hence $y^{-1} \cdot a = a$ and

$$xy^{-1} \cdot a = x \cdot (y^{-1} \cdot a) = x \cdot a = a.$$

Thus $xy^{-1} \in G_a$ and therefore $G_a \leqslant G$.

Now, let b be an element of the orbit of a, i.e. $b = x \cdot a$ for some $x \in G$. Define

$$C(b) = \{y \in G : y \cdot a = b\}.$$

Then $y \in C(b)$ if and only if $y \cdot a = x \cdot a$, and so

$$a = x^{-1} \cdot (y \cdot a) = (x^{-1}y) \cdot a.$$

Therefore $x^{-1}y \in G_a$ and $y \in xG_a$. Therefore $C(b) = xG_a$ is a left coset of G_a.

Conversely, let xG_a be a left coset of G_a. Then $y \in xG_a$ if and only if $x^{-1}y \in G_a$, i.e. $x^{-1}y \cdot a = a$, i.e., $y \cdot a = x \cdot a$. Hence $xG_a \cdot a$ is a single element of A; call it $\theta(xG_a)$.

The maps θ and C are mutually inverse bijections.

Date: November 12, 2008.

Corollary 3. *For each $x \in G$, the centralizer $C_G(x)$ is a subgroup of G, and the number of conjugates of x equals the index of the centralizer*

$$|C_x| = [G : C_G(x)].$$

As an immediate application of the above, we have the following.

Corollary 4. *For any group G and $x \in G$, the following are equivalent.*

(1) $|C_x| = 1$.
(2) $C_G(x) = G$.
(3) $xy = yx$ *for all* $y \in G$.

Theorem 5 (Class equation)**.** *For any group G,*

$$|G| = |Z(G)| + \sum_{|C_x|>1} |C_x|.$$

Proof. The conjugacy classes of elements of G partition G. Thus $G = \bigcup_{x \in G} C_x$, where this union is disjoint, and hence $|G| = \sum_{x \in G} |C_x|$. Separating the trivial from nontrivial conjugacy classes yields the class equation.

$$|G| = \sum_{|C_x|=1} |C_x| + \sum_{|C_x|>1} |C_x| = |Z(G)| + \sum_{|C_x|>1} |C_x|.$$

□

Proposition 6. *Every group of order $p^n > 1$ with p prime has a nontrivial center.*

Proof. Let G have order p^n. By Lagrange's theorem, the index of any subgroup of G is a power of p. Hence the order of every conjugacy class is a power of p. In particular p divides $\sum_{|C_x|>1} |C_x$. Hence by the class equation p divides $|Z(G)|$. Therefore $|Z(G)| \neq 1$. □

Lemma 7. *If $G/Z(G)$ is cyclic, then G is Abelian.*

Proposition 8. *Every group of order p^2 with p prime is Abelian.*

Proof. Let $G = p^2$. By the above, $|Z(G)| = p$ or p^2. If $|Z(G)| = p^2$, then $G = Z(G)$ and G is Abelian. Otherwise,

$$|G/Z(G)| = |G|/|Z(G)| = p.$$

Hence $G/Z(G)$ is cyclic and G is Abelian by the above. □

Remark 9. Note the strange logic here. If G is Abelian, then $G = Z(G)$ and hence $|Z(G)| = p^2$, so the second case can not be realized.

2. Cayley's theorem and permutations

Theorem 10 (Cayley's theorem)**.** *Every group is isomorphic to a subgroup of a group of permutations. If G is a group of order n, then G is isomorphic to a subgroup of S_n.*

Proof. We define a map

$$G \to S_G$$

by

$$g \mapsto \lambda_g,$$

where $g \in G$ and $\lambda_g : G \to G$ is given by

$$\lambda_g(x) = g \cdot x = gx$$

for any $x \in G$.

We need to show that λ_g is indeed a permutation of the elements of G and that G is mapped isomorphically onto its image.

For any $g \in G$, that $\lambda_g \in S_G$ is elementary. It's inverse is given by $\lambda_{g^{-1}}$; for each $x \in G$,

$$\lambda_g \circ \lambda_{g^{-1}}(x) = gg^{-1}x = x = g^{-1}g = \lambda_{g^{-1}} \circ \lambda_g(x).$$

Now we show that our map $G \to S_G$ is a homomorphism. But for each $x \in G$,

$$\lambda_{gg'}(x) = gg'(x) = g(g'x) = \lambda_g(\lambda_{g'}(x)).$$

Finally, we inspect the kernel.

$$\lambda_g = I \iff \lambda_g(x) = x \text{ for all } x \in G.$$

In that case $gx = x$ for all $x \in G$. Therefore $g = 1$. Therefore G is isomorphic to its image, which is a subgroup of S_G. □

Definition 11. *The permutation representation induced by left multiplication (as above) is called the* left regular representation *of* G*.*

This gives us an interesting and historical perspective. One may attempt to study all of group theory via symmetric groups. This is in fact the historical approach. Our more abstract and axiomatic study of the subject arose only later.

With that in mind, let's apply some of our knowledge of group actions to the specific example of the symmetric group.

Definition 12. *Let $\sigma \in S_n$ be a permutation. The* cycle type *of σ is a nonincreasing sequence of positive integers $(l_1, l_2, \ldots, l_r)$,*

$$l_1 \geqslant l_2 \geqslant \cdots \geqslant l_r$$

such that σ may be decomposed into disjoint cycles length l_i,

$$\sigma = \sigma_1\sigma_2\cdots\sigma_r \qquad\qquad |\sigma_i| = l_i.$$

Example 13. *The cycle type of $(123)(34) \in S_4$ is 4, as*

$$(123)(34) = (1234).$$

The cycle type of $(12)(34)$ is $(2,2)$, as this permutation is written as a product of disjoint transpositions.

Proposition 14. *Every permutation is a product of pairwise disjoint cycles; moreover this decomposition is unique up to the order of the terms.*

Theorem 15. *Two permutations in S_n are conjugate if and only if they are of the same cycle type.*

Lemma 16. *For a permutation $\sigma \in S_n$, and $\tau = (a_1, \dots, a_k)$ a k-cycle in S_n,*

$$\sigma\tau\sigma^{-1} = (\sigma(a_1), \dots, \sigma(a_k)).$$

Proof. Note that

$$\sigma\tau\sigma^{-1}(\sigma(a_i)) = \sigma\tau(a_i) = \sigma(a_{i+1}).$$

Also, if $b \neq a_1, \dots, a_k$, then $\sigma^{-1}(b) \neq a_1, \dots, a_k$. Thus τ fixes $\sigma^{-1}(b)$,

$$\tau\sigma^{-1}(b) = \sigma^{-1}(b).$$

Thus $\sigma\tau\sigma^{-1}(b) = \sigma\sigma^{-1}(b) = b$. Therefore

$$\sigma\tau\sigma^{-1} = (\sigma(a_1), \dots, \sigma(a_k)).$$

□

Proof of theorem. Suppose that σ and τ are conjugate in S_n. Then there exists a permutation $\alpha \in S_n$ such that

$$\sigma = \alpha\tau\alpha^{-1}.$$

Inspect the cycle decomposition of τ,

$$\tau = \tau_1\tau_2 \cdots \tau_r,$$

where τ_i are pairwise disjoint cycles of length l_i,

$$\tau_i = (a_{i,1} \dots a_{i,l_i}).$$

Then

$$\begin{aligned}
\sigma &= \alpha\tau\alpha^{-1} \\
&= \alpha\tau_1 \cdots \tau_k\alpha^{-1} \\
&= (\alpha\tau_1\alpha^{-1})(\alpha\tau_2\alpha^{-1})(\cdots \alpha\tau_k\alpha^{-1}) \\
&= (\alpha(a_{1,1}) \cdots \alpha(a_{1,l_1}))(\alpha(a_{2,1}) \cdots \alpha(a_{2,l_2})) \cdots (\alpha(a_{r,1}) \cdots \alpha(a_{r,l_r})).
\end{aligned}$$

These are disjoint cycles and hence σ has the same cycle structure as τ.

Conversely, suppose σ and τ have the same cycle structure. Define α to be the function mapping the i^{th} integer in the cycle decomposition (ignoring parentheses) of σ to the i^{th} integer in the cycle decomposition of τ. Then

$$\alpha\sigma\alpha^{-1} = \tau.$$

□