Group actions in theory of finite groups

Jitender Singh
Department of Mathematics, Guru Nanak Dev University,
Amritsar-143005, Punjab, INDIA
sonumaths@gmail.com

Abstract

Using group action as a tool, we describe some standard results such as generalized Cayley theorem, Class equation, Lagrange theorem, Cauchy theorem, and Sylow theorems which are central in the theory of finite groups. Group actions arise on many occasions in Mathematics; so we feel that, getting familiarity with them is essential and should start at undergraduate learning.

1 Group action

Let G be a group and X be a nonempty set. A group action is a map $\bullet : G \times X \to X$ that satisfy (1) $g_1 \bullet (g_2 \bullet x) = (g_1 g_2) \bullet x \ \forall\ g_1, g_2 \in G, x \in X$ and (2) $1_G \bullet x = x$ for all $x \in X$. Here $g \bullet x := \bullet(g, x)$ and, this new notation is convenient to deal with group actions. If $\bullet : G \times X \to X$ is a group action, we say that the group G acts on the set X. As an example, let $g \bullet x = x$ for all $g \in G$ and $x \in X$. Then $g_1 \bullet (g_2 \bullet x) = g_1 \bullet (x) = x = (g_1 g_2) \bullet x$. Also $1_G \bullet x = x$. Thus $\bullet$ is a group action. Similarly it can be easily seen that the binary operation of the group G itself is a group action! If S_X denote symmetric group consisting of all bijections of a set $X = \{1, ..., n\}$ then S_X acts on X via $\sigma \bullet k = \sigma(k)$.

Group actions arise quite frequently in Mathematics and are not limited to abstract algebra. For example every linear system of ODEs in $\mathbb{R}^n$ is defined

by $\frac{dX}{dt} = A \bullet X = AX$ where $X \in \mathbb{R}^n, A \in GL_n(\mathbb{R})$ using action of $GL_n(\mathbb{R})$ on $\mathbb{R}^n$ via matrix multiplication. Here the orbit $\mathcal{O}_X$ is called the phase space. Also the action of $\mathbb{R}$ on $GL_n(\mathbb{R})$ gives a solution to this linear system via $t \bullet A = \exp\{At\} := I + \sum_{k=1}^{\infty} \frac{A^k t^k}{k!}$.

1.1 Cayley theorem

At the first place, we note that the map $\bullet : G \times X \to X$ is a group action if and only if the map $\Psi : G \to S_X$ defined by $\Psi(g)(x) = \sigma_g(x) = g \bullet x$ is a group homomorphism. This simple fact leads to the Cayley's theorem.

Theorem 1.1. *(Cayley) Every group is isomorphic to a subgroup of some symmetric group.*

Proof. Let G be a group and S_G be its symmetric group. Then the binary operation of G as an action of G on itself induces a homomorphism $\Psi : G \to S_G$ by $\Psi(g) := \sigma_g$ such that $\sigma_g : G \to G$ is a bijection and for all $x \in G$, $\sigma_g(x) := g \bullet x := gx$. To show that Ψ is injective, let $\Psi(g_1) = \Psi(g_2)$ then for all $x \in G$, $\sigma_{g_1}(x) = \sigma_{g_2}(x) \ \Rightarrow \ g_1 x = g_2 x$ which directly gives $g_1 = g_2$. Hence by first isomorphism theorem $G \cong \Psi(G) \leq S_G$. □

Infact a generalization of the Cayley theorem can be easily understood via group actions. This is the next result.

Theorem 1.2. *(Generalized Cayley theorem) Let $H \leq G$. Then there is a homomorphism $\Psi : G \to S_{G/H}$ such that $\ker \Psi \leq H$ and for all $K \trianglelefteq G$, such that $K \leq H$ then $K \leq \ker \Psi$. The case $H = \{1_G\}$ is the Cayley theorem.*

Proof. Define $\Psi : G \to S_{G/H}$ by $\Psi(g) = \sigma_g$ s.t. $\sigma_g(xH) = g \bullet (xH) = (gx)H$. Then clearly Ψ is a homomorphism with $\ker \Psi := \cap_{x \in G} xHx^{-1} \subseteq H$. Finally if $K \trianglelefteq G$ such that $K \leq H$ then $K = xKx^{-1} \subseteq xHx^{-1}$, $\forall x \in G$ hence $K \leq \cap_{x \in G} xHx^{-1} = \ker \Psi$. □

The generalized Cayley's theorem enables us a test for checking non-simplicity of a finite group. In view of this, if $H \leq G$ such that $|G|$ does not divide $|G/H|!$, then H contains a nontrivial normal subgroup of G because then $[G : \ker \Psi]$ divides $|G/H|!$ which forces $|\ker \Psi| > 1$.
If G is simple nonabelian such that G has a subgroup of index n. As Ψ is nontrivial, it follows that $|\ker \Psi| = 1$. Therefore $G \hookrightarrow S_{G/H}$. As G is simple and the standard map sign : $S_{G/H} \to \mathbb{Z}_2$ is a group homomorphism, so is the restriction $\text{sign}|_{\Psi(G)}$. It follows by simplicity of $\Psi(G)$ that sign is not surjective. Hence $G \cong \Psi(G) \leq A_n$. This observation can be used to prove that there does not exist a nonabelian simple group of order 80; if so then by Sylow's first theorem, such a group has a subgroup of index 5, which by previous discussion gives G embedded in A_5 but then by Lagrange's theorem 80 must divide $5! = 120$ a contradiction.

1.2 Orbit-stabilizer theorem

Definition: (Orbit and Stabilizer) Let $\bullet : G \times X \to X$ be a group action. For any $x \in X$ the set $\mathcal{O}_x := \{g \bullet x \mid g \in G\}$ is called orbit of x in X and the set $\text{Stab}(x) := \{g \in G \mid g \bullet x = x\}$ is called stabilizer of x.

If we define a relation $\sim$ on X as follows: $x \sim y$ if there is a $g \in G$ such that $y = g \bullet x$. It is easy to see that $\sim$ is an equivalence relation with each equivalence class $[x] = \mathcal{O}_x$ for all $x \in X$. It follows that the set of all orbits in X is a partition of X. Also for $x \in X$, $|\text{Stab}(x)| = |g\text{Stab}(x)|$ and that $G/\text{Stab}(x) \leq G$. Consequently the map $f : G/\text{Stab}(x) \to \mathcal{O}_x$ sending $g\text{Stab}(x) \mapsto g \bullet x$ is bijective. This discussion proves the following nice relationship called the 'orbit-stabilizer theorem'.

Theorem 1.3. *(Orbit-stabilizer) Let a finite group G acts on a set X. Then for any $x \in X$, $|G| = |\mathcal{O}_x||Stab(x)|$.*

We demonstrate use of orbit-stabilizer theorem in obtaining the order of group G of symmetry preserving rigid rotations of a cube in $\mathbb{R}^3$ with its

bounding faces parallel to the coordinate planes. Identifying the six faces of the cube by six numbers $1, ..., 6$, G acts on the set $\{1, ..., 6\}$ via $g \bullet k =$'rotation of the face k by an angle $\theta = \frac{n\pi}{2},\ n \in \mathbb{Z}$.' Here we assume that face k is the top horizontal face of the cube. Note that two kind of rotations are possible; (1) a horizontal rotation r_{hk} by an angle in multiple of $\pi/2$ and (2) a vertical rotation r_{vk} by an angle in multiple of $\pi/2$. A rotation by 2π is the identity rotation, therefore $r_{hk}^4 = r_{vk}^4 = 1_G$. With these considerations, we observe that $\mathcal{O}_k = \{r_{hk}, r_{hk}^2, r_{hk}^3, r_{vk}, r_{vk}^2, r_{vk}^3\}$ and $\mathrm{Stab}(k) = \langle r_{hk} \rangle$. By orbit stabilizer theorem, we see that $|G| = |\mathcal{O}_k||\mathrm{Stab}(k)| = 6 \times 4 = 24$.

1.3 Class equation, Lagrange, and Cauchy

The class equation can be obtained as an easy consequence of the action of finite group G on itself via conjugation i.e. $g \bullet x = gxg^{-1}$ such that for any $x \in Z(G)$, $\mathcal{O}_x = \{x\}$ and for $y \in G$, $\mathrm{Stab}(y) = C_G(y)$ the centralizer of y in G. By orbit stabilizer theorem $|G| = |\mathcal{O}_x||C_G(x)|$. As G =disjoint union of orbits, this gives the class equation

$$|G| = \sum_{\mathcal{O}_x = \{x\}} |O_x| + \sum_{\mathcal{O}_x \neq \{x\}} |O_x| = |Z(G)| + \sum_{x \notin Z(G)} \frac{|G|}{|C_G(x)|}.$$

Group action can be used to prove the Lagrange theorem i.e. *for any subgroup H of a finite group G, $|H|$ divides $|G|$*. Let us see this now! Define $\bullet : G \times G/H \to G/H$ by $g \bullet (xH) = (gx)H$. Then $\bullet$ is a group action and by the orbit stabilizer theorem $|G| = |\mathcal{O}_H||\mathrm{Stab}(H)|$ where we note that $\mathcal{O}_H = G/H$ and $\mathrm{Stab}(H) = H$ q.e.d. A partial converse of the Lagrange theorem called Cauchy theorem can also be dealt via group action as we see next.

Theorem 1.4. *(Cauchy) Let G be a finite group and p is a prime divisor of $|G|$. Then G has an element of order p.*

Proof. Let $S = \{(x_1, ..., x_p) \mid x_i \in G,\ \&\ x_1 \cdots x_p = 1\}$. Then a $p-$tuple $(x_1, ..., x_p) \in S$ if and only if each $x_i \in G$ and $x_p = (x_1 \cdots x_{p-1})^{-1}$. This

enables easy calculation for $|S|$. Clearly each of the first $p-1$ components in any element of S can be selected from any of the members of G and the last $p-$the component is fixed, therefore $|S| = \underbrace{|G| \times \cdots \times |G|}_{(p-1)-\text{times}} \times 1 = |G|^{p-1}$.
Let $H = \langle (12...p) \rangle$ be the subgroup of the permutation group S_p consisting of all cyclic permutations of $\{1, ..., p\}$. Under the action of H on S define by

$$\sigma \bullet (x_1, ..., x_p) = (x_{\sigma(1)}, ..., x_{\sigma(p)})$$

we obtain a partition of S consisting of all orbits in S. For each $x = (x_1, ..., x_p) \in S$, $\mathcal{O}_x := \{\sigma \bullet x \mid \sigma \in H\}$. Note that $|\mathcal{O}_x| = 1$ if and only if $\sigma \bullet x = x \forall \sigma \in H \Leftrightarrow x_1 = x_{\sigma(1)} = x_{\sigma^2(1)} \cdots = x_{\sigma^{p-1}(1)}$ such that $1 \neq \sigma(1) \neq \sigma^2(1) \cdots \neq \sigma^{p-1}(1)$. It follows that $x = (a, ..., a)$ for some $a \in G$. If $|\mathcal{O}_x| > 1$ then clearly $|\mathcal{O}_x| = p$ since $|\text{Stab}(x)| = 1$. Therefore

$$|S| = |G|^{p-1} = k + pd$$

where k is the number of singleton orbits and d is the number of orbits with $p-$elements each. Clearly p divides k which shows that $k \geq p \geq 2$ and that there is a singleton orbit other than $\{(1, ..., 1)\}$ let it be $\{(a, ..., a)\}$ for some $a \in G$ s.t. $a \neq 1_G$, then $a^p = 1$ and hence $|a| = p$. □

2 Sylow theorems

We start with the following standard result in number theory.

Lemma 2.1. *If p is a prime and r and m be positive integers such that p^r divides m but p^{r+1} does not divide m then p^{r+1} does not divide ${}^{p^\alpha m}C_{p^\alpha}$ for all positive integers α.*

Proof. Note that ${}^{p^\alpha m}C_{p^\alpha} = m \prod_{i=1}^{p^\alpha - 1} \frac{p^\alpha m - i}{p^\alpha - i}$, and for each i the highest power of p that divides $p^\alpha m - i$ and $p^\alpha - i$ is same therefore factors out of $\prod_{i=1}^{p^\alpha - 1} \frac{p^\alpha m - i}{p^\alpha - i}$

and p does not divide this product. Hence the highest power of p dividing ${}^{p^\alpha m}C_{p^\alpha}$ and m is the same. The assertion follows now. □

Definition: (Sylow$-p-$subgroup) Let G be a finite group and p be a prime such that p^α divides $|G|$. Then a subgroup of G of order p^α is called a $p-$subgroup of G. A $p-$subgroup of order p^α such that $p^{\alpha+1}$ does not divide $|G|$ is called a Sylow$-p-$subgroup of G.

Theorem 2.2. *(Sylow's 1st theorem) Let G be a finite group of order n. If p is a prime such that p^α divides n for some positive integer α then G has a subgroup of order p^α.*

Proof. Let $|G| = p^\alpha m$ and r be a positive integer such that p^r divides m but p^{r+1} does not divide m. Let $\mathcal{M}$ be the set of all subsets of G each having p^α elements. We note that $|\mathcal{M}| = {}^{p^\alpha m}C_{p^\alpha}$ and under the action of G on set $\mathcal{M}$ defined by $g \bullet M = gM$, $\mathcal{M}$ is equal to disjoint union of its orbits. With this we obtain

$$ {}^{p^\alpha m}C_{p^\alpha} = |\mathcal{M}| = \sum_{M\in\mathcal{M}} |\mathcal{O}_M| = \sum_{M\in\mathcal{M}} \frac{|G|}{|\mathrm{Stab}(M)|}. $$

Now by preceding lemma 2.1, highest power of p dividing $\displaystyle\sum_{M\in\mathcal{M}} \frac{|G|}{|\mathrm{Stab}(M)|}$ is p^r. Therefore, there must be one term in this summation which is not divisible by p^{r+1}. Let this corresponds to $M_1 \in \mathcal{M}$. Define $H := \mathrm{Stab}(M_1) \leq G$. we will prove that $|H| = p^\alpha$. Since by orbit-stabilizer theorem $|G| = |\mathcal{O}_{M_1}||H|$ and, highest power of p dividing $|G|/|\mathcal{O}_{M_1}|$ is p^α, it follows that $|H| \geq p^\alpha$. For reverse inequality, fix a $m \in M_1$ then

$$ Hm := \{xm, x \in G \mid x \bullet M_1 = xM_1 = M_1\} \subseteq M_1 $$

since each element of Hm is of the form $xm \in xM_1 = M_1$ i.e. $xm \in M_1$. Therefore $|H| = |Hm| \leq |M_1| = p^\alpha$. This proves that G has a subgroup H such that $|H| = p^\alpha$. □

Theorem 2.3. *(Sylow's 2nd theorem). Any two Sylow-p-subgroups of G are conjugate.*

Proof. Let A and B be two distinct Sylow$-p-$subgrops of G such that $|A| = |B| = p^r$ such that p^{r+1} does not divide $|G|$. Define a set $X := \{AxB \mid x \in G\}$ where $AxB := \{axb \mid a \in A,\ b \in B\}$. Then under the action of G on X defined by $g \bullet (AxB) := A(gx)B$, X is equal to disjoint union of orbits. Since highest power of p dividing $|G|$ is r, it follows that there is at least one $x \in G$ for which p^{r+1} does not divide $|\mathcal{O}_{AxB}|$. As $\mathcal{O}_{AxB} = X$ and $\text{Stab}(AxB) := \{g \in G \mid AgxB = AxB\} = AxBx^{-1}$(check this!), we have

$$|G| = |\mathcal{O}_{AxB}||\text{Stab}(AxB)| = |X|\frac{|A||xBx^{-1}|}{|A \cap xBx^{-1}|}$$

Since $|A| = p^r = |B|$ therefore $|A \cap xBx^{-1}| = p^\alpha$ for some nonnegative integer $\alpha < r$. We see that $|G| = |X|p^{2r-\alpha}$. It follows that $2r - \alpha \leq r$ or $r \leq \alpha$ which is possible only when $\alpha = r$. Hence $|A \cap xBx^{-1}| = p^r = |A|$ which implies that $A \cap xBx^{-1} = A$ or $A \subseteq xBx^{-1}$ i.e. $A = xBx^{-1}$. This proves that A is conjugate to B. □

Theorem 2.4. *(Sylow's 3rd theorem) The number n_p of Sylow$-p-$subgroups of G satisfies the following. n_p divides $[G : N_G(H)]$, $n_p \equiv 1 \mod p$ where H denotes a Sylow$-p-$subgroup of G.*

Proof. Let $|H| = p^r$. Define $Y := \{xHx^{-1} \mid x \in G\}$ as the set of all conjugates of H in G which by Sylow's 2nd theorem, consists of all the Sylow$-p-$subgroups of G. Under the action of G on the set Y defined by

$$g \bullet (xHx^{-1}) := g(xHx^{-1})g^{-1} = (gx)H(gx)^{-1}$$

we have by orbit stabilizer theorem $|G| = |\mathcal{O}_H||\text{Stab}(H)| = |Y||N_G(H)|$ from which it follows that $n_p = |Y| = [G : N_G(H)]$. For the remaining part, we consider the action of the group $H \times H$ on G defined by

$$(h_1, h_2) \bullet x = h_1 x h_2^{-1}.$$

Under this action, for any $x \in G$, $\mathcal{O}_x = \{h_1 x h_2^{-1} \mid h_1, h_2 \in H\} = HxH$. Also note that for $x \in N_G(H)$, $\mathcal{O}_x = HxH = xH$ which is a left coset of H in $N_G(H)$. Thus we get

$$|G| = \sum_{x \in G} |\mathcal{O}_x| = \sum_{x \in N_G(H)} |xH| + \sum_{x \notin N_G(H)} |HxH| = |N_G(H)| + \sum_{x \notin N_G(H)} |HxHx^{-1}|$$

since $\sum_{x \in N_G(H)} |xH| = |N_G(H)|$ and the map $hxh' \mapsto hxh'x^{-1}$ is a bijection i.e. $|HxH| = |HxHx^{-1}|$. So we have

$$|G| = |N_G(H)| + \sum_{x \notin N_G(H)} \frac{|H||xHx^{-1}|}{|H \cap xHx^{-1}|} = |N_G(H)| + \sum_{x \notin N_G(H)} p^{2r-\alpha}$$

where $|H \cap xHx^{-1}| = p^\alpha$ for some $\alpha < r$ since $H \neq xHx^{-1}$. Also as $H \leq N_G(H)$ the highest power of p dividing $|N_G(H)|$ is p^r. Consequently $\sum_{x \notin N_G(H)} p^{2r-\alpha} = kp^{r+1}$ for some positive integer k and

$$\frac{|G|}{|N_G(H)|} = n_p = 1 + \frac{kp^{r+1}}{|N_G(H)|} \equiv 1 \mod p.$$

This completes the proof. □

Remark: 2nd part of the Sylow's 3rd theorem can be proved using action of $N_G(H)$ on the set Y via conjugation i.e. $s \bullet (xHx^{-1}) = (sx)H(sx)^{-1}$. Then $\mathcal{O}_{xHx^{-1}} = \{(sx)H(sx)^{-1} \mid s \in N_G(H)\} = H$ if $x \in N_G(H)$. Also $\text{Stab}(xHx^{-1}) = \{s \in N_G(H) \mid s \bullet (xHx^{-1}) = s(xHx^{-1})s^{-1} = xHx^{-1}\} = N_{N_G(H)}(xHx^{-1}) = N_G(H) \cap N_G(xHx^{-1})$. Therefore

$$n_p = |Y| = 1 + \sum_{x \notin N_G(H)} \frac{|N_G(H)|}{|N_G(H) \cap N_G(xHx^{-1})|} \quad \text{or} \quad n_p \equiv 1 \mod p$$

where we now show that each term under the summation is divisible by p. We first claim that for all $x \in G - N_G(H)$, $H \nsubseteq N_G(xHx^{-1})$ otherwise if $H \subseteq N_G(xHx^{-1})$ then $HxHx^{-1}$ is a subgroup of G where p^{r+1} divides $|HxHx^{-1}|$ which is a contradiction. Similarly $xHx^{-1} \notin N_G(H)$. Therefore highest power of p dividing $|N_G(H) \cap N_G(xHx^{-1})|$ is $\leq p^{r-1}$ where as $p^r = |H|$ divides $|N_G(H)|$. Consequently p divides $\dfrac{|N_G(H)|}{|N_G(H) \cap N_G(xHx^{-1})|}$.

Sometimes the following more general result is also known as the Sylow's second theorem.

Theorem 2.5. *Let G be a finite group. Then every $p-$subgroup of G is contained in some Sylow$-p-$subgroup of G.*

Proof. Let P be a Sylow$-p-$subgroup of G and H be a subgroup of G whose order is a power of p. Consider the action of H on the set $X := \{xPx^{-1} \mid x \in G\}$ via conjugation i.e. $h \bullet (xPx^{-1}) = (gx)P(gx)^{-1}$. Under this action $|\mathcal{O}_{xPx^{-1}}||\text{Stab}(xPx^{-1})| = |H|$ therefore $|\mathcal{O}_{xPx^{-1}}|$ is a power of p. Also $n_p = |X| = \sum_{x\in G} |\mathcal{O}_{xPx^{-1}}|$ is not divisible by p, therefore there is at least one $y \in G$ for which p does not divide $|\mathcal{O}_{yPy^{-1}}|$, the only possibility is

$$|\mathcal{O}_{yPy^{-1}}| = 1.$$

Then $H = \text{Stab}(yPy^{-1}) := \{g \in H \mid g(yPy^{-1})g^{-1} = yPy^{-1})\} \leq N_H(yPy^{-1})$.
Claim. *if $z \in N_H(yPy^{-1})$ such that $|z| = p^j$ for some positive integer j, then $z \in yPy^{-1}$.* To prove the claim, note that

$$[G : N_G(yPy^{-1})][N_G(yPy^{-1}) : yPy^{-1}] = [G : yPy^{-1}]$$

which shows that p does not divide $[N_G(yPy^{-1}) : yPy^{-1}] \geq [N_H(yPy^{-1}) : yPy^{-1}]$. Thus p does not divide $[N_H(yPy^{-1}) : yPy^{-1}]$. Consider the quotient group $N_H(yPy^{-1})/(yPy^{-1}) \ni z(yPy^{-1})$, then

$$(z(yPy^{-1}))^{p^j} = z^{p^j}(yPy^{-1}) = (yPy^{-1})$$

which shows that $|z(yPy^{-1})|$ divides p^j and also $|z(yPy^{-1})|$ divides $[N_H(yPy^{-1}) : yPy^{-1}]$. The only possibility is $|z(yPy^{-1})| = 1$ i.e. $z \in (yPy^{-1})$. This proves the claim.
Now as $H \leq N_H(yPy^{-1})$, and since every element of H is of the order equal to a power of p, by the above claim, it follows that $H \subseteq yPy^{-1}$. □

Corollary 2.6. *Any two Sylow$-p-$subgroups are conjugates.*

3 Semidirect Product

Now we study a generalization of the direct product of two groups. The recognition theorem on direct product of subgroups says that if H, K are two subgroups of a group G such that $H \trianglelefteq G$ and $K \trianglelefteq G$ and $H \cap K = \{1\}$; then $HK \cong H \times K$. Is there a recognition theorem to characterize the subgroup HK of G? Answer is yes and leads to a new product called 'semidirect product' of the groups H and K.

Remark: Let G be a group and $H \trianglelefteq G,\ K \leq G$ such that $H \cap K = \{1_G\}$. Then $HK \leq G$ and every element of HK can be written uniquely as $hk,\ h \in H$ and $k \in K$. So there is a bijection between the sets HK and the set $H \times K$. We would like to define a multiplication rule in the set $H \times K$ so that the bijection between HK and $H \times K$ becomes a homomorphism. Then for all $h_1, h_2 \in H$ and $k_1, k_2 \in K$ we have

$$h_1k_1h_2k_2 = h_1 \underbrace{(k_1h_2k_1^{-1})}_{\in H \because H \trianglelefteq G} k_1k_2 \in HK.$$

So we may define a product denoted '$\rtimes$' in the set $H \times K$ by

$$(h_1, k_1) \rtimes (h_2, k_2) := (h_1k_1h_2k_1^{-1}, k_1k_2)$$

where we note that k_1 acts on h_2 via conjugation i.e. $k \bullet h = khk^{-1}$.
Let us generalize this to an arbitrary action $\bullet : K \times H \to H$ of K on H which induces a group homomorphism $\varphi : K \to \mathrm{Aut}(H) \leq S_H$ defined by

$$\varphi(k)(h) = \sigma_k(h) = k \bullet h \ \forall\ h \in H,\ \sigma_k \in \mathrm{Aut}(H).$$

Here each element of k acts as an automorphism of H.

Theorem 3.1. *Let H and K be groups and $\varphi : K \to Aut(H)$ be a group homomorphism. Let $G := H \times K$ be the cartesian product of H and K. Define a binary operation $\rtimes$ on G by $(h_1, k_1) \rtimes (h_2, k_2) = (h_1\varphi(k_1)(h_2), k_1k_2)$. Then the following hold:*

1. *The binary operation $\rtimes$ makes G a group*

2. *The sets $\tilde{H} = \{(h, 1) \mid h \in H\}$ and $\tilde{K} = \{(1, k) \mid k \in K\}$ are subgroups of G. Also the maps $\theta_1 : H \to \tilde{H}$ and $\theta_2 : K \to \tilde{K}$ defined by $\theta_1(h) = (h, 1)$ and $\theta_2(k) = (1, k)$ are isomorphisms. We may identify H with $\tilde{H}$ and K with $\tilde{K}$. Under this identification,*

3. *$H \cong \tilde{H} \trianglelefteq G,\ G/\tilde{H} \cong \tilde{K}$*

4. *$\tilde{H} \cap \tilde{K} = 1$ therefore $\tilde{H}\tilde{K} = G$.*

5. *For all $\tilde{h} \in \tilde{H}$ and $\tilde{k} \in \tilde{K}$, $\tilde{k}\tilde{h}\tilde{k}^{-1} = \tilde{k} \star \tilde{h}$ where $\star : \tilde{K} \times \tilde{H} \to \tilde{H}$ is action of $\tilde{K}$ on $\tilde{H}$ defined by $\tilde{k} \star \tilde{h} = (k \bullet h, 1) = (\varphi(k)(h), 1)$.*

Proof. 1. For $a, b, c \in H,\ x, y, z \in K$ consider

$$\begin{aligned}
(a, x) \rtimes ((b, y) \rtimes (c, z)) &= (a, x) \rtimes (b\varphi(y)(c), yz) \\
&= (a\varphi(x)(b\varphi(y)(c)), x(yz)) \\
&= (a(\varphi(x)(b)\varphi(x)(\varphi(y)(c))), x(yz)) \\
&= (a\varphi(x)(b)(\varphi(x)(\varphi(y)(c))), (xy)z) \\
&= (a\varphi(x)(b)(\varphi(xy)(c))), (xy)z) \\
&= (a\varphi(x)(b), xy) \rtimes (c, z) \\
&= ((a, x) \rtimes (b, y)) \rtimes (c, z),
\end{aligned}$$

which proves associativity of $\rtimes$. The identity element is $(1, 1)$ since for all $(h, k) \in H \rtimes K$ $(1, 1) \rtimes (h, k) = (1\varphi(1)(h), 1k) = (1 \bullet h, k) = (h, k) = (hk \bullet 1, k) = (h, k) \rtimes (1, 1)$ and inverse of (h, k) is $(h, k)^{-1} = (k^{-1} \bullet h^{-1}, k^{-1})$. This proves that G is a group.
2. Since $(1, 1) \in \tilde{H}$ it follows that $\tilde{H} \neq \emptyset$. If $(h_1, 1), (h_2, 1) \in \tilde{H}$ then $(h_1, 1) \rtimes (h_2, 1)^{-1} = (h_1, 1) \rtimes (1 \bullet h_2^{-1}, 1) = (h_1, 1) \rtimes (h_2^{-1}, 1) = (\underbrace{h_1 h_2^{-1}}_{\in H}, 1) \in \tilde{H}$. Therefore by subgroup criterion $\tilde{H} \leq G$. Similarly $\tilde{K} \leq G$. To prove the other part note that the maps θ_1 and θ_2 are bijective maps. Consider for

all $h_1, h_2 \in H$ $\theta_1(h_1h_2) = (h_1h_2, 1) = (h_1, 1) \rtimes (h_2, 1) = \theta_1(h_1)\theta_1(h_2)$ which proves that θ_1 is a homomorphism which is also bijective hence θ_1 is an isomorphism. Similarly θ_2 is an isomorphism.
3 & 5. We have for all $\tilde{h} = (x, 1) \in \tilde{H}$ and $(h, k) \in \tilde{G} = H \rtimes K$

$$\begin{aligned}(h,k) \rtimes \tilde{h} \rtimes (h,k)^{-1} &= (hk \bullet x, k) \rtimes (k^{-1} \bullet h^{-1}, k^{-1}) \\ &= (h(k \bullet x)k \bullet (k^{-1} \bullet h^{-1}), kk^{-1}) \\ &= (h \underbrace{(k \bullet x)}_{\in H} h^{-1}, 1) \in \tilde{H}.\end{aligned} \tag{3.1}$$

This proves that $\tilde{H} \trianglelefteq G$. In particular taking $h = 1$ in Eq.(3.1) we see that for all $(x, 1) \in \tilde{H}$ and $(1, k) \in \tilde{K}$

$$(1,k)(x,1)(1,k)^{-1} = (k \bullet x, 1) =: (1,k) \star (h,1)$$

where we denote the action $\star : \tilde{K} \times \tilde{H} \to \tilde{H}$ which is via conjugation and thus induces a homomorphism $\tilde{\varphi} : \tilde{K} \to \mathrm{Aut}(\tilde{H})$ s.t. $\tilde{\varphi}(\tilde{k})(\tilde{h}) = \tilde{k}\tilde{h}\tilde{k}^{-1} = (k \bullet h, 1)$. this proves *5.* Now define map $f : G \to \tilde{K}$ by $f(h, k) = (1, k)$. Then clearly this map is a surjective homomorphism with kernel $\ker f = \{(h, k) \in G \mid f(h, k) = (1, 1) \Leftrightarrow k = 1\} = \{(h, 1) \in G\} = \tilde{H}$ thus by first isomorphism theorem $G/\tilde{H} \cong \tilde{K}$.
4. Let $(h, k) \in \tilde{H} \cap \tilde{K}$ then $(h, k) \in \tilde{H}$ gives $k = 1$ and $(h, k) = (h, 1) \in \tilde{K}$ gives $h = 1$. Thus $(h, k) = (1, 1) = 1_G$. Hence $\tilde{H} \cap \tilde{K} = \{1_G\}$. □

Definition: (Semidirect product) Let H and K be groups and $\varphi : K \to \mathrm{Aut}(H)$ be a group homomorphism. Let $G := H \times K$ be the cartesian product of H and K. Then under the binary operation $\rtimes$ on G defined by

$$(h_1, k_1) \rtimes (h_2, k_2) = (h_1\varphi(k_1)(h_2), k_1k_2),$$

the group G is called semidirect product of H and K and is denoted by $G = H \rtimes_\varphi K$ or just $H \rtimes K$ when φ is clearly understood.

Remark: In view of the preceding theorem, we make the following important observations.

1. If the action $\bullet : K \times H \to H$ is trivial i.e $k \bullet x = x$ for all $x \in H$ and $k \in K$, then we have $\tilde{k}\tilde{h}\tilde{k}^{-1} = (k \bullet h, 1) = \tilde{h} = \tilde{k} \star \tilde{h}$ i.e. the action $\star : \tilde{K} \times \tilde{H} \to \tilde{H}$ is also trivial and so is the induced homomorphism $\tilde{\varphi}$.

2. Also when $\bullet$ is trivial, for all $(h_1, k_1), (h_2, k_2) \in G$

$$(h_1, k_1) \rtimes (h_2, k_2) = (h_1 k_1 \bullet h_2, k_1 k_2) = (h_1 h_2, k_1 k_2)$$

   which proves that $H \rtimes_\varphi K = H \times K$ i.e. the semidirect product and the direct product coincide.

3. When $\tilde{\varphi} : \tilde{K} \to \mathrm{Aut}(\tilde{H})$ is trivial homomorphism, then for all $(1, y) \in \tilde{K}$ and $(h_1, k_1) \in G$

$$(h_1, k_1)(1, y)(h_1, k_1)^{-1} = (1, k_1 y k_1^{-1}) \in \tilde{K}$$

   which proves $\tilde{K} \trianglelefteq G$. This indeed proves the following.

4. The map $i : H \rtimes_\varphi K \to H \times K$ (where φ is trivial) defined by $i(h, k) = (h, k)$ is a homomorphism because $i((h_1, k_1) \rtimes (h_2, k_2)) = i(h_1 h_2, k_1 k_2) = (h_1 h_2, k_1 k_2) = (h_1, k_1) * (h_2, k_2) = i(h_1, k_1) * i(h_2, k_2)$.

Remark: We can construct "new" non-abelian groups starting with abelian factors using the semidirect product. Let us characterize some of the familiar non-abelian groups with semidirect product.

Note that if H is any abelian group, the map $\psi : H \to H$ defined by $\psi(h) = h^{-1}$ is an automorphism of H.

Example: Let $K = \langle x \mid x^{2n} = 1 \rangle \cong Z_{2n},\ n = 1, 2...$ and H is any abelian group. Define $\varphi : K \to \mathrm{Aut}(H)$ by $\varphi(k)(h) = k \bullet h = h^{-1}$. Using recognition theorem for semidirect products, we see that in $H \rtimes_\varphi K$

$$\tilde{k} \star \tilde{h} = \tilde{k}\tilde{h}\tilde{k}^{-1} = \tilde{h}^{-1} = (h^{-1}, 1)$$

which gives for any $x = (h,k) = \tilde{h}\tilde{k} \in H \rtimes_\varphi K$ and $(a,b) = \tilde{a}\tilde{b} \in H \rtimes_\varphi K$ the following:

$$\begin{aligned} xyx^{-1} =& \tilde{h}\tilde{k}\tilde{a}\tilde{b}\tilde{k}^{-1}\tilde{h}^{-1} = \tilde{h}\underbrace{\tilde{k}\tilde{a}\tilde{k}^{-1}}_{=\tilde{a}^{-1}}\tilde{b}\tilde{h}^{-1} \ (\because \tilde{K} \text{ is abelian}) \\ =& \tilde{h}\tilde{a}^{-1}\tilde{b}\tilde{h}^{-1} = \tilde{a}^{-1}\tilde{h}\tilde{b}\tilde{h}^{-1} \ (\because \tilde{H} \text{ is abelian}) \\ =& \tilde{a}^{-1}\tilde{h}^2\underbrace{\tilde{h}^{-1}\tilde{b}\tilde{h}^{-1}}_{=\tilde{b}} = \tilde{a}^{-1}\tilde{h}^2\tilde{b} = \tilde{h}^2\tilde{a}^{-1}\tilde{b} \\ \therefore \ x^2yx^{-2} =& x(xyx^{-1})x^{-1} = \tilde{h}^2(\tilde{h}^2\tilde{a}^{-1})^{-1}\tilde{b} = \tilde{a}\tilde{b} = y. \end{aligned}$$

We have proved that $x^2yx^{-2} = y \ \forall \ x, y \in H \rtimes_\varphi K$. Thus $x^2 \in Z(H \rtimes_\varphi K)$. In particular if we take $H = Z_3$ and $K = Z_4$ and $\varphi : K \to \mathrm{Aut}(H)$ be defined by $\varphi(k)(h) = h^{-1}$ then the semidirect product $H \rtimes_\varphi K$ is a non abelian group of order 12 containing cyclic subgroup of order 4 which is its one of the Sylow$-2-$subgroups. Since the Sylow$-2-$subgroup of A_4 and any Sylow$-2-$subgroup of D_{12} is isomorphic to the Klein-4-group, it follows that $D_{12} \ncong H \rtimes_\varphi K \ncong A_4$. This way we obtain upto isomorphism three distinct non abelian groups of order 12.

Example: Since there is only the trivial automorphism of Z_2, it follows that for any abelian group K the semidirect product $Z_2 \rtimes K = Z_2 \times K$.

Example: Let $Z_n = \langle x \rangle$ and $Z_2 = \langle y \rangle$. Consider semidirect product $Z_n \rtimes_\varphi Z_2$ where $n \geq 3$ and $\varphi : Z_2 \to \mathrm{Aut}(Z_n)$ is a non-trivial homomorphism defined by the action $y \bullet (x) = x^a$, for some integer a. Then $\tilde{y} \star \tilde{x} = \tilde{y}\tilde{x}\tilde{y}^{-1} = \tilde{x}^a$. This gives $\tilde{y}\tilde{x}^a\tilde{y}^{-1} = \tilde{x}^{a^2} \ \Rightarrow \ \tilde{y}(\tilde{y}\tilde{x}\tilde{y}^{-1})\tilde{y} = \tilde{x}^{a^2}$ which further yields $\tilde{x}^{a^2-1} = 1$. Since $|\tilde{x}| = n$ it follows that $n \mid (a^2 - 1)$. Clearly $a = -1$ satisfies this. Therefore for $\tilde{y} \star \tilde{x} = \tilde{x}^{-1}$, the semidirect product $Z_n \rtimes_\varphi Z_2$ is given by

$$Z_n \rtimes_\varphi Z_2 = \left\langle \tilde{x}, \tilde{y} \mid \tilde{x}^n = 1 = \tilde{y}^2; \ \tilde{x}\tilde{y} = \tilde{y}\tilde{x}^{-1} \right\rangle = D_{2n}.$$

Example: Try showing that $S_3 \cong Z_3 \rtimes_\varphi Z_2$ for the nontrivial homomorphism $\varphi : Z_2 \to \mathrm{Aut}(Z_3) \cong Z_2$.

3.1 Semidirect product of subgroups

We have the following recognition theorem regarding semidirect product of subgroups of a group G.

Theorem 3.2. *(Recognition) Suppose H and K are subgroups of a group G such that $H \trianglelefteq G$ and $H \cap K = \{1\}$. Then $HK \leq G$ and $HK \cong H \rtimes_\varphi K$ where $\varphi : K \to Aut(H)$ is a homomorphism defined by $\varphi(k)(h) = khk^{-1}\ \forall\ h \in H,\ k \in K$. In particular if $HK = G$ then $G \cong H \rtimes_\varphi K$.*

Proof. Since $H \trianglelefteq G$ and $K \leq G$, it follows that $HK \leq G$. Also as $H \cap K = \{1\}$ every element of HK can be uniquely written as a product hk for some $h \in H$ and $k \in K$. So the map $\psi : HK \to H \rtimes_\varphi K$ defined by $\psi(hk) = (h, k)$ is a bijection. Finally we prove that ψ is a group homomorphism. For all $h_1, h_2 \in H$ and $k_1, k_2 \in K$ consider

$$\begin{aligned}\psi(h_1k_1h_2k_2) =& \psi(h_1 \underbrace{k_1h_2k_1^{-1}}_{\in H\cdot\, H \trianglelefteq G} k_1k_2) = (h_1k_1h_2k_1^{-1}, k_1k_2)\\ =& (h_1\varphi(k_1)(h_2), k_1k_2) = (h_1, k_1) \rtimes (h_2, k_2) = \psi(h_1k_1) \rtimes \psi(h_2k_2).\end{aligned}$$

This completes the proof. □

Definition: Let $H \leq G$. A subgroup K of G is called compliment of the subgroup H if $H \cap K = \{1\}$ and $G = HK$.

Remark: G is a semidirect product if and only if G has a proper normal subgroup H such that H has compliment in G. So for some finite orders such as $|G| = pq$, where p and q are distinct primes we can deduce that G must be a semidirect product. Then we can classify upto isomorphism all groups of that order. However unlike finite abelian groups, there is no fundamental theorem for classification of all finite non abelian groups.

Example: Let $|G| = pq,\ (p < q),\ p \mid q - 1$ where p, q are distinct primes. Then $H \cong Z_q$ and $K \cong Z_p$ such that $H \trianglelefteq G$ and $K \leq G$. Since $\mathrm{Aut}(H) \cong$

Z_{q-1} we see that there are $q-2$ distinct automorphisms of H. If $p \mid (q-1) = |\mathrm{Aut}(H)|$ then $\mathrm{Aut}(H)$ has an element σ of order p. Consider the subgroup $\langle\sigma\rangle$. Then $\sigma(x) = x^c$ for all $x \in Z_q = \langle x\rangle$ for some $c \in \mathbb{Z}$. Then $x = \sigma^p(x) = x^{c^p}$ or $x^{c^p-1} = 1$. Since $|x| = q$ it follows that $q \mid (c^p - 1)$. Using Fermat's little theorem, choose a $c = d^{\frac{q-1}{p}}$ for any $d = 1, 2..., q-1$. Therefore here

$$Z_q \rtimes_{\varphi_i} Z_p = \langle x, y \mid x^q = 1 = y^p;\ yx = x^c y\rangle\ ,\ c = d^{\frac{q-1}{p}}$$

where $\varphi_i(y)(x) := \sigma^i(x) = yxy^{-1}$ for any $i = 0, ..., p-1$. For $i = 0$, φ_0 is the trivial homomorphism ($c = 1$) and in this case the semidirect product is same as the direct product of abelian groups $Z_q \times Z_p$. For $i = 1, 2..., p-1$ each homomorphism φ_i is nontrivial and the semidirect product is a non-abelian group. Also note the $H \rtimes_{\varphi_1} K \cong H \rtimes_{\varphi_j} K,\ \forall\ j = 1, 2..., p-1$ with the isomorphism $\Psi(x, y) = (x^j, y)$. This proves that there is "unique" non-abelian group of order pq with $p \mid (q-1)$.

4 Transformation Groups

Consider the semidirect product $G = \mathbb{R}^n \rtimes GL_n(\mathbb{R})$ where $(x, A) \rtimes (y, B) = (x + A\bullet y, AB)$ with the standard inner product where $GL_n(\mathbb{R})$ acts on $\mathbb{R}^n$ via matrix multiplication. This defines affine action of G on $\mathbb{R}^n$ given by $(x, A) \bullet y = x + Ay$. This G is called affine group. If we consider the standard inner product of $\mathbb{R}^n$, then $\|(x, A) \bullet y_1 - (x, A) \bullet y_2\|^2 = \langle A(y_1 - y_2), A(y_1 - y_2)\rangle = A(y_1 - y_2)(A(y_1 - y_2))^T = AA^T\|y_1 - y_2\|^2$. Therefore on the orthogonal group $O(n) := \{A \in GL_(\mathbb{R}) \mid AA^T = I\}$, $\|(x, A) \bullet y_1 - (x, A) \bullet y_2\| = \|y_1 - y_2\|$ i.e. each element of $E_n := \mathbb{R}^n \rtimes O(n)$ is an isometry. E_n is called the Euclidean group. Also note that the map $\det : O(n) \to \{-1, 1\}$ is surjective homomorphism, therefore it contains a subgroup of index 2 which we call the special orthogonal group denoted $SO(n)$.
We will prove the following

Proposition 4.1. *Let $A \in SO(3)$, $A \neq I$. Then there is a one dimensional subspace $W_A = \{v \in \mathbb{R}^3 \mid Av = v\}$ of $\mathbb{R}^3$ left invariant by A. If $\{e_1, e_2, e_3\}$ is*

the standard ordered ortho normal basis of $\mathbb{R}^3$ *such that* $W_A = \langle e_1 \rangle$, *then* A *has the matrix representation*

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & \sin\theta \\ 0 & -\sin\theta & \cos\theta \end{pmatrix}$$

where eigenvalues of A *are* $1, e^{\pm i\theta},\ \theta \in [0, 2\pi)$.

Proof. Let $f(t) = \det(tI - A)$. Then $f(0) = -1$ and $\lim_{t\to\infty} f(t) = \infty$ since f is a nonconstant polynomial function. It follows that f has a real zero lying in $(0, \infty)$ which must be 1 as $A \in SO(3)$. This shows that $\dim(W_A) \geq 1$. If $\dim(W_A) = 2$ then $\dim(W_A^\perp) = 1$ therefore there is a $w \in W_A^\perp$ such that $Aw = -w$ which gives $\det(A) = -1$ which is absurd. Therefore $\dim(W_A)$ is either 1 or 3. Since $A \neq I$, this means $\dim(W_A) \neq 3$ i.e. $\dim(W_A) = 1$. Hence $\dim(W_A^\perp) = 2$ and for any $x \in \mathbb{R}^3 = W_A \oplus W_A^\perp$ we have $x = v + Ay$ where $v \in W_A$ and $Ay \in W_A^\perp \cong \mathbb{R}^2$. □

Definition: A rotation in $\mathbb{R}^3$ is an element of $A \in SO(3)$ which leaves a straight line (an element of $\mathbb{R}^3$) invariant with a rotation about this straight line by an angle θ.

We will explore on finite subgroups of $SO(3)$. So let $H \leq SO(3)$ be finite. Consider action of H on $\mathbb{R}^3$ via $h \bullet x = hx$. If $x \in \mathbb{R}^3,\ x \neq 0$ be an axis of rotation for some $1_H \neq h \in H$ i.e. $hx = x$. Then $h \in \mathrm{Stab}(x) = \{h \in H \mid hx = x\} \leq H$. Let $\theta \mod 2\pi$ be the minimum among positive angles of rotation of all $h \in \mathrm{Stab}(x)$. Since $\mathrm{Stab}(x)$ is finite, it follows that $|h|$ is finite for each $h \in \mathrm{Stab}(x)$, let $|h| = n > 1$. As h is of the form

$$h = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & \sin\theta \\ 0 & -\sin\theta & \cos\theta \end{pmatrix} \Rightarrow h^n = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos n\theta & \sin n\theta \\ 0 & -\sin n\theta & \cos n\theta \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

which gives $\cos n\theta = 1$ and $\sin n\theta = 0$. These equations have unique solution $\mod 2\pi$, given by $n\theta = 2\pi$. This gives $\theta = \frac{2\pi}{n}$. Thus any element h of $\mathrm{Stab}(x)$

has minimum angle of rotation $\frac{2\pi}{|h|}$. If t is any element of $\mathrm{Stab}(x)$ with angle of rotation $\theta' \geq \theta$ then for all $k = 0..., n-1$, we have $h^k x = x = tx$ which gives $t^T h^k x = x$. For $x \neq 0$, $\det(t^T h^k - I) = 0$ which on solving reduces to $\cos(\theta' - k\theta) = 1$. Since $|\theta' - k\theta| < 2\pi$ this forces $\theta' = k\theta$.We have proves that $t = h^k$ for some $k = 0, 1, ..., n-1$. Thus $\mathrm{Stab}(x) \cong \mathbb{Z}_n$.
Let $X = \{x \in \mathbb{S}^2 \mid hx = x, \text{ for some } h \in H,\ x \neq 1_H,\ \|x\| = 1\}$. Then under the action of H on X, for $hx = x$ we have $(ghg^{-1}) \bullet gx = gx$ for all $g \in H$. So let X be disjoint union of k orbits $\mathcal{O}_{x_i},\ i = 1, ..., k$ with $|\mathrm{Stab}(x_i)| = n_i$. This leads to the following:

Theorem 4.2.

$$\sum_{i=1}^{k} \left(1 - \frac{1}{n_i}\right) = 2 - \frac{2}{|H|}. \tag{4.1}$$

Proof. Consider the set $Y = \{(x, h) \mid x \in X,\ h \in H,\ h \neq 1_H,\ hx = x\}$. Fix $h \in H$; for this h there are exactly two points on the sphere $\mathbb{S}^2$ lying on axis of rotation of h. Therefore $|Y| = 2 + ... + 2((|H|-1)\text{times}) = 2(|H|-1)$. On the other hand for each $x \in \mathcal{O}_{x_i}$ there are exactly $|\mathrm{Stab}(x)|-1$ nontrivial rotations fixing x. Therefore $|Y| = \sum_{i=1}^{k} |\mathcal{O}_i|(n_i - 1)$ where $|\mathrm{Stab}(x)| = |\mathrm{Stab}(x_i)| = n_i$. We have proved that

$$2(|H| - 1) = |Y| = \sum_{i=1}^{k} |\mathcal{O}_i|(n_i - 1) = \sum_{i=1}^{k} \frac{|H|}{n_i}(n_i - 1)$$

from which the result follows. □

Remark: The result (4.1) is useful in classifying all finite subgroups of $SO(3)$. Infact every finite subgroup of $SO(3)$ is conjugate to one of the following five groups: $\mathbb{Z}_n,\ D_{2n},\ (\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_3,\ (\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes S_3$ and A_5. See for proof [3].

References:

[1] D.S. Dummit and R.M. Foote. *Abstract Algebra*, John Wiley 2007.

[2] Joseph A. Gallian. *Contemporary Abstract Algebra*. Brooks/Cole Pub. 7th Ed. 2010.

[3] Barry Simon. *Representations of Finite and Compact Groups*. AMS (Indian Edition) 2009