Proceedings of the 3rd International Conference on Computing Innovation and Applied Physics
DOI: 10.54254/2753-8818/9/20240733

Group action and its application on classification of low order groups

Shuang Liang

Institute of Mathematical Sciences, ShanghaiTech University, Shanghai, China

Liangshuang1@shanghaitech.edu.cn

Abstract. The classification of finite groups is an important topic in mathematics throughout history of mathematics. The topic of this paper is to use group action as a tool, to classify some special finite groups and some low order groups. First this paper introduces some concepts of group action. Then this paper states and proves some important theorems related to group action. For example, the Sylow's theorem, which is very important in this paper. Research has found that, groups of specific order, such as groups whose order are $2p, p^2$, $pq(p, q$ are distinct prime numbers), p^3(p is prime) can be classified using group action and the technique of semi-direct product, and groups whose order are no more than 15 are classified which can be seen as the special situations of the above ones. But in general, to make classification of a larger range of finite groups, more tools should be introduced.

Keywords: Finite Groups, Group Action, Sylow's Theorem.

1. Introduction

Group theory is a very essential part of mathematics, the occurrence of group theory marks the birth of abstract algebra. In the formation of the concept of group, the British mathematician, Cayley, made outstanding contributions [1]. The classification problem of finite groups is a very important and complex topic in group theory, and it was not until the sixties of the last century that the problem of classifying simple groups with finite order was completely solved [2]. A_5 is the simple group of the smallest order [3].

The significance of the topic of classifying finite groups is far-reaching. For example, it is proved that every finite abelian group is isomorphic to the direct product of some cyclic groups [4], and this result allows us to make some Fourier analysis on finite abelian groups and draw a series of beautiful conclusions [5].

Group action is the core and basis of group theory. As an important tool, group action reflects some essential properties of a group (a set with special structure). Group action also has some strong geometric intuition, which can be seen from the action of dihedral groups on regular polygons and some special groups acts on the set which consists of all real symmetric matrices whose order is two, which gives an interesting result [6]. Also, group action has a broad application in other fields of mathematics. For example, in Combinatorial mathematics, it can be used to prove Burnside's lemma, which can be used to solve the 'coloring problem' [7].

DOI: 10.54254/2753-8818/9/20240733

When mentioning a group action, it is natural to think of its permutation representation, which is known as the Cayley's theorem. Furthermore, the famous Sylow's theorem, is also related to group action. There are many ways to proof this theorem, most of which using group action and the orbit-stabilizer theorem, but there exist some new ways to proof this old theorem [8]. The Sylow's theorem, which can be seen as the result of a group act on a special set (the set consists of all $Sylow - p$ subgroups) by conjugation, is very useful since it has many applications. For example, applying this theorem, the isomorphic types of some special finite groups can be classified [9], including the group of order 24[10]. This paper introduces the group action, proves some important theorems, including Cauchy's theorem, Sylow's theorem, the class equation, etc. Then combine these theorems to classify some special finite groups, such as groups of order pq (p, q are distinct prime numbers), p^3(p is prime), etc. Also, the isomorphic types of some groups of lower order will be classified, such as groups of order 8 and 12, etc. Their isomorphic table will be listed.

2. Methods

2.1. Group action

Definition (Group action): A (left) group action of a group G on a set S is a map: $G \times S \to S$, which satisfies: Identity law: $1_G \cdot s = s$ Associative law: $(g \cdot g') \cdot s = g \cdot (g' \cdot s)(g, g' \in G, s \in S)$. A group action $G \times S \to S$ is faithful if the following holds: $g \cdot s = s$ ($\forall s \in S$), then $g = 1_G$.

Remark that when mentioning a group action, it's important to consider its permutation representation, i.e., the homomorphism from G to the permutation group of the set S, which is also known as the Cayley's theorem. If the group action is faithful, then the homomorphism is injective, vice versa.

A group action $G \times S \to S$ is transitive if the following holds: $\exists s \in S, \text{st } S = Os, Os$ represents the orbit of s.

2.2. Additional theorems

Orbit-Stabilizer theorem: A bijective map from O_s to G/Gs by defining as $\mapsto$ aGs, this map is well defined and bijective. Thus, by the Lagrange's theorem, $|Os||Gs| = |G|$.

Class equation: G is a finite group and assume $g_1, g_2 \dots g_n$ be representatives of the disjoint conjugacy classes in G which aren't in Z(G), then $|G| = |Z(G)| + \sum_{i=1}^{n} |G: C_G(g_i)|$.

Cauchy's theorem: G is a finite group, p is prime & $p\backslash n$, then G contains an element whose order is p.

Proof: First consider when G is abelian. If $|G| = 1$, it's trivial case. For the inductive step, choose $g \in G$ whose order is $k > 1$. If p|k, say k = pl, then g^l has order p. If p isn't divisible by k, consider the group $H \triangleq < g >$, whose order is k. $H \lhd G$ so G/H is a group & $[G: H] = n/k$. Since $p|[G: H]$, by inductive step, $\exists aH \in G/H$ of order p. Assume the order of a in G is m, then $(aH)^m = H$, which indicates that $p|m$. This sends us back to the first case.

For the general case, one proves again using induction on $|G|$. If |G|=1, it's the trivial case. Let $x \in G$, by the Orbit-Stabilizer theorem, $|x^G|$= [G: $C_G(x)$]. Assume $x \notin Z(G)$, then $C_G(x) \neq G$, which implies $|C_G(x)| < |G|$. If $p||C_G(x)|$ for some x with $x \notin Z(G)$, then by inductive hypothesis, the theorem holds.

Therefore, one may assume that p doesn't divide $|C_G(x)|$ for every x with $x \notin Z(G)$. Since $p||G|$, we conclude that p| $[G: C_G(x)]$ for all x with $x \notin Z(G)$, by the Class equation: $|G| = |Z(G)| + \sum_{i=1}^{n} |G: C_G(g_i)|$, $p||Z(G)|$. Because Z(G) is an abelian group, it has an element whose order is p, so does G, thus completes the proof.

Lemma 1: Consider $G \times 2^G \to 2^G$ by left multiplication, then |Stab(U)|||U| satisfy:

$$g \cdot U \overset{\text{def}}{=} gU = \{gu | u \in U\} \tag{1}$$

Proof: Stab(U)$\overset{\text{def}}{=}$H, consider the induced group action: $H \times U \to U$ by left multiplication.$\forall u \in U, H_U \overset{\text{def}}{=} \{h \in H | hu = u\} = \{1_H\}$, then $|O_U|$=|H|. Since U is the disjoint union of orbits, |U|=$\sum_{i=1}^{n} |O_{U_i}|$, we conclude |H|||U|.

Sylow's theorem: If G is a finite group, p is prime & p||G|=n, then G contains a Sylow-p subgroup. Furthermore, ∀ p-subgroup of G is contained in a Sylow-p subgroup and Sylow-p subgroups are conjugate groups ($\forall H, H' Sylow - p\ subgroups, \exists g \in G\ st\ gHg^{-1} = H'$). If $n = p^e m(\ p\ is\ not\ divisible\ by\ m)$, let $t = \#\ of\ Sylow\ p -\ subgroups$ in G, then t|m & $t \equiv 1(mod\ p)$.

Proof: Observe that p is NOT divisible by $\binom{n}{p^e}$. Consider G acts on {subsets of G of order p^e}, then $\binom{n}{p^e} = \sum_{Orbits} |O|$, since p is NOT divisible by $\binom{n}{p^e}$, *then there* exists some orbit O_U st p is not divisible by $|O_U|$.$\begin{cases} p^e m = n = |G| = |O_U||G_U| \\ (by\ lemma)|G_U||p^e = |U| \end{cases} \xrightarrow{yields} |G_U| = p^e, |O_U| = m$, which completes the first part of this theorem.

Let K be any p subgroup of G and let H be any Sylow p-subgroup of G. We prove:$\exists g \in G, st\ K \leq gHg^{-1}$. Consider the group action:$G \times G/H \to G/H$ by left multiplication. Observation: G_H=H & G_{gH}=gHg^{-1}, consider the restriction: $K \times G/H \to G/H$, since m=|G/H|=$\sum_{i=1}^{k} |O_i|$&$|O_i|$||K| and p is NOT divisible by m, then there exists an orbit, denoted by O_{gH}, st $|O_{gH}| = 1$, i.e. $K \leq G_{gH} = gHg^{-1}$, which completes the second part of this theorem.

Consider the group action: $G \times \{Sylow\ p - subgroup\} \overset{\text{def}}{=} S \to S\ by\ conjugation$, i.e. $g \cdot H \overset{\text{def}}{=} gHg^{-1}$, t=|S|, by Orbit-Stabilizer theorem, $p^e m = |G| = t|N_G(H)|$, also, $|H| = p^e||N_G(H)|$, then $t|m$.

Next, consider the restriction: $H \times S \to S$, note that $\forall\ orbit\ O, either\ p||O|or|O| = 1$ since $|H| = p^e$. $H \leq N_G(H) \xrightarrow{yields}$ orb(H)={H} Suppose $H' a\ Sylow\ p - subgroup\ that\ satisfies$: $H \leq N_G(H')$ (note that $H \leq N_G(H') iff\ orb(H') = \{H'\}$), then $\begin{cases} H \leq N_G(H') \\ H' \leq N_G(H') \end{cases} \xrightarrow{yields} H = H' since\ they\ are\ conjugate\ in\ N_G(H')$, then $t \equiv 1(mod\ p)$, which completes the last part of this theorem.

3. Results and discussion

3.1. Group whose order is p^2(p is prime)

Group G of order p^2(p is prime) is either isomorphic to C_{p^2} or $C_p \times C_p$.

Proof: If there exists an element in G of order p^2, then it's clear that $G \approx C_{p^2}$. Otherwise, we may assume that no element in G is with order p^2. Consider the center of G, since the center of a p group is nontrivial, we conclude that $Z(G) \approx C_p$. Choose an element in G but not in $Z(G)$, say y, and denote H the group generated by y. Consider the map $f: H \times Z(G) \to G$:

Where f is injective since $H \cap Z(G) = \{1_g\}$(by Lagrange's theorem), $(h, k) \mapsto hk$, f is group homomorphism since $\forall h, k, hk = kh$.(the definition of Z(G)), f is surjective since $|HZ(G)| = \frac{|H||Z(G)|}{|H \cap Z(G)|}$=$p^2$=|G|. Thus, f is isomorphism, G≈ $H \times Z(G) \approx C_p \times C_p$.

3.2. Group whose order is $2p$(p is prime)

If $p = 2$, then G is an abelian group and $|G| = 4 = p^2$, by the results in group with order p^2(p is prime) above, $G \approx C_4 or$ G≈ $C_2 \times C_2 \approx K_4$. If $p > 2$, by Cauchy's theorem, G has a subgroup H whose order is p. Because the index of H in G is 2, H is normal in G, H≈ $C_p \overset{\text{def}}{=} < x >$. Also there exists a subgroup K$\overset{\text{def}}{=}< y >$ of G whose order is 2. Because HK=G, by introducing the concept of semi-direct product, one concludes that $G \approx H \rtimes K$. Consider all homomorphisms from $K\ to\ Aut(H)$, since $Aut(H) \approx C_{p-1}$, there are only two possible situations: (a) $\varphi: K \to Aut(H)\ with\ yxy^{-1} = x$, which represents the trivial homomorphism, then $G \approx H \rtimes K \approx H \times K \approx C_p \times C_2 \approx C_{2p}$. (ii) WLOG, $\varphi: K \to Aut(H)\ with\ yxy^{-1} = x^{-1}$, then $\begin{cases} x^p = y^2 = 1_G \\ yxy^{-1} = x^{-1} \end{cases} \xrightarrow{yields} G \approx D_{2p}$. Thus, if $|G| = 2p$ (p is prime), then G is either isomorphic to $D_{2p}\ or\ C_{2p}$.

3.3. *Groups of order* $pq(p, q\ primes\ with\ p < q)$

Let $P \stackrel{\text{def}}{=} < x >$ denote the Sylow-p subgroup of G and R denote the Sylow-q subgroup of G. Note that R is normal. Furthermore, if P is normal, then G is a cyclic group. Let n_p denote $\#\ of\ Sylow - p\ subgroups\ in\ G$ and n_q denote $\#\ of\ Sylow - q\ subgroups\ in\ G$. By Sylow's theorem, $n_q = 1, so\ R \lhd G$. Since $PR = G\ \&\ P \cap R = \{1_G\} \&\ R \lhd G$, we conclude that $G \approx R \rtimes P$. Since |R|=q, $Aut(R) \approx C_{q-1}$.

Consider all the homomorphism from $P\ to\ Aut(R)$. If p doesn't divide $q-1$, then the map can only be trivial. Thus, the semi-direct product is actually direct product, and $G \approx R \rtimes P \approx C_q \times C_p \approx C_{pq}, G\ is\ cyclic.$ If $p|q-1$, since $Aut(R)$ is a cyclic group, it has a unique subgroup of order p, say $H \stackrel{\text{def}}{=} < y >$. Let $\varphi: P \to Aut(R)\ be\ the\ homomorphism,\ Ker(\varphi) = \{1_G\}$(Otherwise, it's the trivial map.), so $\varphi\ is\ injective.$ It must map P to H. WLOG, assume $\varphi(x) = y$, then $G \approx R \rtimes_\varphi P$, which is a non-abelian group.

Thus, all the isomorphic types of groups of order $pq(p, q\ primes\ with\ p < q)$ are given.

3.4. *Groups of order* $p^3(\ p\ an\ odd\ prime)$

If G is an abelian group, then by the fundamental theorem of finite abelian groups, $G \approx C_{p^3}$or $G \approx C_{p^2} \times C_p\ or\ G \approx C_p \times C_p \times C_p$. If G is not cyclic, we first claim that G must contain an element of order p^2or every nontrivial element of G has order p. This can be seen from the homomorphism f: $G \to Z(G)$ by sending $g\ to\ g^p$.

Case 1. G contains an element whose order equals to p^2. Let x be the element with order p^2 and define $H \stackrel{\text{def}}{=} < x >$. H is abelian since H is of order p^2. $H \lhd G\ since\ H\ is\ the\ unique\ Sylow - p\ subgroup\ in\ G$. Denote K the kernel off, then $K \approx C_p \times C_p$, $E \cap H = < x^p >$. Choose $y \in K - H, and\ P \stackrel{\text{def}}{=} < y >. Then\ H \cap P = \{1_G\}$, since H is normal, we have $G \approx P \rtimes H \approx C_{p^2} \rtimes C_p$. Consider all the homomorphism φ from P to $Aut(H)$: (a) $\varphi\ is\ the\ trivial\ map$, then $G \approx C_{p^2} \times C_p$, which is the abelian case. (b) $\varphi\ is\ nontrivial, since\ Aut(H) \approx C_{p(p-1)}$. $Aut(H)$ contains a unique element of order p, say $\gamma, with\ \gamma(x) = x^{p+1}$. Then, up to a choice of generator of P, obtaining the only homomorphism φ from P to $Aut(H)\ given\ by\ \varphi(y) = \gamma$. Hence $G \approx H \rtimes_\varphi P$ in this case.

Case 2. The order of every nontrivial element in G equals to p. Denote H a subgroup with order $p^2, then\ H \approx C_p \times C_p$. Choose $y \in G - H, denote\ K = < y >$, then $H \lhd G\ and\ H \cap K = \{1_G\}$. Thus, $G \approx H \rtimes K \approx (C_p \times C_p) \rtimes C_p$. Again, consider all the homomorphism φ from K to $Aut(H)$: 1. φ is the trivial map, then $G \approx C_p \times C_p \times C_p$, which is the abelian case. 2. $\varphi\ is\ nontrivial$, observe that $Aut(H) \approx GL_2(F_p)$, $|Aut(H)| = p(p+1)(p-1)^2$. So, these Sylow-p subgroups all have order p. These Sylow-p subgroups are conjugate in G. Say $< \gamma >$ a Sylow-p subgroup, denote $H = < a > \times < b >$, then define $\gamma : \gamma(a) = ab\ and\ \gamma(b) = b$; $\varphi: \varphi(y) = \gamma$. One can prove that in this situation, this is the only isomorphism type of G, so $G \approx H \rtimes_\varphi K$.

4. Application

The results above can be used for classifying some finite groups of low order (no more than 15). Let G be the finite group and let n denote the cardinality of G. For n=1, 2, 3, 5, 7, 11, 13 which are primes, $G \approx C_n$. If n=6, 10, 14 then this is the case where the groups are of order 2p (p prime), so $G \approx C_{2p}\ or\ D_{2p}$. If n=4, 9, this is the case that the groups are of order p^2(p is prime), so $G \approx C_{p^2}\ or\ C_p \times C_p$. If n=15, this is the case that the groups are of order pq (p, q primes with $p < q$), so $G \approx C_{15}$. If n=8, there are 5 isomorphic types:$C_8, C_2 \times C_4, C_2 \times C_2 \times C_2, Q_8, D_8$.

Proof: Assume G has an element whose order is 8, $G \approx C_8$. Assume G has an element whose order is 4, say a, denote $M =< a >$. Choose $b \in G - M$, with $b^2 \in M$ (this is possible), denote $K =< b >$. Then either $b^2 = 1_G \; or \; b^2 = a^2$. If $b^2 = 1_G$, then $M \cap K = \{1_G\}$ and $M \lhd G$, so $G \approx M \rtimes K$. There are two types of semi-product in this case, which leads to $G \approx C_2 \times C_4 \; or \; G \approx D_8$. If $b^2 = a^2$, consider bab^{-1}, then either $bab^{-1} = a$ or $bab^{-1} = a^3$. In the first one, $G \approx C_2 \times C_4$; in the second one, $G = \{a, b | a^4 = \{1_G\}, bab^{-1} = a^3, b^2 = a^2\}$, so $G \approx Q_8$. Assume the order of every nontrivial element in G is 2, then clearly $G \approx C_2 \times C_2 \times C_2$.

Thus, all the isomorphic types of group G of order 8 are shown. If n=12, then there are 5 isomorphic types of G, which are represented by: $C_{12}, C_2 \times C_2 \times C_3, A_4, D_{12}, < x, y | x^4 = y^3 = 1_G, xy = y^2 x >$. Proof: From Sylow's theorem, there is a Sylow-2 subgroup in G, denoted by M. Also, a Sylow-3 subgroup of G, denoted by N. Denote m and n the number of Sylow-p subgroups respectively. Then by Sylow's theorem, m=1 or 3; n=1 or 4. Observation: At least one of M & N is normal in G. Denote f: $M \times N \to G, (m, n) \mapsto mn$, then f is bijective. Case1: Both M and N are normal in G. Then $G \approx M \times N \approx C_{12} \; or \; C_2 \times C_2 \times C_3$. Case2: N isn't normal in G. Claim: $G \approx A_4$. Proof: Let G act on $\{N_1, N_2, N_3, N_4\}$ by conjugation, then look at the permutation representation: $\varphi: G \to S_4$, then φ is injective, so $G \approx \varphi(G) \leq S_4$, therefore $G \approx A_4$. Case3: N is normal but M isn't normal in G and $M \approx C_4$. Suppose $M =< x >, N =< y >$. Consider $xyx^{-1} = y^i$, then either $i = 1$ or $i = 2$. If $i = 1$, then back to Case1. If $i = 2$, then $G \approx C_3 \rtimes_\varphi C_4$ with $\varphi: C_4 \to Aut(C_3)$; $\varphi(x) = \gamma \; and \; \gamma(y) = y^2$. So $G \approx < x, y | x^4 = y^3 = 1_G, xy = y^2 x >$. Case4: $N \lhd G$ but M isn't normal in G and $H \approx K_4$.Iin this case, we again look at the semi-direct product and conclude that $G \approx S_3 \times C_2 \approx D_{12}$. Thus, all the isomorphic types of group G of order 12 are shown.

We then make Table 1 to demonstrate all the isomorphic types of the groups whose order is no more than 15:

Table 1. Groups of small order.

Order of G	# of isomorphic types of G	Abelian	Non-abelian
1	1	$\{1_G\}$	null
2	1	C_2	null
3	1	C_3	null
4	2	C_4, K_4	null
5	1	C_5	null
6	2	C_6	S_3
7	1	C_7	null
8	5	$C_8, C_2 \times C_4, C_2 \times C_2 \times C_2$	Q_8, D_8
9	2	$C_9, C_3 \times C_3$	null
10	2	C_{10}	D_{10}
11	1	C_{11}	null
12	5	$C_{12}, C_2 \times C_2 \times C_3$	A_4, D_{12}
13	1	C_{13}	null
14	2	C_{14}	D_{14}
15	1	C_{15}	null

5. Conclusion

Group action indicates the relation between an arbitrary group and a symmetry group. To be more specific, it says that every element in an arbitrary group can always be embedded into a symmetry group.

Through applying group action to group classification, some groups of low order can be classified, and some specific types of finite groups can also be classified. The key of this method is that one can use the theorems above to find a normal Sylow-p subgroup in the big group first then one can use other subgroups act on this normal subgroup by conjugation to find more information of the big group. To use this method, there are two things that are indispensable. The first thing is that one can manage to find a normal Sylow-p subgroup in G, say H. The second thing is that one can find the complement of this normal subgroup H, which is a subgroup, say K, which satisfies two conditions: G=HK. H∩K= $\{1_G\}$. Then one can construct a semi-direct product of the two subgroups, so that G≈H⋊K. After finding all the possible types of the semi-direct product and identify the same ones, one can obtain all the isomorphic types of G. This method is useful to classify the group where the order of the group is small because in those cases, the two conditions are easy to be satisfied.

However, this method is limited because in more general cases, where the order of G may be very large, it may be very difficult to find one normal Sylow-p subgroup, and so its complement. So, in order to classify a larger range of finite groups, more techniques should be considered and applied, such as the techniques from the representation theory of finite groups.

References

[1] Gu B B 2016 Arthur Cayley's Contribution to the Abstract Group Concept. Hebei Normal University.
[2] Hu J M 2009 A Research on the History of the Classification of the Finite Simple Groups. Hebei Normal University.
[3] Cheng S G 1979 A brief proof of a Simple Group of Order 60. Journal of Hangzhou Normal University (Natural Science Edition), 2, 30-31.
[4] Dummit D S, Foote R M 2003 Abstract Algebra. *Inc, New York*.
[5] Stein E M, Shakarchi R 2010 Fourier analysis an introduction. *Princeton University Press, 41 William Street, Princeton, New Jersey*.
[6] Huo L J, Cheng W D 2022 An interesting example on group actions. *College Mathematics*, 38(03), 89-92.
[7] Rotman J J 2016A First Couse in Abstract Algebra with Applications. *Pearson Education Asia Limited and China Machine Press*.
[8] Li Q L 1995 Another proof of the Solow theorem. *Journal of Yanbei teachers' college*, 1-3.
[9] Zhang L C, et al. 2014 On applications of Sylow's theorem. *Journal of Southwest China Normal University (Natural Science Edition)*, 39(08), 137-140.
[10] Li Z X 2011 A Classification of Finite Groups of Order 24. *Journal of Jinzhong University*, 28(03), 11-13.