KTH Teknikvetenskap

SF2729 GROUPS AND RINGS
LECTURE NOTES
2010-02-09

MATS BOIJ

3. The third lecture - permutations

In the third lecture, we take a closer look at the example of the symmetric groups of permutations which turns out to be the general example in the sense that any group is isomorphic to a subgroup of some symmetric group. In the case of finite groups, this is Cayley's theorem. [1]

Definition 3.1 (Symmetric group)**.** If X is any set, the *symmetric group on* X is the set of bijective functions $\sigma : X \longrightarrow X$ under composition. In the special case when $X = \{1, 2, \dots, n\}$, we write S_n for $S_{\{1,2,\dots,n\}}$ — *the symmetric group on* n *letters*.

We shall now look more closely on finite permutations. There are several notations we use for the same permutation:

Example 3.2. Let σ denote the pemutation in S_7 which is given by $\sigma(1) = 4$, $\sigma(2) = 6$, $\sigma(3) = 3$, $\sigma(4) = 7$, $\sigma(5) = 5$, $\sigma(6) = 2$, $\sigma(7) = 1$, can be written in the *two-row notation* as

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

in the *one-row notation* as

$$\sigma = [4\,6\,3\,7\,5\,2\,1]$$

or in the *cycle notation* as

$$\sigma = (1\,4\,7)(2\,6)(3)(5)$$

since σ partitions the set $\{1, 2, \dots, 7\}$ into the four disjoint cycles

$$1 \overset{\sigma}{\mapsto} 4 \overset{\sigma}{\mapsto} 7 \overset{\sigma}{\mapsto} 1, \qquad 2 \overset{\sigma}{\mapsto} 6 \overset{\sigma}{\mapsto} 2, \qquad 3 \overset{\sigma}{\mapsto} 3, \qquad 5 \overset{\sigma}{\mapsto} 5$$

of lengths 3, 2, 1 and 1. We often omit the cycles of length one and write $\sigma = (1\,4\,7)(2\,6)$.

Theorem 3.3. *If X is finite, any permutation σ in S_X is a product of disjoint cyclic permutations. The cycles are the minimal invariant subsets.*

[1] The third lecture is based on the sections 8-9 of Chapter II in A First Course in Abstract Algebra [1].

Proof. Let x be any element of X and let $Y = \{\sigma^i(x) | i \in \mathbb{Z}\}$ — the *orbit of* x *under* σ. Now Y is an invariant subset of X which contains no non-empty subset invariant under σ. Thus σ defines a cyclic permutation on Y.

Moreover, σ defines a permutation of $X \setminus Y$, and by induction on $|X|$, we can write this permutation as a product of cycles. (The base for the induction is the empty set for which the statement is trivially true.) □

Definition 3.4 (Cycle type)**.** The *cycle type*, or just *type*, of the permutation $\sigma \in S_n$ is the partition of the integer n into cycle lengths corresponding to the lengths of the cycles in σ.

Definition 3.5 (Conjugate permutations)**.** Two permutations, σ and τ, are the same up to relabelling of the elements of X if there is a permutation ρ such that

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

which means that the diagram

$$\begin{array}{ccc} X & \xrightarrow{\sigma} & X \\ \rho\downarrow & & \rho\downarrow \\ X & \xrightarrow{\tau} & X \end{array}$$

commutes.

Remark 3.6. Observe that the same definition makes sense for any group G. In particular, we recognize this from linear algebra when two matrices, A and $P^{-1}AP$, define the same linear map with respect to different bases.

Exercise 3.7. *Show that if X is finite, two permutations in S_X are conjugate if and only if they have the same cycle type.*

Exercise 3.8. *Show that the symmetric group S_n is generated by the adjacent transpositions,* $(1\,2)$, $(2\,3)$,..., $(n-1\,n)$.

Definition 3.9 (Inversions, length)**.** An *inversion* in a permutation $\sigma \in S_n$ is a pair (i, j), such that $1 \le i < j \le n$ and $\sigma(i) > \sigma(j)$. The number of inversions in σ is the *length* of σ, denoted by $\ell(\sigma)$.

Example 3.10. The permutation $\sigma = [4\,6\,3\,7\,5\,2\,1]$ has has length $\ell(\sigma) = 3+4+2+3+2+1 = 15$ since 4 comes before 3 smaller numbers, 6 comes before 4 smaller numbers, etc.

Theorem 3.11. *The length of σ equals the minimal number of factors in an expression $\sigma = s_{i_1}s_{i_2}\cdots s_{i_\ell}$, where $s_{i_1}, s_{i_2}, \ldots, s_{i_\ell}$ are adjacent transpositions.*

Idea of proof. The number of inversions is either increased or decreased by one by multiplication with an adjacent transposition $s_i = (i\,i+1)$. Thus $\ell(\sigma)$ is a lower bound for the numbers of adjacent transpositions needed. On the other hand, we can make sure to use only transpositions that increases the length, so it can be done with $\ell(\sigma)$ transpositions. □

Example 3.12.

$$(1\,4) = [4\,2\,3\,1] = (1\,2)(2\,3)(3\,4)(2\,3)(1\,2)$$

and $\ell([4\,2\,3\,1]) = 3 + 1 + 1 = 5$.

Definition 3.13 (Even and odd permutations, sign)**.** A permutation $\sigma \in S_n$ is *even* or *odd* depending on if its length is even or odd. The sign of σ is $+1$ if σ is even and -1 if σ is odd.

Theorem 3.14. *The sign function defines a group homomorphism*

$$\operatorname{sgn} : S_n \longrightarrow \{\pm 1\}.$$

Proof. Let σ and τ be permutaions of length $a = \ell(\sigma)$ and $b = \ell(\tau)$. Then we can write $\sigma\tau$ as a product of $a + b$ adjacent transpositions. Since the length increases or decreases by one for each factor in such an expression, we get that

$$\ell(\sigma\tau) \equiv a + b \pmod 2.$$

Hence

$$\operatorname{sgn}(\sigma\tau) = (-1)^{a+b} = (-1)^a(-1)^b = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$$

which proves that sgn is a group homomorphism. □

Definition 3.15 (Alternating group)**.** The even permutations form a subgroup A_n of the symmetric group S_n. This subgroup is called the *alternating group on n letters*.

Remark 3.16. Seen in this way, it is clear that $A_n \leq S_n$, since it is the kernel of the homomorphism sgn.

3.1. **Group actions.** For any group G we say that G *acts* on a set X of there is an operation

$$\begin{array}{ccc} G \times X & \longrightarrow & X \\ (g, x) & \longmapsto & g.x \end{array}$$

such that

(1) $(g * h).x = g.(h.x)$, for all $g, h \in G$ and $x \in X$.
(2) $e.x = x$, for all $x \in X$.

Remark 3.17. This is a generalization of the way we look at the symmetric group on X as function on X. The symmetric group on X acts on X by definition.

Theorem 3.18. *An action of G on the set X is equivalent to a group homomorphism $G \to S_X$.*

Proof. If we have a group action, we can define function $G \longrightarrow S_X$ by $g \mapsto \sigma_g$, where σ_g is the permutation given by $\sigma_g(x) = g.x$, $\forall x \in X$. Observe that σ_g is a permutation since $\sigma_g \circ \sigma_{g^{-1}} = \sigma_e = \mathrm{Id}$ by (1) and (2).

On the other hand, given a group homomorphism $\phi : G \longrightarrow S_X$, we can define a group action on X by

$$g.x = \phi(g)(x), \qquad \forall g \in G, \forall x \in X.$$

This is a group action since $e \in G$ is mapped to the identity permutation and

$$(g * h).x = \phi(g * h)(x) = (\phi(g) \circ \phi(h))(x) = \phi(g)(\phi(h)(x)) = g.(h.x).$$

□

Definition 3.19 (Faithful action)**.** The action of G on X is *faithful* if all elements of G corresponds to different permutations, i.e., if the corresponding homommorphism is injective.

Theorem 3.20 (Cayley's theorem)**.** *Any finite group G is isomorphic to a subgroup of a symmetric group.*

Proof. The group G acts on the *set* G by the binary operation. Hence we have a homomorphism $G \longrightarrow S_G$ and in order to conclude the theorem, it is sufficient to see that this is an injective homomorphism, i.e., that the action is faithful. (An injective homomorphism gives an isomorphism between the source and the image.)

Suppose that g and h acts in the same way. Then we have that $g.e = g = h.e = h$, which implies that $g = h$. $\square$

In general, G can be identified with a subgroup of a much smaller symmetric group. The good news in the theorem is that we don't loose any generality by just studying permutation groups, rather than all finite groups.

Definition 3.21 (Orbits)**.** If G acts on X we define the *orbit* of $x \in X$ under G as

$$Gx = \{g.x | g \in G\}.$$

Theorem 3.22. *The action of G on X partitions X into disjoint orbits. In particular we have that $Gx = Gy$ or $Gx \cap Gy = \emptyset$.*

Proof. If $x \in Gy$, we have that $x = h.y$ for some element $h \in G$. Hence we have that

$$Gx = \{g.x|g \in G\} = \{g.(h.y)|g \in G\} = \{gh.y|g \in G\} = \{g.y|g \in Gh\} = \{g.y|g \in G\} = Gy$$

since $Gh = \{gh|g \in G\} = G$.

If $Gx \cap Gy \neq \emptyset$ we can find $g, h \in G$ such that $g.x = h.y$, but this means that $x = g^{-1}.(g.x) = g^{-1}.(h.y) = (g^{-1}h).y \in Gy$. Hence by the above argument $Gx = Gy$.

Any element in x is in some orbit, Gx, which proves that the orbits partition X into disjoint subsets. $\square$

Example 3.23. We can look at the symmetry group G of the cube as acting on different sets:

- The set of six faces. G acts faithfully and we get $G \hookrightarrow S_6$.
- The set of eight corners. G acts faithfully and we get $G \hookrightarrow S_8$.
- The set of twelve edges. G acts faithfully and we get $G \hookrightarrow S_{12}$.
- The set of four diagonals. G acts faithfully and we get $G \hookrightarrow S_4$. Actually, this is an isomorphism.
- The set of three pairs of opposite faces. G does not act faithfully and we get a surjective homomorphism, $G \longrightarrow S_3$.

Recommended excercises

II-8 Groups of Permutations. 28, 29, 30-34, 35, 36, 40-43, 44, 45, 46, 48

II-9 Orbits, Cycles and the Alternating Groups. 20-23, 27, 29, 30, 33, 34, 36, 39

References

[1] J. B. Fraleigh. *A First Course In Abstract Algebra*. Addison Wesley, seventh edition, 2003.