Sep. 29, 2006 (Fri.)

2.3. **group action.**
Group action is one of the most fundamental concept in group theory. There are many situations that group actions appear naturally. The purpose of this section is to develop basic language of group action and apply this to the study of abstract groups.

We will first define the group action and illustrate some previous known theorem as examples.

Definition 2.3.1. *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 2.3.2. *There is a bijection between $\{$group action of G on $S\}$ with $\{$group homomorphism $G \to A(S)\}$.*

Example 2.3.3 (Cayley's Theorem)**.**

Let G be a finite group of $|G| = n$. Then there is an injective homomorphism $G \to S_n$.

To see this, we consider G acts on G via the group operation, i.e. $G \times G \to G$. Thus we have a homomorphism $\varphi : G \to A(G)$.

It's clear that $A(G) = S_n$. It's easy to see that φ is injective. □

This give an example of "permutation representation". That is, represent a group into permutation groups. We gave another example:

Example 2.3.4.

Let $\mathbb{F}_2$ be the field of 2 elements. We would like to see that $GL(2, \mathbb{F}_2) \cong S_3$.

We consider V the 2 dimensional vector space over $\mathbb{F}_2$. There are 3 non-zero vector in V, denoted, $W := \{v_1 := e_1, v_2 := e_2, v_3 := e_1 + e_2\}$. It's clear that $GL(2, \mathbb{F}_2)$ acts on W. Thus we have a representation $GL(2, \mathbb{F}_2) \to A(W) \cong S_3$. One can check that this is indeed an isomorphism. □

We now introduce two important notions:

Definition 2.3.5. *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*

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

It's immediate to check the following:

Lemma 2.3.6. *Given a group G acting on S. For $x, y \in S$, we have:*
1. $G_x < G$.
2. either $\mathcal{O}_x = \mathcal{O}_y$ or $\mathcal{O}_x \cap \mathcal{O}_y = \emptyset$.
3. if $y = gx$, then $G_y = gG_xg^{-1}$.

Proposition 2.3.7.

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

Sketch. For given $y \in \mathcal{O}_x$, we consider $S_y := \{g \in G | gx = y\}$. Then

$$G = \cup_{y \in \mathcal{O}_x} S_y,$$

which is a disjoint union.

Furthermore, for each $y \in \mathcal{O}_x$, we can write $y = gx$. Then one has $S_y = gG_x$. In particular $|S_y| = |G_x|$. We fix a g_y such that $y = g_y x$ once and for all. We may define a bijection $G \to \mathcal{O}_x \times G_x$ as sets by $g \mapsto (gx, g(g_{gx})^{-1})$. Thus

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

□

Corollary 2.3.8 (Lagrange's Theorem)**.** *Let $H < G$ be a subgroup. Then $|G| = |G/H| \cdot |H|$.*

Proof. We 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 a disjoint union:

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

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 2.3.9 (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 $(h, x) \mapsto hx$. In this setting, $\mathcal{O}_x = Hx$. And the set of orbits is G/H, the right cosets of H in G. Then

$$|S| = \sum_{x \in I} |\mathcal{O}_x| = |G/H| \cdot |H|$$

gives Lagrange theorem again. □

Example 2.3.10 (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 of x in G. And $\mathcal{O}_x = \{gxg^{-1} | g \in G\}$ the conjugacy classes of x in G. So in general, we have

$$|G| = \sum_{\text{conj. classes}} |C|,$$

which is the **class equation**.

Now assume that G is finite. The class equation now reads:

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

where I denotes a representative of conjugacy classes.

And $\mathcal{O}_x = \{x\}$ if and only if $x \in Z(G)$, the center of G. So, for G finite, the class equation now gives

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

Which is the usual form of class equation. □

The class equation is very useful if the group is a finite p-group. We recall some definition

Definition 2.3.11. *If p is a prime, then a p-**group** is a group in which every element has order a power of p.*
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 2.3.12. *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 $1 \neq |\mathcal{O}_x| = p^k$ because $|G| = |\mathcal{O}_x| \cdot |G_x|$. □

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

Corollary 2.3.13. *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 2.3.14 (Cauchy)**.** *Let G be a finite group such that $p \mid |G|$. Then there is an element in G of order p.*

sketch. We keep the notation as in Lemma 2.3.12. Let

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

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

By the Lemma, one has $|S| \equiv |S_0| \pmod{p}$. 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 $o(a) = p$. □

Corollary 2.3.15. *A finite group G is a p-group if and only it is a finite p-group.*

2.4. **Sylow's theorems.** We are now ready to prove Sylow theorems. The first theorem regards the existence of p-subgroups in a given group. The second theorem deals with relation between p-subgroups. In particular, all Sylow p-subgroups are conjugate. The third theorem counts the number of Sylow p-subgroups.

Theorem 2.4.1 (First Sylow theorem)**.** *Let G be a finite group of order $p^n m$ (where $(p, m) = 1$). Then there are subgroups of order p^i for all $0 \leq i \leq n$.*

Furthermore, for each subgroup H_i of order p^i, there is a subgroup H_{i+1} of order p^{i+1} such that $H_i \lhd H_{i+1}$ for $0 \leq i \leq n-1$.

In particular, there exists a subgroup of order p^n, which is maximal possible, called Sylow p-subgroup. We recall the useful lemma which will be used frequently.

Lemma 2.4.2. *Let G be a finite p-group. Then*

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

proof of the theorem. We will find subgroup of order p^i inductively. By Cauchy's theorem, there is a subgroup of order p. Suppose that H is a subgroup of order p^i. Consider the group action that H acts on

$S = G/H$ by translation, i.e. $H \times G/H \to G/H$ by $h(xH) := hxH$. One shows that $xH \in S_0$ if and only if $xH = hxH$ for all $h \in H$ if and only if $x \in N_G(H)$. Thus $|S_0| = |N_G(H)/H|$.

If $i < n$, then

$$|S_0| \cong |S| = p^{n-i}m \equiv 0 \pmod{p}.$$

By Cauchy's theorem, the group $N_G(H)/H$ contains a subgroup of order p. The subgroup is of the form H_1/H, hence $|H_1| = p^{i+1}$. Moreover, $H \lhd H_1$. □

Example 2.4.3. *If G is a finite p-group of order p^n, then one has a series of subgroups $\{e\} = H_0 < H_1 < ... < H_n = G$ such that $|H_i| = p^i$ and $H_i \lhd H_{i+1}, H_{i+1}/H_i \cong \mathbb{Z}_p$. In particular, G is solvable.*

Definition 2.4.4. *A subgroup P of G is a Sylow p-subgroup if P is a maximal p-subgroup of G.*

If G is finite of order $p^n m$ then a subgroup P is a Sylow p-subgroup if and only if $|P| = p^n$ by the proof of the first theorem.

Theorem 2.4.5 (Second Sylow theorem)**.** *Let G be a finite group of order $p^n m$. If H is a p-subgroup of G, and P is any Sylow p-subgroup of G, then there exists $x \in G$ such that $xHx^{-1} < P$.*

Proof. Let $S = G/P$ be the set of left cosets and H acts on S by translation. Thus by Lemma 2.3.12, one has $|S_0| \equiv |S| = m \pmod{p}$. Therefore, $S_0 \neq \emptyset$. One has

$$xP \in S_0 \Leftrightarrow hxP = xP \quad \forall h \in H \Leftrightarrow x^{-1}Hx < P.$$

This completes the proof. □

An immedaitely but important consequence is that any two Sylow p-subgroups are conjugate.

Theorem 2.4.6 (Third Sylow theorem)**.** *Let G be a finite group of order $p^n m$. The number of Sylow p-subgroups divides $|G|$ and is of the form $kp + 1$.*

Proof. Let S be the conjugate class of a Sylow p-subgroup P (this is the same as the set of all Sylow p-subgroups). We consider the action that G acts on S by conjugation, then the action is transitive, i.e. for any $x, y \in S$, there exists $g \in G$ such that $y = gx$. In particular $\mathcal{O}_x = S$. Hence $|S| \mid |G|$ for $|G| = |G_x| \cdot |\mathcal{O}_x|$.

Furthermore, we consider the action $P \times S \to S$ by conjugation. Then

$$Q \in S_0 \Leftrightarrow xQx^{-1} = Q \quad \forall x \in P \Leftrightarrow P < N_G(Q).$$

Both P, Q are Sylow p-subgroup of $N_G(Q)$ and therefore conjugate in $N_G(Q)$. However, $Q \lhd N_G(Q)$, Q has no conjugate other than itself. Thus one concludes that $P = Q$. In particular, $S_0 = \{P\}$. By Lemma 2.3.12, one has $|S| = 1 + kp$. □

Example 2.4.7.

Group of order 200 must have normal Sylow subgroups. Hence it's not simple. To see this, let $r_p :=$ number of Sylow p-subgroups. Then $r_5 = 1$. So if P is a Sylow 5-subgroup. Since gPg^{-1} is also a Sylow subgroup, it follows that $gPg^{-1} = P$ for all $g \in G$. Thus $P \lhd G$. □

Example 2.4.8.

There is no simple group of order 36. To see this, we consider P a Sylow 3-subgroup. Then $r_3 = 1$ or 4. In case that $r_3 = 4$, let S be the set of Sylow 3-subgroups. We have a group action $G \times S \to S$ by conjugation. Thus we have a group homomorphism $\varphi : G \to A(S) \cong S_4$. Comparing the cardinality of groups, one sees that φ must have non-trivial kernel. Hence G is not simple. □

2.5. **groups of small order.** We can use the technique developed in the previous sections to study group of small order in more detail.

First of all, as a direct consequence of Cauchy's theorem,

Proposition 2.5.1. *Let p be a prime. A group of order p is cyclic.*

Example 2.5.2.

Classify groups of order $2p$.

If $p = 2$, then this is well-known. So we may assume that $p > 2$. First of all there is a subgroup $H < G$ of order p, generated by x, by Cauchy's theorem. By Sylow's third theorem, we have $r_p = 1$, hence H is normal. Similarly, there is an element of order 2, say y. By normality of H, we have $yxy^{-1} = x^k$ for some k. Since

$$x = y^2xy^{-2} = yx^ky^{-1} = x^{k^2},$$

it follows that $k^2 \equiv 1(\mod p)$. Hence $k \equiv 1$ or $\equiv -1$.

Case 1. $k \equiv 1$, then $xy = yx$. It follows that G is abelian. By chinese Remainder Theorem, G is cyclic.

Case 2. $k \equiv -1$, then $xy = yx^{-1}$. These kind of group is called **dihedral groups**, denoted D_{2p}. □

Example 2.5.3.

Let p, q be primes. If $|G| = pq$, then its structure can be determined similarly.

We assume that $p > q$. Then there are $x, y \in G$ of order p, q respectively. Moreover, $H :=< x > \lhd G$. We have $yxy^{-1} = x^k$ for some k. Since

$$x = y^qxy^{-q} = yx^ky^{-1} = x^{k^q},$$

it follows that $k^q \equiv 1(\mod p)$. Now the situation depends on the structure of $\mathbb{Z}_p^*$. Recall that $\mathbb{Z}_p^* \cong \mathbb{Z}_{p-1}$ is cyclic.

Case 1. $q \nmid p - 1$, then $k^q \equiv 1(\mod p)$ implies that $k \equiv 1$. Hence $xy = yx$. It follows that G is abelian. By chinese Remainder Theorem,

G is cyclic.
Case 2. $q \mid p-1$, then $k^q \equiv 1(\mod p)$ has q solutions, $k \equiv a, a^2, ..., a^{q-1}, a^q \equiv 1$. If we pick $k \equiv a$, then we determined a group G_1 which is generated by x_1, y_1 with $y_1 x_1 y_1^{-1} = x_1^a$. If we pick $k \equiv a^2$, then we determined a group G_2 which is generated by x_2, y_2 with $y_2 x_2 y_2^{-1} = x_2^{a^2}$. Note that the map $\varphi : G_2 \to G_1$ by $\varphi(y_2) = y_1^2, \varphi(x_2) = x_1$ gives an isomorphism. Therefore, for different solution $k \equiv a, a^2, ..., a^{q-1}$, they determined the same group. □

There is a useful construction to produce groups from simple ones called **semi-direct product** which we now introduce. Given two groups G, H and a homomorphism $\theta : H \to \mathrm{Aut}(G)$. Let $G \times_\theta H$ be the set $G \times H$ with the binary operation $(g,h)(g',h') = (g(\theta(h)(g')), hh')$. One can verify that this produce a group.

For example, in the case 2 of above example, we have $G = \mathbb{Z}_p, H = \mathbb{Z}_q$ and we consider $\theta : \mathbb{Z}_q \to \mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_p^*$ by $\theta(1) = a$. Then we obtained $\mathbb{Z}_p \times_\theta \mathbb{Z}_q$. Such group is called a **metacyclic groups**.

Proposition 2.5.4. *Let p be a primes. If $|G| = p^2$, then G is abelian.*

We will discuss the structure of finite ableina groups later. In principle, their structure are pretty easy.

sketch. By class equation, one sees that $Z(G)$ is non-trivial.
Case 1. if $|Z(G)| = p^2$, then G is abelian.
Case 2. if $|Z(G)| = p$, then $G/Z(G)$ is a group of order p , hence cyclic. We pick $x \in G$ such that $G/Z(G)$ is generated by $xZ(G)$. We also pick $y \in G$ such that $Z(G)$ is generated by y. It's easy to check that G is generated by x, y. Note that $xy = yx$, it follows that G is abelian. □

Using above properties, one can classified groups of order ≤ 15 completely unless for order 8 and 12. In fact groups of order 8 are either abelian or D_8 or Q_8. Where Q_8 is the quaterion group defined by $\{i, j, k, -i, -j, -k, 1, -1 | i^2 = j^2 = k^2 = -1, ijk = -1\}$.

Easy example of non-abelian groups of order 12 includes A_4, D_{12}. In fact there is one more, $T =< a, b | a^6 = b^4 = 1, b^2 = a^3 = (ab)^2 >$.

Theorem 2.5.5. *every non-abelian group G of order 12 is isomorphic to A_4, D_{12} or T.*

sketch. Let P be a Sylow 3-subgroup. We first consider the action $G \times G/P \to G/P$ by translation. It gives rise to a homomorphism $\varphi : G \to A(G/P) \cong S_4$. It's clear that $\ker(\varphi) < P$.
Case 1. $\ker(\varphi) = \{e\}$, then $G \cong A_4$.
Case 2. $\ker(\varphi) = P$. Then we need to wok harder. So now, $P \lhd G$ and P is the unique Sylow 3-subgroup. Let $P = \{x, x^2, x^3 = e\}$, then x, x^2 are the only element in G of order 3.

Let K be a Sylow 2-subgroup, then K is either V_4 or $\mathbb{Z}_4$.
Case 2.i. If $K \cong V_4$, by computing the relation between generators,

one can show that $G \cong D_{12}$.
Case 2.ii. If $K \cong \mathbb{Z}_4$, by computing the relation between generators, one can show that $G \cong T$.

□

Groups of order p^n, $n \geq 3$ could be very complicated. Here just give two more examples.

Example 2.5.6.

Let $G < GL(2, \mathbb{C})$ be the group generated by $A = \begin{pmatrix} 0 & \omega \\ \omega & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, where ω is a primitive 2^{n-1}th root of unity for $n \geq 3$. Then G is a group of order 2^n. □

Example 2.5.7.

Let $G < GL(3, \mathbb{C})$ be the group generated by $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$, where ω is a primitive 3th root of unity. Then G is a group of order 27. □