

Using Groups32 in Instruction

JOHN J. WAVRIK

Department of Mathematics
University of California – San Diego
La Jolla, CA 92093 USA
email: jjwavrik@ucsd.edu

This article discusses the process of integrating the use a software system into a conventional course in Abstract Algebra. It is a description of how and why a software system was used. It uses a particular system, Groups32, as an example.

1. Introduction

This article is intended to be read in conjunction with Groups32, a software system accessible on the Internet [3].

Abstract algebra is a problematic course. For many potential mathematics majors it is the first course which deals with an abstract subject matter. For many it is the first course where proof is prominent. It marks a major departure from earlier courses in content and presentation. There are many reasons why students have difficulty with abstract algebra. The purpose and orientation of the course is unfamiliar: rather than learning to perform computations, students are expected to prove theorems. Rather than solving problems using memorized templates, students are expected to develop an original approach to non-routine problems. Students must develop appropriate mental images in an effort to conceptualize a large bestiary of varied and unfamiliar objects. They must modify and discard schemas built on years of experience. Students must examine, modify (and in some cases abandon) modes of thought and procedure which have served them, with varying degrees of success, during their previous academic career.

Let us step back and take a broad view of the learning and teaching of abstract algebra. The objects of abstract algebra (groups, rings, fields, vector spaces as well as related concepts like cosets and quotient groups) are conceptual objects. They are objects in the sense of having reality, but are distinguished from physical objects in the sense that they exist in thought. The process of learning abstract algebra is a process of developing ways to think and manipulate these objects: endowing them with a solidity and familiarity that one might have with physical objects or with persons. The problem of learning is to make conceptual objects seem real. One can give formal definitions, but the reality of a conceptual object is not in the formal definitions. One can give examples, but the reality of a conceptual object is not in examples. One can give properties of a conceptual object, but the reality is not in the properties. One can give connections between properties, but the reality is not in the connections. Yet the formal definitions, examples, properties, and connections contribute to the development of the sense of reality of a conceptual object. Students experience problems both with finding suitable ways to think about algebraic objects themselves and with fitting together rela-

tionships among the objects, their properties, and operations on them. Part of the learning problem is a matter of expectation. Conceptual objects do not assume a full-blown immediate reality (as students expect). They instead become more distinct as we come closer to them in the fog. Students do not realize that they must develop a pattern of activity that assists in the process of making clarity emerge. They are accustomed to memorizing features and methods. The learning difficulty is compounded by a traditional style of presentation: material is presented in an order dictated by logic rather than importance. Thus, for example, we introduce (axiomatically) the definition of a group. Typically the first theorem proved is that the identity of a group is unique. Surely many students wonder why we are taking such interest in this particular factoid when they still have no real reason to be interested in groups. Many students do eventually learn to cope with the subject, but few students catch on quickly. It would be useful to see how the subject appears to a student initially, and what separates the students who become successful from those who do not.

2. A Metaphor

In this article we will look at the problem of learning one part of abstract algebra: group theory. We will not, however, examine particular concepts or theorems in an effort to determine what learning problems they pose. We will, instead, develop a metaphor to understand the problem of learning the subject – and discuss, in terms of that metaphor, ideas for overcoming the problems.

A useful metaphor is for us to see a class in abstract algebra as a first visit to a strange and unfamiliar country. Everything seems alien. The inhabitants dress differently, they speak an unfamiliar language, they have a different culture and customs, they eat different foods. The geography is new to our tourists, it is hard for them to get their bearings. They are in far away places with strange sounding names. Most of the tourists have no idea of what is available in these places and where things are located. It is a task just to find a restroom and return to the group after visiting it. None of the tourists initially feel at home.

So our approach is to take the tourists on a bus tour. Our intent is to provide some exposure to the interesting things about the geography, language, and culture. Like a bus tour, we are constrained by the fact that we must follow a road. Some of the features we really want them to see lie further down the road – so we must wait until we reach them in our tour.

We travel in a landscape full of richly interesting things. The sun is shining. We, as the tour guides, have trained ourselves to present with enthusiasm. We know the land very well – so we can tell the tourists what they will see on the left and right before we get there. We even have a repertoire of jokes and folksy stories that we have polished by having told them many times. We can try to keep up their spirits by describing some of the things they will be seeing in the future.

Unfortunately, it never quite seems to work. Very few of the tourists show signs of acquiring real familiarity with the country. At best a few can parrot back some

things they memorized from the guidebook or from our description. Many cannot recall if the ancient church was in Upswyth or Downswyth. Some don't even remember that we had passed an ancient church!

There are very good reasons for this phenomenon. First, we are taking tourists on a brief bus tour through a country we have explored over a period of many years. We have explored on foot, by bike, and by car. Our tourists rarely get off the bus. Second, we assume that because the sun is shining for us, it is shining for them. For many tourists, who are taking their first tour of a theoretical subject, the trip is taking place in the middle of the night. They are relying on our description of things they are not really seeing for themselves. Most have never had the experience of finding a strange new country gradually become familiar. Thus they do not have the expectation that everything will eventually become clear. Some tourists do not even try to assimilate. They believe that their task is just to remember some of the statistics we mention in passing (population size, rainfall, etc) and to learn a few phrases of the native language.

It is expected that tourists bring perspectives and understandings rooted in their native country. They expect the food to taste like the food they have at home; the music to sound like that to which they are accustomed; and the same social protocols to be operative. Americans expect that everyone speaks English but they have little opportunity to find out about what the natives speak: they don't meet any real people – they just see them through the bus window.

Our tour is not a total disaster. There are several of our tourists who will become so interested and well-oriented that they will be able to come back next year and hitchhike around the country. A bus tour often is a good way to make a first acquaintance with a new country. It is a success if it provides tourists with the desire and ability to explore more extensively on their own. Unfortunately very few tourists reach this stage.

There is no doubt that students in an abstract algebra class provide examples of faulty reasoning, misconceptions, etc. A facile explanation is that intelligence accounts for the difference between successful and unsuccessful students. It can be persuasively argued that some of the learning problems stem from a faulty presentation of the subject. We often do not recognize the importance of presenting mathematics so that students perceive it satisfies an “intellectual need” [2]. We often chose notation that, in the interest of precision, inhibits the formation of good conceptualization (see [1] for a discussion of the connection between symbolism and conceptualization). We almost always present mathematics in a way that the things that are most interesting and important come later.

At the end of it all, however, the differences between successful and unsuccessful students stem mostly from the way students approach learning. A bus tour can be a very passive experience. Good students make for themselves “off the bus” experiences. They examine artifacts and architecture, they try to meet some of the

natives and attempt to speak their language. The weaker students mainly look at the features and inhabitants through the bus window.

It is not the intent of this article to present a complete revision of the way that abstract algebra is taught or notated. It is rather to introduce the use of a software system (Groups32) which can be used in conjunction with a traditional course in abstract algebra. Its purpose is to help more students have productive "getting off the bus" experiences. It can be used to exploit and develop students' growing awareness of the theory and increase their acquaintance with the populace.

Group theory is usually the part of abstract algebra which is presented first. It is a good introductory subject since each finite group has a personality, so groups can be fun to meet individually. It is also a subject which justifies theory. Amazing truths can be established in a few lines of proof. Groups of small order can be made accessible, and the power of theory can be exhibited. Group Theory is usually presented in a manner consistent with the presentation of the rest of abstract algebra. Thus students who have come to grips with this part of the subject usually do well at the rest.

3. Introducing Groups32

Groups32 is, underneath, a software system and language designed for elementary group theory. It provides an electronic representation of the objects of interest (groups, sets, subgroups, permutations, etc.) and implements a set of fundamental algorithms. It also provides a programming language designed to make it easy to "talk" to the computer about groups and to allow the system to be extended. In this form, the underlying system is very much like a research system. Groups32 represents internally groups of order 1-32 as multiplication tables (there are 144 of them). Information about the groups is computed "on the fly" using algorithms designed for this representation. The system has a package which can produce tables from a permutation representation. It also can search the groups to find those having given generators and relations. It connects with the way groups are treated at the undergraduate/beginning graduate level.

Groups32 is accessible on the Internet at <http://math.ucsd.edu/~jwavrik/g32/>. It is assumed that the reader will use the program while reading this article. Thus we indicate things to do but not reproduce the complete dialog.

Integrating software into instruction poses several problems. The software must cover enough to justify introducing it. Research software, however, often has a steep learning curve. It can pose a serious problem if learning how to use the software becomes the focus of the course. A critical problem is the design of a user interface which makes the software accessible and useful. Thus an important design criterion for Groups32 was *ease of use*. During the 5 year testing of Groups32 it became clear that students were using Groups32 more like a calculator than a programmable software system. Very few students made efforts to program the system (even though they were provided with information to do so).

Speed and flexibility became the important factors in the current user interface. It appeared to be less important to make available the programming features. For reasons of security programming is not available in the Internet version [3].

The interface presents the user with a table of commands:

CENTER	CENTRALIZER	CHART	CONJ-CLS
COSETS	EVALUATE	GENERATE	GROUP
HELP	INFO	ISOMORPHISM	LEFT
NORMALIZER	ORDERS	PERMGRPS	POWERS
QUIT	RESULT	RIGHT	SEARCH
STOP	SUBGROUPS	TABLE	X

To carry out a command, the user needs only to type enough letters to distinguish it from other commands. When this happens, the system will automatically complete the command and prompt for any parameters needed. It is not necessary for the user to count letters, just to notice when the system has completed the command and has moved to the next step. The CHART command, for example, makes a chart of groups of a given order (or all groups listed by order). This command will be executed as soon as the user types CH. It will prompt for the desired order:

```
G1>> CHART   Order of Groups (1-32 or 0) Number 12
      20   21   22*  23*  24*
           There are 5 Groups of order 12
           2 abelian and 3 non-abelian
```

Here we have underlined what the user must type, everything else is produced by the system.

A chart showing the numbers of all of the groups in the system, sorted by order, can be found using the CHART command with 0 as the parameter.

4. Using Groups32

Harel [2] stresses the importance of students having an "intellectual need" for the things they are learning. We introduce the study of group theory (the bus tour) by establishing one way of conceptualizing and by providing something students (tourists) can look for as they travel. A group can be thought of as corresponding to a multiplication table (Cayley table). Some important facets of group theory can be connected to questions about tables. In this section we show how to establish an intellectual need for some of the things we plan to teach. This approach provides a degree of organization for learning.

A group can be thought of as corresponding to a multiplication table (Cayley table). Groups will eventually arise in other ways and a table will be an inadequate tool for a human to use for gathering information. However, a table is a good way

for students to begin conceptualizing. One can immediately notice that the multiplication defined by some tables may have special properties. Some tables, for example, define a commutative operation and others do not. The properties of an operation which define a group are reasonably natural requirements. We point out that students know examples of infinite groups.

Now we are going to ask a significant question. How many ways are there to fill in a table of a given size to get a group? We have posed a problem which can be easily understood. Every student can play with filling in tables. Every student learns some things about groups in the process.

There is only one way to fill in a 1×1 table. We can convince ourselves that there are two ways to fill in a 2×2 table to get a group (depending on which element is the identity). At this point we can naturally introduce the idea of isomorphism: two tables are isomorphic if one is obtained from the other by renaming the elements.

The task of filling in a 3×3 table is already complicated. We can ask how many 3×3 tables there can be (i.e. how many ways to fill a 3×3 grid with letters A,B,C). The answer is 19,683. It is already quite clear that we will not get far by forming all possible tables and then checking which are groups!

Here a simple first theorem helps: a group table must have different elements in each row and column. With this theorem we find that there is (up to isomorphism) only one group of order 3. This is a theorem with a purpose. It supplies some useful information about the task of filling in tables.

Something interesting happens for 4×4 . There are four possible tables if we use letters A,B,C,D for elements and make A the identity:

Table 1 <u> A B C D </u> A A B C D B B C D A C C D A B D D A B C	Table 2 <u> A B C D </u> A A B C D B B A D C C C D A B D D C B A
Table 3 <u> A B C D </u> A A B C D B B D A C C C A D B D D C B A	Table 4 <u> A B C D </u> A A B C D B B A D C C C D B A D D C A B

The problem is to see that one of these tables is not like the others – while the other three tables are kinda the same. It is in fact possible to obtain tables 1,3,4 from each other by renaming the elements. Table 2, however is essentially different. Students should be able to see these things and explain why, no matter how you rename, you cannot get table 2 from table 1. (Students can come up with the fact that the square of any element in table 2 is the identity and that this property is preserved under isomorphism.)

Finding a systematic way to generate the 4×4 tables and showing that these are the only that can occur is, in itself, an interesting problem. How many groups there can be of various orders seems an interesting thing to ask. It becomes abundantly clear that we cannot deal with this by trying to fill in tables – so how can we do it? How can we decide whether or not two groups are isomorphic? The work so far indicates that we will try to find properties that are preserved under isomorphism. What are some of these properties?

We have introduced the group concept in a way that provides a focus for learning and accessible mental images. We have introduced the concept of isomorphism in a natural setting. We have started dealing with some interesting problems. We have illustrated how the use of theorems can give us valuable information. We have provided our tourists with some things to look for: how groups come about; properties which distinguish groups; how many groups are there of each order.

Groups32 provides another interesting observation: Using the CHART command (with input 0) we see that there is only one group of order n for each of the following n (between 2 and 32): 2,3,5,7,11,13,15,17,19,23,29,31
Why is this? We are led to make a conjecture that if n is prime there is only one group of order n (up to isomorphism). How to prove this. Why is 15 in this list?

Groups32 eventually turns out to be a source of observations as well as a toolkit for getting information about groups. The important thing is that we can quickly

start our bus tour with the tourists having something to look for in the things we see along the way. The most powerful thing about this type of presentation, however, is that we can manage to get students to appreciate why we want to prove theorems.

5. Making Observations

The idea that every element has an order (defined in the usual way) is not obvious. Why, when we take powers of an element x , why must we eventually get to the identity? Couldn't the powers just jump around among the non-identity elements? A nice thing is to ask students to prove this can't happen: if x is an element in a finite group, there must always be a first power of x which is the identity. Now use the POWERS command to check the powers of an element in a group of prime order. Determine the orders of all the elements of some of the smaller groups by hand (using the table, for example). Finally use the ORDERS command to list the elements of a given group by order. Here are the orders for elements of the two groups of order 6.

```
G8>> ORDERS    for Group Number 7

Group number 7 of Order 6
  1 elements of order 1:  A
  1 elements of order 2:  D
  2 elements of order 3:  C E
  2 elements of order 6:  B F

G7>> ORDERS    for Group Number 8

Group number 8 of Order 6
  1 elements of order 1:  A
  3 elements of order 2:  D E F
  2 elements of order 3:  B C
  0 elements of order 6:
```

Notice that group 7 has two elements (B,F) of order 6 – so the entire group consists of the powers of these elements. Group 8 has no such elements. Neither group has an element of order 4 or 5. A good, tough, brute force problem is to give a reason why a group of order 6 cannot have an element of order 4 or of order 5.

Perhaps there is some way to see, at this point, that for a group of prime order p , all non-identity elements have order p . If so, it would then provide some closure to introduce the concept of a cyclic group and show that any two cyclic groups of the same order are isomorphic. Otherwise we will need to wait until we prove Lagrange's Theorem.

If there is any one thing that using Groups32 has done for the course, it is to put students in a position to see things, make conjectures, and find proofs or counter-examples. The same course was taught from the same book prior to use of Groups32. It appears that "off the bus" experiences using Groups32 have changed the matter. There is less a sense of performing magic tricks for people who haven't a clue as to what you are doing or why. There is more a sense that of being able to communicate a rationale for the subject very early on. It makes students more active in the process of learning.

6. Lagrange's Theorem

The usual proof of Lagrange's theorem is very simple, very slick, and very unfortunate. It is presented early. It is unfortunate that students get the impression, two weeks into the course, that we have entered an area accessible only to those with supreme intellect. If there is any way to convince students that there is a jungle out there, and that they should not try to get off the bus, it is to present Lagrange's theorem in the usual way.

Cosets, equivalence relations, and a counting argument are put together as a kind of *Deus ex Machina*. We spend time explaining the details, but not how anyone would have thought of putting these things together in this way.

It is worthwhile to have students think first about a special consequence of Lagrange's theorem: a group of order 5 cannot have an element of order 3. The proof is to show that if there is an element, x , of order 3 then e, x, x^2 are distinct. There must be an element y not one of these. And that e, x, x^2, y, yx, yx^2 would be distinct (use the cancellation laws). This would make 6 different elements but we only can have 5. In a similar way we can show that there can be no elements of order 2 or 4. From this we can show that there is only one group; of order 5. We note that this is far superior to trying to fill in multiplication tables.

Once the concept of partitioning is at hand, the concept can be formalized and students can use Groups32 to look at other groups. Notice that in the case above we have partitioned G into cosets of the subgroup $H = \langle x \rangle$. The coset concept with the related idea of partitioning into equivalence classes begins to emerge from the chaos – rather than springing full blown from the head of Zeus (or Lagrange). Use of the SUBGROUPS and COSETS commands take the "edge" off the formal proof. It is even possible to use the EVALUATE command to see how the cosets are obtained. The concept of a coset can be clarified. The fact that the cosets partition a group and have the same number of elements can be observed.

```

G8>> COSETS    of subg generated by set: { e }

    Left Cosets                Right Cosets
    { A E }                    { A E }
    { B D }                    { B F }
    { C F }                    { C D }

The subgroup { A E }  is NOT a NORMAL subgroup

G8>> EVALUATE   (use ' for inverse) ba= B
G8>> EVALUATE   (use ' for inverse) be= D
G8>> EVALUATE   (use ' for inverse) ca= C
G8>> EVALUATE   (use ' for inverse) ce= F

```

After we have taken this gentle back door approach to Lagrange's theorem (rather than a frontal assault) we can settle the matter of why there is only one group of order n when n is prime. Why there is only one group of order 15 will need to wait.

The SUBGROUPS command is eventually used for more sophisticated study of the structure of subgroups. There are matters like why certain subgroups must be normal; the implications of this; Sylow subgroups (existence and number); etc.

7. Identifying Groups // Isomorphism

An interesting use of Groups32 is to identify which numbered group correspond to examples that come up in the text. Students are asked to keep a journal with a page for each group of order 1-15 (there are 28 of them). They write down things they have learned about each group – particularly any "common names". One tool for discovery is the PERMGROUPS subpackage. It allows groups to be generated by permutations and, if they have order up to 32, to be "installed" into the main program and studied.

```

PERM>> CREATE
Subgroup of Sn -- what is n?  Number 3
      Put in generators as product of cycles.
      End with a blank line
Generator (1 2)
Generator (1 2 3)
Generator
Group is of order 6
A ( )      B (2 3 )      C (1 2 )
D (1 2 3 )  E (1 3 2 )      F (1 3 )

PERM>> INSTALL
      Install as table k (1..5)  Number 1
PERM>> MAIN

```

We have created the symmetric group S_3 . It is now installed as group number 1. The correspondence between letters and permutations is shown above.

```
G1>> ORDERS    for Group Number 1
Group number 1 of Order 6
  1 elements of order  1:  A
  3 elements of order  2:  B C F
  2 elements of order  3:  D E
  0 elements of order  6:
```

Notice that this distribution of orders is like that which we have seen in group 8, but not like group 7. Groups32 provides an ISOMORPHISM command which lets us try mappings between groups to find an isomorphism. An isomorphism must preserve the orders of elements. An isomorphism is determined once we know the image of the generators (a concept not introduced formally at this point). The ISOMORPHISM command makes this visible since once an element is mapped to the target group, all consequences of the mapping (all products of currently mapped elements) are filled in.

While on this subject, let us try to identify which numbered group is the group of symmetries of a square. It is not hard to turn the geometric representation into a permutation representation. Students should recognize that every symmetry of a square can be described by a permutation of the four vertices (but that not every permutation gives a symmetry):

```

PERM>> CREATE
Subgroup of Sn -- what is n? Number 4
Put in generators as product of cycles.
End with a blank line
Generator (1 2 3 4)
Generator (1 3)
Generator
Group is of order 8
A ( )          B (2 4 )          C (1 2 )(3 4 )
D (1 2 3 4 )  E (1 3 )          F (1 3 )(2 4 )
G (1 4 3 2 )  H (1 4 )(2 3 )
PERM>> INSTALL
Install as table k (1..5) Number 1
PERM>> MAIN
G1>> ORDERS for Group Number 1
Group number 1 of Order 8
1 elements of order 1: A
5 elements of order 2: B C E F H
2 elements of order 4: D G
0 elements of order 8:

G1>> SUBGROUPS of Group Number 1
... wait
* = Normal subgroup
Generators          Subgroup
0 { }               *{ A }
1 { B }             { A B }
2 { C }             { A C }
3 { E }             { A E }
4 { F }             *{ A F }
5 { H }             { A H }
6 { B E }           *{ A B E F }
7 { D }             *{ A D F G }
8 { C F }           *{ A C F H }
9 { B C }           *{ A B C D E F G H }

```

A good "off the bus" experience is to examine the subgroups and elements in the context of the geometry. Geometry is a way some groups naturally arise. The center of this group is {A,F}. Why is $F = (1\ 3)(2\ 4)$ the only symmetry (besides the identity) which commutes with everything? Notice that F is actually a rotation – but it is a combination of two flips. Notice in passing that there are 3 subgroups of order 4, and all are normal. This is a good example to keep in mind later, for those students who believe that the Sylow subgroups of a group of order 8 must have order 4. Notice that only one of the subgroups of order 4 is cyclic. Notice that the group is not abelian. How can these things be seen geometrically?

8. Classifying Groups

It should be apparent that, for each order n from 1 to 32, there are only a relatively small number of groups (up to isomorphism). It is useful to try to identify groups with special properties. By now the students should know (and be able to prove) that there can only be one cyclic group of order n for each n . An "off the bus" experience is to examine all of the groups numbered 1-28 to identify which is cyclic. The cyclic groups can also be located using the SEARCH command. Here we specify that a group is to have one generator, but we do not specify its order. The result is a list of all the cyclic groups. Similarly the SEARCH command can be used to find all dihedral groups. We require two generators x, y . We do not specify an order for x but we require y to have order 2. The relation is $yx = x^{-1}y$. Notice that the group of symmetries of the square is in this list.

How does one show that there can only be 2 groups of order 6? Or 5 groups of order 8? This information can be obtained from Groups32 – but students should understand that someone had to know how to classify the groups before Groups32 could be constructed.

Classification is a good "off the bus" experience. In the process, a whole host of ideas can be brought to bear: special properties of groups; ways to represent groups; theorems about groups and their subgroups; etc. Along the way students will notice that neither the permutation representation of a group nor its description in terms of generators and relations is unique. Thus a problem is how to efficiently tell if two groups, presented in different ways, are isomorphic. (It might be of interest to note that groups of order up to 15 can be distinguished by the distribution of orders of their elements).

This classification problem has the virtue of having many levels. Every student in the class should be able to explain why \mathbb{Z}_6 and $\mathbb{Z}_2 \times \mathbb{Z}_3$ are actually the same group. Or, for that matter, why $\mathbb{Z}_2 \times \mathbb{Z}_3$ and $\mathbb{Z}_3 \times \mathbb{Z}_2$ are the same – but yet $\mathbb{Z}_2 \times \mathbb{Z}_2$ and \mathbb{Z}_4 are not the same. On the other hand, showing that there are 5 groups of orders 8, 12 and 20 and describing how they are obtained is more substantial.

Students should now be able to classify groups of order pq (p, q are primes) and finally settle the problem of why there is only one group of order 15.

During most of the course, students use Groups32 as a calculator to gather information, test conjectures, and find counterexamples. There should be no need to give step-by-step worksheets. Students should use Groups32 to explore in a free-form way. The instructor might raise questions or respond to observations students make.

9. Summary

It has been found useful to integrate computer use in teaching an abstract course. Groups32 has been designed to be instructionally non-invasive. It is easy to learn to use, is useful for the entire topic of group theory, and it can be integrated into traditional courses. It can help overcome one of the major barriers to learning: that students do not acquire sufficient intimacy with most mathematics they study. Groups32 has allowed students to experiment, work out details of examples, etc. in a way that would be very time-consuming with pencil and paper. The subject, and particularly its theoretical parts, starts to make sense to them.

10. References

- [1] HAREL, GUERSHON and KAPUT, JAMES, 1991, *The Role of Conceptual Entities and their Symbols in Building Advanced Mathematical Concepts*, Advanced Mathematical Thinking, D. Tall (Ed), Kluwer Academic Publishers, pp. 82-94.
- [2] HAREL, GUERSHON, 1998, *Two Dual Assertions: The First on Learning and the Second on Teaching (or Vice Versa)* American Math Monthly, pp. 597-507.
- [3] WAVRIK, JOHN , 2000, *Groups32* (computer program) accessible at <http://math.ucsd.edu/~jwavrik/g32>