Journal of Advances and Scholarly Researches in Allied Education
Vol. 13, Issue No. 2, July-2017, ISSN 2230-7540

An Analysis upon Various Basic Strategies of Group Theory: Fundamental Concept

Vijay Singh Digambar Gaikwad*

Assistant Professor

Abstract – The research reported in this paper explores the nature of student knowledge about group theory, arid how an individual may develop an understanding of certain topics in this domain. As part of a long-term research and development project in learning and teaching undergraduate mathematics, this report is one of a series of papers oil the abstract algebra component of that project.

We end the paper with a brief discussion of some pedagogical suggestions arising out of our considerations. We defer, however, a full consideration of instructional strategies and their effects oil learning these topics to some future time when more extensive research can provide a more solid foundation for the design of specific pedagogies.

---------------------------♦-----------------------------

INTRODUCTION

Most lectures on group theory actually start with the definition of what is a group. It may be worth though spending a few lines to mention how mathematicians came up with such a concept.

Around 1770, Lagrange initiated the study of permutations in connection with the study of the solution of equations. He was interested in understanding solutions of polynomials in several variables, and got this idea to study the behavior of polynomials when their roots are permuted. This led to what we now call Lagrange's Theorem. If a function f(x1, . . . , xn) of n variables is acted on by all n! possible permutations of the variables and these permuted functions take on only r values, then r is a divisior of n!. It is Galois (1811-1832) who is considered by many as the founder of group theory.

He was the first to use the term "group" in a technical sense, though to him it meant a collection of permutations closed under multiplication. Galois theory will be discussed much later in these notes. Galois was also motivated by the solvability of polynomial equations of degree n. From 1815 to 1844, Cauchy started to look at permutations as an autonomous subject, and introduced the concept of permutations generated by certain elements, as well as several notations still used today, such as the cyclic notation for permutations, the product of permutations, or the identity permutation. He proved what we call today Cauchy's Theorem, namely that if p is prime divisor of the cardinality of the group, then there exists a subgroup of cardinality p. In 1870, Jordan gathered all the applications of permutations he could find, from algebraic geometry, number theory, function theory, and gave a unified presentation (including the work of Cauchy and Galois). Jordan made explicit the notions of homomorphism, isomorphism (still for permutation groups), he introduced solvable groups, and proved that the indices in two composition series are the same (now called Jordan-H¨older Theorem). He also gave a proof that the alternating group An is simple for n > 4.

Apart permutation groups and number theory, a third occurence of group theory which is worth mentioning arose from geometry, and the work of Klein (we now use the term Klein group for one of the groups of order 4), and Lie, who studied transformation groups, that is transformations of geometric objects.

The work by Lie is now a topic of study in itself, but Lie theory is beyond the scope of these notes.

The abstract point of view in group theory emerged slowly. It took something like one hundred years from Lagrange's work of 1770 for the abstract group concept to evolve. This was done by abstracting what was in commun to permutation groups, abelian groups, transformation groups... In 1854, Cayley gave the modern definition of group for the first time:

"A set of symbols all of them different, and such that the product of any two of them (no matter in what order), or the product of any one of them into itself, belongs to the set, is said to be a group. These symbols are not in general convertible [commutative], but are associative."

In this| paper we hope to open a discussion concerning the nature of knowledge about abstract algebra, in particular group theory, and how an individual may develop an understanding of various topics in this domain. Our goal in making such a study is to eventually contribute to basic knowledge about human thinking as well as to serve the purposes of this specific area of mathematics. One way to do this is to introduce an increased degree of specificity to an analysis of student difficulties in understanding abstract concepts. Our present emphasis will be on interpreting the struggles of a class of in-service high school mathematics teachers as they tried to make sense out of a number of topics in group theory.

Of course, we are also interested in using these and other observations in the development of pedagogical strategies that can improve student success in learning abstract algebra. The work reported here is part of a long term research and development project in learning and teaching undergraduate mathematics.

We include, at the end, a brief discussion of some pedagogical suggestions arising out of our observations, but a full consideration of instructional strategies arid their effect 011 learning this subject must await future investigations yet to be conducted. Nevertheless, we offer the current discussion as an opening to what we hope becomes a continuing investigation of this important area.

Why Group Theory?

Abstract algebra in general, and group theory in particular, presents a serious educational problem. Mathematics faculty and students generally consider it to be one of the most troublesome undergraduate subjects. It appears to give students a great deal of difficulty, both in terms of dealing with the content and the development of attitudes towards abstract mathematics. The literature contains some reports that support this judgement, such as Hart, in press and Selden & Selden, 1987.

In many colleges, abstract algebra is the first course for students in which they must go beyond learning “imitative behavior patterns” for mimicing the solution of a large number of variations on a small number of themes (problems). In such a course, students must come to grips with abstract concepts, work with important mathematical principles, and learn to write proofs. Although there are no formal studies, many students report that, after taking this course, they tended to turn off from abstract mathematics. Since a significant percentage of the student audience for abstract algebra consists of future mathematics teachers, it is particularly important that the profession of mathematics education develop effective pedagogical strategies for improving the attitude of high school mathematics teachers towards mathematical abstraction.

There is another reason, related to abstraction, for the importance of abstract algebra in general and quotient groups in particular. An individual’s knowledge of the concept of group should include an understanding of various mathematical properties and constructions independent of particular examples, indeed including groups consisting of undefined elements and a binary operation satisfying the axioms.

Even if one begins with a very concrete group, the transition from the group to one of its quotients changes the nature of the elements and forces a student to deal with elements (e.g., cosets) that are, for her or him, undefined. This relationship between abstract groups and quotient groups has important historical antecedents (Nicholson, 2003).

GROUP AND SUBGROUP

In this section we suggest that an individual’s development of the concepts of group and subgroup may be synthesized simultaneously. Our observations are consistent with a progression in understanding that moves through various intermediate (and incomplete) ways of understanding groups and subgroups. That understanding may move from seeing groups and subgroups as primarily sets of discrete elements, to a stage where the operations as well as the group elements are incorporated into the necessary definition. Finally, a student may construct a thorough understanding of a group as an object to which actions can be applied.

It appears possible that some students try to deal with problem situations involving a set and an operation by assimilating the situations to an existing set schema, ignoring the operation which is also present. We suggest that such a strategy may represent an early misconception of the concepts of group and subgroup.

Groups as sets-

In the very first phase of learning the group concept, a student may interpret a group primarily in terms of its elements, that is, as a set. If the individual remains at this elementary understanding of groups, he or she may not distinguish a group by anything more than the number of elements in it.

One example of a student’s response which may indicate a strong emphasis on groups as sets of elements occurred when Kim was asked if $Z_{(i}$ were isomorphic to a S_3?[2] Kim says the following :

Kim: Probably so, S_3 has 6 elements in it and Z_6 has 6 elements in it, so without going through the whole procedure, 1 would say yes.

In addition to confusion about isomorphism, this student’s understanding seems to emphasize the number of elements as a characterizing feature of a group.

Thus, it may be that Z_3 is considered to be any set with three elements that is known to be a group. For example, in the written assessment and the interview, another student, Cal, variously considers Z_3 to be the set {0,1, 2}, {1, 2, 3}, {0, 2, 3}, or {0,2,4}.

Also consider Sue who answered Question 1(b) (on| subgroups of Z_6 on the written assessment, specifying a group by its elements; she wrote {10} for a subgroup of Z_6 with two elements and {2 10} for a subgroup of Z_6 with three elements.

At the earliest stages of understanding groups, the students may construct their own idea of group by considering familiar objects (elements of the group) and forming a process of associating these objects with each other in a set. Eventually, the students may encapsulate that process into an object which, for them, represents the group in question.

Subgroup as a subset-

Understanding a subgroup as a subset is similar to understanding a group as a set. For a student at this stage, sometimes "being a subset", that is, having all its elements included in a bigger set, is sufficient to conclude the existence of a subgroup. In other cases students require that such subsets of elements share a common property.

In looking for subgroups of D_3, many students correctly mentioned the "rotations". Similarly, but incorrectly, some listed "the flips" as a subgroup. Consider for example Cal who, in responding to Question 2(a) of the written assessment, listed the elements of D_3 as $\{R_0,R_1,R_2,D_1,D_2,D_3\}$ and identified the first three as the rotations and the second three as the flips. Then in responding to Question
2(c) he listed $\{R_0,R_1,R_2\}$ as a subgroup of D_A isomorphic to Z_3 and in responding to Question 2(d) he listed $\{D_1,D_2,D_3\}$ as a subgroup of D_3 also isomorphic to Z_3. In all cases, he mentions the correct operation. Here is what happens when the interviewer asks Cal about his choice of $\{D_1,D_2,D_3\}$ as a subgroup

I: And what about this out' here? You want it isomorphic t o Z3. What vou write he is $\{D_1,D_2,D_3\}$.

Cal: Yeah. I thought if you do them all...

I: The three flips.

Cal: Right.

I: You think it's a subgroup.

Cal: Well, like' you told me you have to have the same operation, it works on it the same as addition.

I: Well, that's not the point because it has to be a subgroup of this D_3. But is it a group at all under composition?

Cal: I thought it was. I didn't see anything that...I thought it was closed.

Individuals who have not progressed beyond this point would probably have no difficulty in considering the even integers to be a subgroup of Z. but they might also think that the odd integers were a subgroup as well.

This demonstrates a misconception caused by some students' efforts to construct a new concept (group) by relating it to a familiar concept (set). This is an example of reequilibration by assimilating the situation to existing available schemas before those schemas have been reconstructed to achieve a higher level of sophistication. It may happen that a student leaps over this step, or passes through it very quickly.
But nevertheless, as we witnessed above, some students exhibited vestiges of this misconception after five weeks (approximately 50 contact hours) of instruction in group theory.

ISOMORPHISM THEOREMS

The following theorems are useful in the classification of quotient groups of a given group G, or (vice versa) its normal subgroups.

Homomorphism Theorem. If $\varphi : G \to G'$ is a homomorphism, then

$$G/\ker\varphi \simeq \varphi(G).$$

Proof. Set $K = \ker\varphi$. We know $K \trianglelefteq G$. Define the map

$$\Phi : G/K \to \varphi(G)\, gK \mapsto \varphi(g)$$

The following proves the maps is well defined $(\Rightarrow)$ and injective $(\Leftarrow)$:

$$aK = bK \Leftrightarrow b^{-1}a \in K \Leftrightarrow \varphi(b^{-1}a) =$$
$$e' \Leftrightarrow \varphi(a) = \varphi(b) \Leftrightarrow \Phi(aK) = \Phi(bK).$$

Φ is trivially surjective (by construction), and it is a homomorphism because

$$\Phi((aK)(bK)) = \Phi(abK) = \varphi(ab) = \varphi(a)\varphi(b) = \Phi(aK)\Phi(bK).$$

Corollary. If $\varphi : G \to G'$ is a monomorphism, then $G \simeq \varphi(G)$

This is a straightforward consequence of the above theorem. We also achieve a classification of all cyclic groups:

Theorem. Every cyclic group of order $n \in \mathbb{N}$ is isomorphic to $(\mathbb{Z}_n, +)$, and every infinite cyclic group is isomorphic to $(\mathbb{Z}, +)$

Proof. Let $G = \langle a \rangle$ be cyclic. We have $G = \{a^m : m \in \mathbb{Z}\}$. The map $\mathbb{Z} \to G, m \mapsto a^m$ defines an epimorphism, with kernel $s\mathbb{Z}$ and $s = 0$ or the smallest positive integer such that $a^s = e$, i.e., $s = \text{ord } a = |G|$. The homomorphism theorem

implies that $G \simeq \mathbb{Z}/\{0\} \simeq \mathbb{Z}$ if G is infinite and otherwise $G \simeq \mathbb{Z}_s = \mathbb{Z}/s\mathbb{Z}$ with $s = |G|$•

First Isomorphism Theorem-

Let $H \leq G, N \trianglelefteq G$. Then $HN \leq G, (H \cap N) \trianglelefteq H$

and $HN/N \simeq H/(H \cap N)$.

Proof. Since N is normal, $aN = Na$ for all $a \in G$. So $HN = \bigcup_{h \in H} hN = \bigcup_{h \in H} Nh = NH$ and by Theorem HN is a subgroup. Note that $N \trianglelefteq HN$, and consider the restriction of the canonical epimorphism $\pi : G \to G/N$ to H, which we denote by $\pi_0 : H \to G/N, h \mapsto hN$. For the image,

$$\pi_0(H) = \{hN : h \in H\} = \{hnN : hn \in HN\} = HN/N.$$

Recall N is the identity in G/N, and $aN = N$ if and only if $a \in N$. So $\ker \pi_0 = \{h \in H : hN = N\} = \{h \in H : h \in N\} = H \cap N$.

Therefore $H \cap N$ is normal, and the isomorphism follows from the homomorphism theorem (take $\varphi = \pi_0$).

Second Isomorphism Theorem-

Let $K \leq H \trianglelefteq G, K \trianglelefteq G$. Then $H/K \trianglelefteq G/K$ and

$$(G/K)/(H/K) \simeq G/H.$$

Proof. Let $\varphi : G/K \to G/H, gK \mapsto gH$. We have $aK = bK \Rightarrow ab^{-1} \in K \subseteq H \Rightarrow aH = bH$, so the map is well defined. Evidently, φ is a homomorphism, with image $\varphi(G/K) = G/H$ and kernel

$$\ker \varphi = \{gK : gH = H\} = \{gK : g \in H\} = H/K.$$

The theorem now follows from the homomorphism theorem.

THE SYLOW THEOREMS

We look at orders of groups again, but this time paying attention to the occurrence of prime factors. More precisely, we will fix a given prime p, look at the partial factorization of the group order n as n = p^rm where p does not divide m, and study the existence of subgroups of order p or a power of p. In a sense, this is trying to establish some kind of converse for Lagrange's Theorem. Recall that Lagrange's Theorem tells that the order of a subgroup divides the order of the group. Here we conversely pick a divisor of the order of the group, and we try to find a subgroup with order the chosen divisor.

Definition. Let p be a prime. The group G is said to be a p-group if the

order of each element of G is a power of p.

Examples. We have already encountered several 2-groups.

1.We have seen in Example 1.15 that the cyclic group C_4 has elements of order 1,2 and 4, while the direct product C_2 × C_2 has elements of order 1 and 2.

2.The dihedral group D_4 is also a 2-group.

Definition. If |G| = p^rm, where p does not divide m, then a subgroup P of order p^r is called a Sylow p-subgroup of G. Thus P is a p-subgroup of G of maximum possible size.

The first thing we need to check is that such a subgroup of order pr indeed exists, which is not obvious. This will be the content of the first Sylow theorem.

Once we have proven the existence of a subgroup of order p^r, it has to be a p-group, since by Lagrange's Theorem the order of each element must divide p^r. We need a preliminary lemma.

Lemma. *If* $n = p^r m$ *where p is prime, then*mod p. *Thus if p does not divide m, then p does not divide* $\binom{n}{p^r}\binom{n}{p^r} \equiv m$

Proof. We have to prove that

$$\binom{n}{p^r} \equiv m \mod p,$$

after which we have that if *p* does not divide m, the $m \not\equiv 0$ mod *p* implying that $\binom{n}{p^r} \not\equiv 0$ mod *p* and thus *p* does not divide $\binom{n}{p^r}$

Let us use the binomial expansion of the following polynomial

$$(x+1)^{p^r} = \sum_{k=0}^{p^r} \binom{p^r}{k} x^{p^r-k} 1^k \equiv x^{p^r} + 1 \mod p$$

where we noted that all binomial coefficients but the first and the last are divisible by *p.* Thus $(x+1)^{p^r m} \equiv (x^{p^r}+1)^m \mod p$

which we can expand again into

$$\sum_{k=0}^{p^r m} \binom{p^r m}{k} x^{p^r m-k} \equiv \sum_{k=0}^{m} \binom{m}{k} (x^{p^r})^{m-k} \mod p.$$

We now look at the coefficient of x^{p^r} on both sides:

- on the left, take $k = p^r(m-1)$, to get $\binom{p^r m}{p^r}$,
- on the right, take $k = m-1$, to get $\binom{m}{m-1} = m.$

The result follows by identifying the coefficients of x^{p^r}. We are ready to prove the first Sylow Theorem.

Theorem. (1st Sylow Theorem). *Let G be a finite group of order p^{r}m, p a prime such that p does not divide m, and r some positive integer. Then G has at least one Sylow p-subgroup.*

Proof. The idea of the proof is to actually exhibit a subgroup of *G* of order p^r For that, we need to define a clever action of *G* on a carefully chosen set *X.* Take the set

$$X = \{\text{subsets of } G \text{ of size } p^r\}$$

and for action that *G* acts on *X* by left multiplication. This is clearly a well- defined action. We have that

$$|X| = \binom{p^r m}{p^r}$$

which is not divisible by *p* (by the previous lemma). Recall that the action of *G* on *X* induces a partition of *X* into orbits: $X = \sqcup B(S)$

where the disjoint union is taken over a set of representatives. Be careful that here *S* is an element of *X*, that is *S* is a subset of size p^r. We get

$$|X| = \sum |B(S)|$$

and since *p* does not divide $|X|$, it does not divide $\sum |B(S)|$, meaning that there is at least one *S* for which *p* does not divide $|B(S)|$. Let us pick this S, and denote by *P* its stabilizer.

The subgroup *P* which is thus by choice the stabilizer of the subset $S \in X$ of size p^r whose orbit size is not divisible by *p* is our candidate: we will prove it has order p^r.

$|P| \geq p^r$. Let us use the Orbit-Stabilizer Theorem, which tells us that

$$|B(S)| = |G|/|P| = p^r m/|P|.$$

By choice of the *S* we picked, *p* does not divide $|B(S)|$, that is *p* does not divide $p^r m/|P|$ and $|P|$ has to be a multiple of p^r, or equivalently p^r divides $|P|$.

$|P| \leq p^r$. Let us define the map $\lambda_x,\ x \in S,$ by

$$\lambda_x : P \to S,\ g \mapsto \lambda_x(g) = gx.$$

In words, this map goes from P, which is a subgroup of *G,* to S, which is an element of *X*, that is a subset of *G* with cardinality p^r. Note that this map is well-defined since $gx \in S$ for any $x \in S$ and any $g \in P$ by definition of P being the stabilizer of *S.* It is also clearly injective *(gx = hx* implies *g = h* since *x* is an element of the group *G* and thus is invertible). If we have an injection from P to 5, that means $|P| \leq |S| = p^r$.

PEDAGOGICAL SUGGESTIONS

For many students, their early mathematical career consists of learning algorithms to solve repetitive problems. With abstract algebra, the abrupt change in mathematical style from learning algorithms to understanding concepts and the overall complexity of the subject imply that this course, above all, is not likely to succeed if taught in a traditional manner. Indeed, it may be the case that abstract algebra is not very successful at most universities. Although there are no studies, anecdotal evidence tends to support this supposition. Thus, we have a situation in which it may be important to consider alternative, innovative instructional strategies.

REFERENCES

Aschbacher, M. AND Smith, S. D. (2004). The classification of quasithin groups. I, II, volume 111, 112 of Mathematical Surveys and Monographs. American Mathematical

Society, Providence, RI. Structure of strongly quasithin K-groups.

Besche, H. U., Eick, B., and O'brien, E. A. (2001). The groups of order at most 2000. Electron. Res. Announc. Amer. Math. Soc. 7: pp. 1–4 (electronic).

Breidenbach, D., E. Dubinsky, J. Hawks, & D. Nichols (2001). 'Development of the process concept of function', Educational Studies in Mathematics. pp. 247-285.

Dubinsky, E. & U. Leron (2003). Learning Abstract Algebra with ISETL, New York: Springer-Verlag.

Kaput, J. (2002). 'Patterns in students' formalization of quantitative patterns' in Harel & E. Dubinsky (Eds.), The Concept of Function: Aspects of Epistemology and Pedagogy. MAA Notes Series No. 25, Math. Assn. Amer., pp. 290-318.

Nicholson, J. (2003). 'The development and understanding of the concept of quotient group', Ilistoria Mathcmat ica 20. pp. 68-88.

Ronan, M. (2006). Symmetry and the monster. One of the greatest quests of mathematics. Oxford University Press, Oxford.

Rotman, J. J. (1995). An introduction to the theory of groups, volume 148 of Graduate Texts in Mathematics. Springer-Verlag, New York, fourth edition.

Sfard, A. (2002). 'Operational origins of mathematical objects and the quandary of reification — the case of function.in G. Harel & E. Dubinsky (Eds.), The Concept of Function: Aspects of Epistemology and Pedagogy. MAA Notes, No. 25, Math. Assn. Amer., pp. 59-84.

Corresponding Author

Vijay Singh Digamber Gaikwad*

Assistant Professor

E-Mail – vijaysinghgaikwad0@gmail.com