KTH Teknikvetenskap

SF2729 GROUPS AND RINGS
LECTURE NOTES
2011-03-01

MATS BOIJ

6. THE SIXTH LECTURE - GROUP ACTIONS

In the sixth lecture we study what happens when groups acts on sets.[1] Recall that we have already when looking at permutations defined what an action of a group on a set is.

Definition 6.1 (Group action)**.** A *group action* of a group G on a set X is a function

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

satisfying the following conditions:

$i)$ $e.x = x$, for all $x \in X$.
$ii)$ $(ab).x = a.(b.x)$, for all $a, b \in G$ and all $x \in X$.

Example 6.2. There are a number of natural action that we have already met:

- The general linear group $\mathrm{Gl}_n(\mathbb{R})$ acts on the vector space $\mathbb{R}^n$.
- Any group acts on itself by *left multiplication*, $a.b = ab$.
- Any group acts on itself by *conjugation*, $a.b = aba^{-1}$.
- The symmetric group S_X acts on the set X.

We also looked at the following result which shows that the notion of group actions can be seen as a generalization of the notion of symmetric groups.

Theorem 6.3. *An action of G on X is equivalent to a group homomorphism $\Phi : G \longrightarrow S_X$.*

Proof. Given Φ we get the group action by

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

[1]The sixth lecture is based on the sections 16-17 of Chapter III in A First Course in Abstract Algebra [1].

On the other hand, if we have a group action, we may define $\Phi : G \longrightarrow S_X$ by $\Phi(a)(x) = a.x$ for all $a \in G$ and all $x \in X$. The map $\Phi(a) : X \longrightarrow X$ is bijective since $\Phi(a^{-1})$ is the inverse as

$$\Phi(a^{-1})(\Phi(a)(x)) = a^{-1}.(a.x) = (a^{-1}a).x = e.x = x, \quad \forall x \in X.$$

□

Definition 6.4 (Transitive action, faithful action, kernel of action)**.** The action of G on X is said to be *transitive* if for any pair $(x, y) \in X \times X$, there is an element $a \in G$ such that $a.x = y$.

The action of G on X is *faithful* if any two elements $a \neq b$ in G have different actions on X, i.e, if

$$a.x = b.x, \quad \forall x \in X \quad \Longrightarrow \quad a = b.$$

The *kernel* of the action of G on X is given by all $a \in X$ which acts trivially on X, i.e., satisfies $a.x = x$ for all $x \in X$.

Remark 6.5. The kernel of the action of G on X is equal to the kernel of the homomorphism $\Phi : G \longrightarrow S_X$ given by the action. Hence the kernel of the action is a normal subgroup. Furthermore, we have that we get an induced action of $G/\ker\Phi$ on X since the homomorphism $G \longrightarrow S_X$ factors through $G/\ker\Phi$.

Exercise 6.6. *Show that the action is faithful if and only if its kernel is trivial.*

Definition 6.7 (Orbits)**.** For any element $x \in X$, the *orbit of x* under the action of G is given by

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

Exercise 6.8. *Show that the action is transitive if and only if there is a single orbit.*

Theorem 6.9. *The orbits give a partition of X into disjoint subsets.*

Proof. We get an equivalence relation on X by $x \sim y \Leftrightarrow a.x = y$ for some $a \in G$. We check that

$i)$ (reflexivity) $x \sim x$ since $e.x = x$.
$ii)$ (symmetry) $x \sim y \Leftrightarrow a.x = y$ for some $a \in G \Leftrightarrow x = a^{-1}.y$ for some $a \in G \Leftrightarrow y \sim x$.
$iii)$ (transitivity) $x \sim y$ and $y \sim z$ implies that $a.x = y$ and $b.y = z$ for $a, b \in G$, but then $(ba).x = b.(a.x) = b.y = z$ and $x \sim z$.

The equivalence classes under this equivalence relation are the orbits of G on X. □

Definition 6.10 (Stabilizer or Isotropy subgroup)**.** For each element $x \in X$, we define the *stabilizer* of x in G to be

$$G_x = \{a \in G | a.x = x\}.$$

In the text book, the stabilizer of x is called the *isotropy subgroup of* x.

Exercise 6.11. *Show that G_x is in fact a subgroup of G for any $x \in X$.*

Remark 6.12. The kernel of the action is the intersection of all the stabilizers.

Theorem 6.13. *For a given $x \in X$, the non-empty sets*

$$G_{x\to y} = \{a \in G | a.x = y\}$$

are the left cosets of the stabilizer, G_x.

Proof. If $b.x = y$ we have that

$$G_{x\to y} = \{a \in G | a.x = y\} = \{a \in G | a.x = b.x\} = \{a \in G | b^{-1}a \in G_x\} = bG_x.$$

□

Theorem 6.14. $|Gx| = (G : G_x)$ *if the orbit Gx is finite and $|G| = |Gx| \cdot |G_x|$ if G is finite.*

Proof. By the Theorem 6.13, the elements in the orbit of x is in one-to-one correspondence with the left cosets of G_x which proves that their number is the same. The second statement follows from the fact that $(G : G_x) = |G|/|G_x|$ if G is finite. □

Example 6.15. We can use this result in order to compute the order of the general linear group over a finite field $\mathbb{F}_q$. The general linear group $G = \mathrm{Gl}_n(\mathbb{F}_q)$ acts on the finite vector space $\mathbb{F}_q^n$. Look at the stabilizer of the vector $x = (1, 0, \ldots, 0)^t$ under this action.

We get that G_x is given by all the invertible matrices which first column equals x. Hence $|G_x| = q^{n-1}|\mathrm{Gl}_{n-1}(\mathbb{F}_q)|$. Furthermore, G acts transitively on the non-zero vectors of $\mathbb{F}_q^n$. Thus we get from Theorem 6.14 that

$$|\mathrm{Gl}_n(\mathbb{F}_q)| = |Gx| \cdot |G_x| = (q^n - 1)q^{n-1}|\mathrm{Gl}_{n-1}(\mathbb{F}_q)|$$

and by induction, we get

$$|\mathrm{Gl}_n(\mathbb{F}_q)| = q^{n(n-1)/2}\prod_{i=1}^{n}(q^i - 1)$$

We can use the notion of group actions to prove the following partial converse to Lagrange's theorem:

Theorem 6.16. (Cauchy's Theorem) *If p is a prime divisor of the order of G, then G has an element of order p.*

Proof. Let p be a prime divisor of $|G|$ and let X be the set of elements in $G^p = G \times G \times \cdots \times G$ satisfying

$$a_1a_2\cdots a_p = e.$$

The cardinality of X is $|G|^{p-1}$ since we can choose the $p-1$ first elements in arbitrarily and the solve for the last element. Hence $|X| \equiv 0 \pmod p$.

The cyclic group $\mathbb{Z}_p$ acts on X by cyclic permutations of the components since

$$(a_1a_2\cdots a_i)(a_{i+1}\cdots a_p) = e \quad \iff \quad (a_{i+1}a_{i+2}\cdots a_p)(a_1a_2\cdots a_i) = e$$

for all $i = 1, 2, \ldots, p-1$.

The stabilizer of an element is a subgroup of $\mathbb{Z}_p$, which means that it is either trivial or equal to $\mathbb{Z}_p$, since p is a prime. If it is equal to $\mathbb{Z}_p$, the element has to be of the form $(a, a, \ldots, a)$, med $a^p = e$.

The orbits have size one or p by Theorem 6.14. If there was only one orbit, $\{(e, e, \dots, e)\}$ of size 1, we would have that $|X| \equiv 1 \pmod p$, which contradicts $|X| \equiv 0 \pmod p$. Hence there is at least p orbits $\{(a, a, \dots, a)\}$ of size one. Each such element $a \neq e$ has order p. □

As we have seen, any group acts on itself in two natural ways, by *left multiplication* ($a.b = ab$) and by *conjugation* ($a.b = aba^{-1}$). In the case of left multiplication, the action is transitive so there is a single orbit and all the stailizers are trivial.

In the case of conjugation, the orbits are called *conjugacy classes* and the stabilzers G_a are non-trivial apart from when a is in the center $Z(G)$.

Definition 6.17 (Centralizer)**.** For each element a in G, the *centralizer* of a in G is given by

$$C_G(a) = \{b \in G | ab = ba\} = \{b \in G | bab^{-1} = a\}.$$

Theorem 6.18 (**The Class Equation**)**.** *For a finite group G we have that*

$$|G| = |Z(G)| + \sum_{i=1}^{k} \frac{|G|}{|C_G(a_i)|}$$

where $a_1, a_2, \dots, a_k$ are representatives for all the non-trivial conjugacy classes in G.

Proof. G acts on itself by conjugation and we get at partition of G into orbits, which are the conjugacy classes. The elements of the center are in a trivial conjugacy class. The remainder of the elements are in non-trivial conjugacy classes and the size of the conjugacy class containing a is $|G|/|C_G(a)|$ by Theorem 6.14. □

Example 6.19. We can deduce from the class equation that the center of a p-group, i.e., a group of prime power order, is non-trivial. In fact, if p is a prime and $|G| = p^n$, $n > 0$, we have that the left hand side of the class equation is divisible by p. On the other hand, all the terms in the sum on the right hand side are divisible by p since $|C_G(a)| < |G|$ if $a \notin Z(G)$. Hence $|Z(G)|$ is divisible by p and $Z(G)$ is non-trivial.

The following result will help us count the number of orbits when a finite group acts on a finite set. In particular, it will help when counting objects up to symmetries.

Theorem 6.20 (Burnside's Lemma)**.** *If G is a finite group acting on a finite set with r orbits, we have*

$$|G|r = \sum_{a \in G} |X_a|,$$

where $X_a = \{x \in X | a.x = x\}$, for $a \in G$.

Proof. We count the set $S = \{(a, x) | a.x = x\} \subseteq G \times X$ in two ways. Firstly, for each orbit Gx, there is the same number of elements in the stabilizor for each of the elements in the orbit. The contribution from each orbit is $|Gx| \cdot |G_x| = |G|$, which shows that $|S| = r|G|$.

Secondly, we make a sum over all elements $a \in G$ and add the number of elements x fixed by g. In this way, we get that $|S| = \sum_{a \in G} |X_a|$. □

Exercise 6.21. *Count the number of essentially different cubes that can be made with three pairs of identical faces.*

RECOMMENDED EXCERCISES

III-16 Group Action on a Set. 8, 11, 12, 14-16

III-17 Applications of G-Sets to Counting. 1-9

REFERENCES

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