Advanced Algebra I

Group Action

We will define the group action and illustrate some previous known theorem from group action point of view.

Definition 0.1. *We say a group G acts on a set S, or S is a G-set, if there is function $\alpha : G \times S \to S$, usually denoted $\alpha(g, x) = gx$, compatible with group structure, i.e. satisfying:*

(1) *let $e \in G$ be the idetity, then $ex = x$ for all $x \in S$.*
(2) *$g(hx) = (gh)x$ for all $g, h \in G$, $x \in S$.*

By the definition, it's clear to see that if $y = gx$, then $x = g^{-1}y$. Because $x = ex = (g^{-1}g)x = g^{-1}(gx) = g^{-1}y$.

Moreover, one can see that given a group action $\alpha : G \times S \to S$ is equivalent to have a group homomorphism $\tilde{\alpha} : G \to A(S)$, where $A(S)$ denote the group of bijections on S.

Exercise 0.2. *Check the equivalence of α and $\tilde{\alpha}$.*

An application is to take a finite group G of order n, and take $S = G$. Then the group multiplication gives a group action. Thus we have a group homomorphism

$$\tilde{\alpha} : G \to A(G) \cong S_n.$$

One can check that in this case $\tilde{\alpha}$ is an injection. Thus we have the Cayley's theorem.

We now introduce two important notions:

Definition 0.3. *Suppose G acts on S. For $x \in S$, the orbit of x is defined as*

$$\mathcal{O}_x := \{gx | g \in G\}.$$

And the stabilizer of x is defined as

$$G_x := \{g \in G | gx = x\}.$$

Then one has the following

Proposition 0.4.

$$|G| = |\mathcal{O}_x| \cdot |G_x|.$$

Sketch. Consider $S_y := \{g \in G | gx = y\}$. Then G is a disjoint union of S_y for all $y \in \mathcal{O}_x$. Furthermore, fix a g such that $y = gx$, then one has $S_y = gG_x$. Thus

$$|G| = |\cup_{y \in \mathcal{O}_x} S_y| = \sum_{y \in \mathcal{O}_x} |G_x| = |\mathcal{O}_x| \cdot |G_x|.$$

□

By applying this to the situation that $H < G$ is a subgroup and take $S = G/H$ with the action $G \times G/H \to G/H$ via $\alpha(g, xH) = gxH$. For $H \in S$, the stabilizer is H, and the orbit is G/H. Thus we have

$$|G| = |G/H| \cdot |H|,$$

which is the Lagrange's theorem.

Another way of counting is to consider the decomposition of S into disjoint union of orbits. Note that if $\mathcal{O}_x = \mathcal{O}_y$ if and only if $y \in \mathcal{O}_x$. Thus for convenience, we pick a representative in each orbit and let I be a set of representatives of orbits. We have:

$$S = \cup_{x \in I} \mathcal{O}_x.$$

In particular,

$$|S| = \sum_{x \in I} |\mathcal{O}_x|.$$

This simple minded equation actually give various nice application. We have the following natural applications.

Example 0.5 (translation)**.** *Let G be a group. One can consider the action $G \times G \to G$ by $\alpha(g, x) = gx$. Such action is called translation. More generally, let $H < G$ be a subgroup. Then one has translation $H \times G \to G$ by $(h, x) \mapsto hx$. Then $|S| = \sum_{x \in I} |\mathcal{O}_x|$ gives Lagrange theorem again.*

Example 0.6 (conjugation)**.** *Let G be a group. One can consider the action $G \times G \to G$ by $\alpha(g, x) = gxg^{-1}$. Such action is called conjugation. For a $x \in G$, $G_x = C(x)$, the centralizer. And $\mathcal{O}_x = \{x\}$ if and only if $x \in Z(G)$, the center of G. So, for G finite, the equation $|S| = \sum_{x \in I} |\mathcal{O}_x|$ now gives*

$$|G| = \sum_{x \in I} |G|/|C(x)|.$$

Which is the class equation.

The class equation (we mean the general form $|S| = \sum_{x \in I} |\mathcal{O}_x|$) is very useful if the group is a finite p-group. By a finite p-group, we mean a group G with $|G| = p^n$ for some $n > 0$. Consider now G is a finite p group acting on S. Let

$$S_0 := \{x \in S | gx = x, \forall g \in G\}.$$

Then the class equation can be written as

$$|S| = |S_0| + \sum_{x \in I, x \notin S_0} |\mathcal{O}_x|.$$

One has the following

Lemma 0.7. *Let G be a finite p-group. Keep the notation as above, then*

$$|S| \equiv |S_0| \pmod{p}.$$

Proof. If $x \notin S_0$, then $1 \neq |\mathcal{O}_x| = p^k$.

□

By consider the conjugation $G \times G \to G$, one sees that

Corollary 0.8. *If G is a finite p-group, then G has non-trivial center.*

By using the similar technique, one can also prove the important Cauchy's theorem

Theorem 0.9. *Let G be a finite group such that $p \mid |G|$. Then there is an element in G of order p.*

Proof. Let

$$S := \{(a_1, ..., a_p) | a_i \in G, \prod a_i = e\}.$$

And consider a group action $C_p \times S \to S$ by $(1, (a_1, .., a_p)) \mapsto (a_p, a_1, ..., a_{p-1})$. One claims that $S_0 = \{(a, a, ..., a) | a \in G\}$.

By the Lemma, one has $|S| \equiv |S_0| \pmod{.}$ It follows that $p \mid |S_0|$. In particular, $|S_0| > 1$, hence there is $(a, ..., a) \in S_0$ with $a \neq e$. One sees that $o(a) = p$. □