Looking at Groups

John W. Jones
jj@asu.edu
School of Mathematical and Statistical Sciences
Arizona State University
Tempe, AZ 85287
USA

Abstract

We describe a piece of web-based software for use in abstract algebra courses, and several ways it can be used to help students work with examples of groups to understand concepts of the course.

Every math teacher knows that working with examples is important. That said, math teachers may underestimate the importance of examples in their teaching. Mathematicians are particularly adept at thinking abstractly – it is their stock in trade. However, psychologists have found that in general, people naturally generalize from specific examples more readily than they make simple logical deductions. Nisbett and Borgida [2] summarize their findings: "Subjects' unwillingness to deduce the particular from the general was matched only by their willingness to infer the general from the particular".[1] Human thinking works much more easily in the wrong direction from what is needed for mathematical rigor. The implication is that use of examples is much more important than one would think.

Here we describe various ideas in group theory which can be illuminated by looking at group tables and subgroup diagrams of specific groups. Technology can facilitate the process by giving students ready access to many groups. There are different tools one may use. We will describe the Group Calculator, a web-based tool which allows the user to work with a fairly large collection of groups, including all groups of order less than 32. This puts a wealth of examples at the fingertips of students.

The only other software we are aware of with the same capabilities, whether free or commercial, needs to be installed on the user's computer. Web-based software does not depend on the user's operating system, available memory, or the willingness/ability to install the software. It can be used from a public computer, or a friend's machine with no hassle.

The Group Calculator can be accessed at `http://hobbes.la.asu.edu/groups/groups.html`. It is free to use, and runs as javascript in the user's web browser. There are no plug-ins required making it effectively platform independent. One only needs a web connection and a computer. The

[1] See Kahneman [1] for a discussion of this research.

usual barriers to having students access mathematical software have been removed as much as possible. Section 1 describes features of the Group Calculator. The remaining sections discuss various applications to the study of group theory. Due to space limitations, we will not discuss every feature and how it can be used.

1 The Group Calculator

In this section we describe some of the features of the Group Calculator as background for the later sections.

1.1 Choosing a group

First, one needs to have some examples of groups at their disposal. The Group Calculator allows the user to select a group from one of several families: cyclic group of order n, dihedral group D_n of order $2n$, the group $\mathbb{Z}_n^*$ of units modulo n, the abelian group $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$, and the affine group $\text{Aff}(\mathbb{Z}_n) = \{ax + b \mid a \in \mathbb{Z}_n^* \text{ and } b \in \mathbb{Z}_n\}$ under composition. The affine groups may not be familiar to some people, even those who teach abstract algebra. However, they give good examples of modest sized non-abelian groups. After students get acquainted with them through the Group Calculator, they can do interesting exercises involving them.[2]

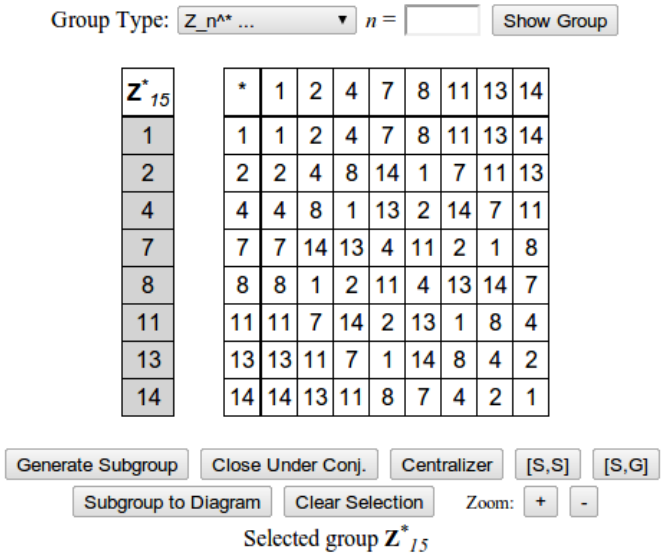
Additionally, the Group Calculator allows the user to select "By order..." for "Group Type". The user selects the group order from a menu ranging from 1 to 31, and can then select a group from a menu of all groups of that order up to isomorphism. In addition to giving easy access to these groups, this feature has several other advantages. Browsing groups by order helps give students a sense of how simple/rich the set of groups of order n are, depending on n. Right from the beginning, if directed to look at groups of prime order, most students can conjecture that there is a unique such group up to isomorphism, and they can see that conversely, the number of groups tends to be large with the order is divisible by a big power of a prime. Finally, seeing that the number of groups is usually fairly modest makes the set of groups (up to isomorphism) seems less daunting. It also motivates one of the basic problems in group theory — to classify the finite groups of each order.

Usually elements of groups are shown in their natural notation. The Group Calculator also allows one to pick a "Mystery Group" by specifying a bound on its order and an index. The program then uses this information to select a group whose order is in the specified range, but then it renames and shuffles its elements. The identity will be listed first and denoted by e, but the other group elements are simply named a, b, c, d, f,... The output is deterministic, so that a pair (B, j) where B is the bound for the order and j is the index will always present the same group in exactly the same way. This can be used in exercises where the instructor either wants students to identify a group, or to answer other questions about a group where the names of elements might give away too much information.

[2]For example, one can deduce the formula for the inverse of an element of $\text{Aff}(\mathbb{Z}_n)$, prove that $H = \{ax \mid a \in \mathbb{Z}_n^*\}$ and $N = \{x + b \mid b \in \mathbb{Z}_n\}$ are subgroups, that N is a normal subgroup of $\text{Aff}(\mathbb{Z}_n)$, but that H is not a normal subgroup for $n \geq 3$. Moreover, students can use information from the group calculator to identify $\text{Aff}(\mathbb{Z}_n)$ for $n \leq 4$ and $n = 6$ (which are isomorphic to familiar groups best known by other names). Finally, one can use use these groups to construct other interesting groups, such as the non-abelian group of order 21 which is a subgroup of $\text{Aff}(\mathbb{Z}_7)$.

1.2 Group tables

Figure 1 shows the Group Calculator after the user has selected $\mathbb{Z}_{15}^*$. In the center is the group table,



Z^*_{15}	*	1	2	4	7	8	11	13	14
1	1	1	2	4	7	8	11	13	14
2	2	2	4	8	14	1	7	11	13
4	4	4	8	1	13	2	14	7	11
7	7	7	14	13	4	11	2	1	8
8	8	8	1	2	11	4	13	14	7
11	11	11	7	14	2	13	1	8	4
13	13	13	11	7	1	14	8	4	2
14	14	14	13	11	8	7	4	2	1

Figure 1: The group $\mathbb{Z}_{15}^*$.

with the identity listed first. On the left is a column listing elements of the group. The user can select/unselect elements by clicking on them in this column. At the bottom are various operations one can perform on the selected elements. The most common operation comes first, *Generate Subgroup*. For example, if the user clicks on one element from the left column and then *Generate Subgroup*, they get the cyclic subgroup generated by that element.

Figure 2 shows two screenshots; both are the results of producing cyclic subgroups of $\mathbb{Z}_{15}^*$. In each

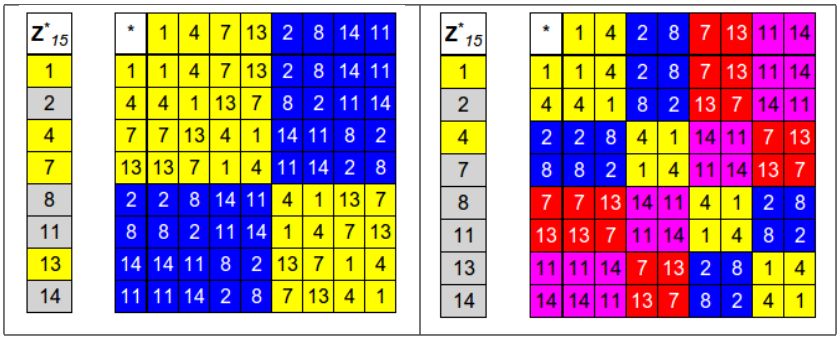


Figure 2: The group $\mathbb{Z}_{15}^*$ with the subgroups selected: $\langle 7 \rangle$ on the left and $\langle 4 \rangle$ on the right.

case, all elements of the subgroup are highlighted in the left column, but there are bigger changes to the group table.

First, the elements of the group table are now in a different order — they are grouped by left coset of the selected subgroup. The identity element comes first, so the subgroup itself is listed first.

Second, elements in the table are colored based on their coset. So, the group table for the subgroup will be shown in the upper left-hand corner of the group table, highlighted in yellow, making it easily accessible. We will discuss other uses of this in the sections below. This feature can be used to study the cyclic subgroups of a group, but of course, can be used to generate subgroups from larger subsets of a group's elements.

The other buttons after *Generate Subgroup* perform the following actions. In each case, we denote by S the set of elements selected before clicking the button.

- *Close Under Conj.* finds all conjugates of elements of the selected set by elements of G: $\{gsg^{-1} \mid g \in G \text{ and } s \in S\}$
- *Centralizer* finds elements of G which commute with every selected element: $\{g \in G \mid gs = sg \text{ for all } s \in S\}$
- *[S,S]* finds commutators using elements of S: $\{s_1 s_2 s_1^{-1} s_2^{-1} \mid s_1, s_2 \in S\}$
- *[S,G]* finds commutators of elements of S with elements of G: $\{sgs^{-1}g^{-1} \mid s \in S \text{ and } g \in G\}$

Note that of these constructions, only the centralizer is guaranteed to give a subgroup. Consequently, clicking on *Centralizer* triggers the reordering of the group table and coloring of left cosets. The other buttons simply change the set of elements in the left column which are highlighted.

The second row of buttons allow the user to clear the selections and reset the table (*Clear Selection*), and to zoom in or out on the group table (without applying the zoom to the rest of the web page). It can be useful to zoom out on larger groups. Finally, it contains the button *Subgroup to Diagram* which jumps to the subgroup diagram of the group, and if there is a subgroup selected, it is highlighted in the diagram.

1.3 Subgroup diagrams

The second view of a group provided by the Group Calculator is its subgroup diagram. One can access it by loading its group table, and then either clicking on *Subgroup to Diagram* at any time, or by clicking on the *Subgroup Diagram* tab at the top of the calculator. In the latter case, one may then have to click *Show Diagram* for the program to generate the diagram.

Figure 3 shows the subgroup diagram for D_5, the dihedral group of order 10, with one subgroup selected. The diagram shows all of the subgroups with relevant inclusions. Each subgroup is given a label of the form dNk where d is the order of the subgroup, and k is an index which counts the subgroups of order d. The notation is a mnemonic for "subgroup of order d Number k".

Subgroups are represented by diamonds if they are normal, and by circles if they are not. Conjugate subgroups are always positioned next to each other. The user can drag subgroups around the screen, which is especially useful with complicated diagrams. In doing so, conjugate subgroups will move together, so dragging a subgroup can clarify if two subgroups are conjugate, or simply next to each other by accident.

If a specific subgroup is clicked on, it is highlighted and a little more information is given to the left of the diagram. As shown in Figure 3 where subgroup 2N5 is highlighted, the size of the subgroup and a minimal generating set is shown on the left.

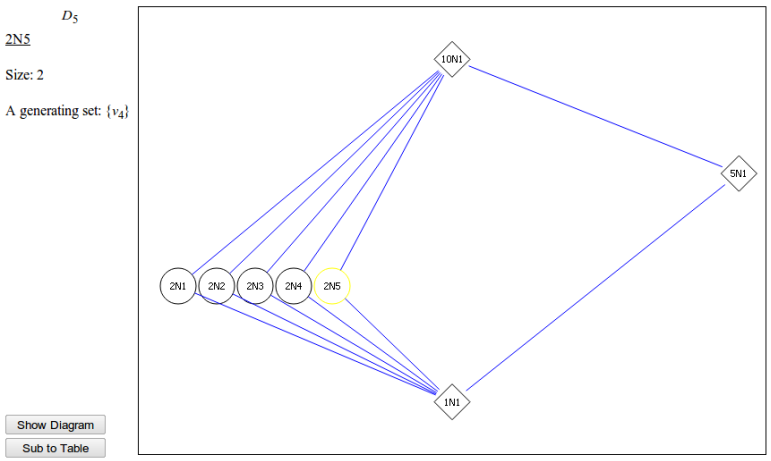


Figure 3: Subgroup diagram for D_5.

2 Recognizing groups

The Group Calculator provides two views of a given group, its group table and its subgroup diagram. For small groups, students can learn to recognize a group from either of these views. If the order of a group is not composite, then it must be cyclic so there is only one group so there is nothing to do. For other groups of order less than 12, one can distinguish them fairly easily.

First note that one can easily count the elements of order 2 from a group table: count the number of times the identity appears on the main diagonal and subtract 1 (for the identity itself). From a subgroup diagram one can just count the subgroups of order 2. For groups of order less then 12, this combined with the order of the group is enough to distinguish all but two cases.

The first case is the groups of order 8: both $\mathbb{Z}_8$ and the quaternion group, Q_8, have a unique element of order 2. These are easily distinguished in a subgroup diagram (Q_8 has 3 subgroups of order 4 but $\mathbb{Z}_8$, being cyclic has only 1). In a group table, one can observe that $\mathbb{Z}_8$ is abelian (the group table is symmetric along the main diagonal) whereas Q_8 is not.

The other case is the two groups of order 9: $\mathbb{Z}_9$ and $\mathbb{Z}_3 \times \mathbb{Z}_3$. These are easy to distinguish from a subgroup diagram by counting subgroups of order 3. With a group table, it is a little more difficult, but one can still count elements of order 3 (look for $a^2 = a^{-1}$ for $a \neq e$).

Why do this? On one hand, this kind of recognition may seem to be an auxiliary skill. However, the things being used to distinguish groups are structural properties of groups which we teach anyway. Learning to think in those terms reinforces the concepts and theorems in an abstract algebra course (e.g., that for a cyclic group of order n, there is a unique subgroup of order d for each d dividing n).

Since subgroups of subgroups are subgroups, one can look at the subgroup diagram of a small group and usually determine the isomorphism types of the subgroups. For example, the subgroup diagram shown in Figure 4 has three subgroups of order 8. By the method described above, we can determine that 8N1 $\cong D_4$, 8N2 $\cong Q_8$, and 8N3 $\cong \mathbb{Z}_8$. Interestingly, the three subgroups are pairwise non-isomorphic and include both non-abelian groups of order 8. One would not typically have such easy access to groups such as this and see its properties so clearly by other means. We will see applications of these skills in the sections below.

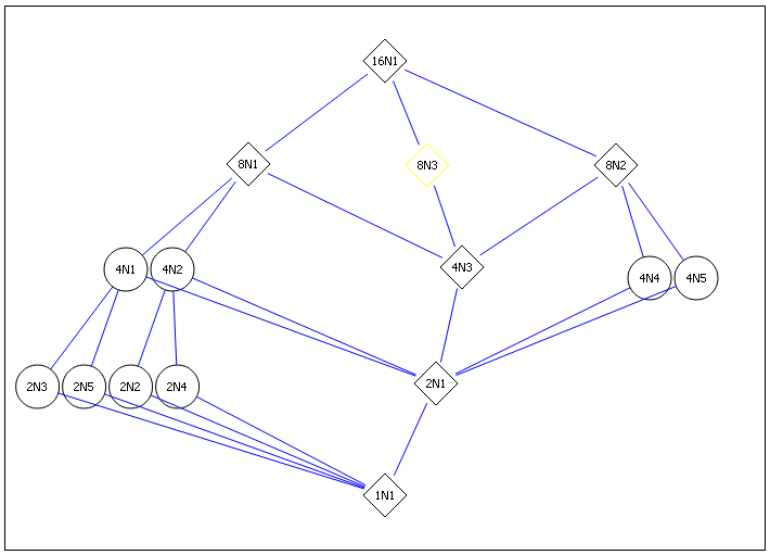


Figure 4: Subgroup diagram for $\mathbb{Z}_8 : \mathbb{Z}_2$.

3 Normal subgroups and quotient groups

One of the best known applications of group table is given a subgroup $H \leq G$, to organize the table by left cosets of the subgroup and to color the cosets as the Group Calculator does. Then one can ask if multiplication gives a binary operation on the set of left cosets, i.e., the set of colors. The issue is whether or not this is well-defined: if $aH = a'H$ and $bH = b'H$, does $(ab)H = (a'b')H$? Algebra courses typically prove at least the forward direction of the following theorem.

Theorem 1 *Let G be a group and H a subgroup of G. Then H is a normal subgroup of G if and only if*

$$(aH) \cdot (bH) = (ab)H$$

is a well-defined binary operation on the set of left cosets of H.

With the coloring of group elements by coset and grouping the cosets, it is easy to see at a glance if the selected subgroup is normal. In Figure 2, both subgroups are normal. As a result, the colors form nice k by k blocks throughout the table where k is the order of the subgroup. For example, in the right-hand table from Figure 2, one can see that red times blue is always fuchsia, regardless of which elements are selected.

On the other hand, in Figure 5, the group table is not comprised of 2×2 blocks of color. The multiplication of colors is not well-defined: red times blue is sometimes fuchsia and sometimes blue. So, the selected subgroup in that case is not normal.

In both cases, the user can use the Group Calculator to connect what they see as far as the coset multiplication being well-defined with the more standard criterion for normality, namely that the subgroup be closed under conjugation. The user can click on *Close under Conj.*; for the normal subgroup the number of selected elements will not change but for the non-normal subgroup additional elements will be selected.

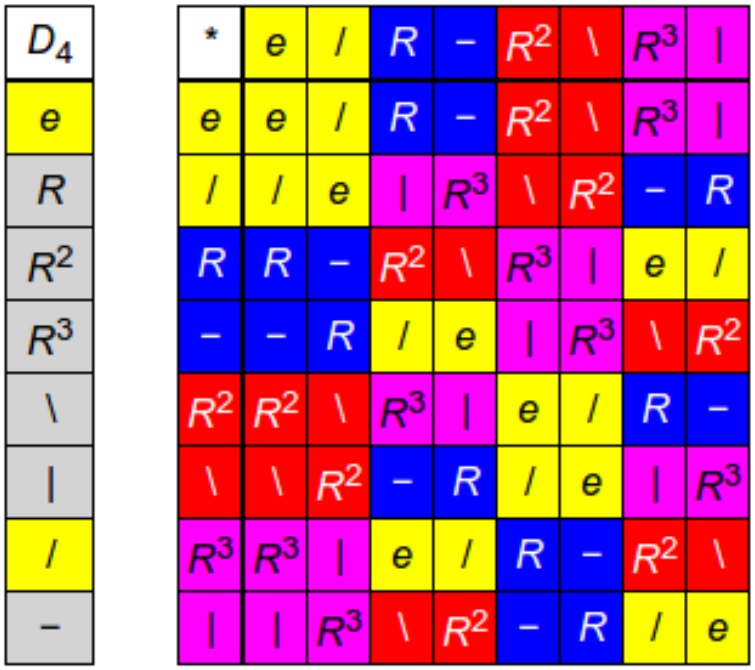


Figure 5: Dihedral group D_4 with a selected subgroup.

In the case of normal subgroups, one can see even more from the colored group table. If N is a normal subgroup of G, the binary operation on left cosets has the structure of a group, the quotient group G/N. Identifying cosets with colors, this is equivalent to thinking of the set of colors as forming a group. The group table for this set of colors is then visible in the colored group table. Referring again to Figure 2, the group table on the left has only two colors, and it is clear that the table of colors matches the group table for $\mathbb{Z}_2$ with $0 \leftrightarrow$ yellow and $1 \leftrightarrow$ blue. Similarly, the group table on the right has four colors, so it must be the table for either $\mathbb{Z}_4$ or V_4. For every color C, $C * C$ is yellow, the identity color. This matches the fact that in $V_4 = \{e, a, b, c\}$, $e = e^2 = a^2 = b^2 = c^2$. Moreover, V_4 has the property that the product of any two distinct non-identity elements is the third non-identity element. This is clearly visible in the group table: blue times red is fuchsia, blue times fuchsia is red, and red times fuchsia is blue.

Dealing with cosets as colors has an added advantage. Cosets are more complicated than we may want to admit. A coset is a single object, but inside it is a set of elements of a group. One often has to be able to shift between these two views when thinking about cosets and quotient groups. The use of colors in a group table facilitates this. Having a set of colors is not as much of a conceptual jump as a set of sets. On the other hand, when looking at a colored group table, all of the information is there. One is constantly reminded that cosets consist of sets of elements from the original group – the group elements are visible through the colors.

Thus far we have considered quotient groups in terms of group tables, but there is an important theorem which is reflected in the subgroup diagram, namely the lattice isomorphism theorem.

Theorem 2 (Lattice Isomorphism Theorem) *Let G be a group and N a normal subgroup of G. Then there is a bijection between the set of subgroups of G/N and the set of subgroups of G which contain N such that:*

- *normal subgroups correspond to normal subgroups*
- *the bijection preserves inclusions*
- *the bijection preserves intersections*
- *the bijection preserves joins.*[3]

Consider Figure 6. This is a group of order 16 with three normal subgroups of order 2 (recall, normal

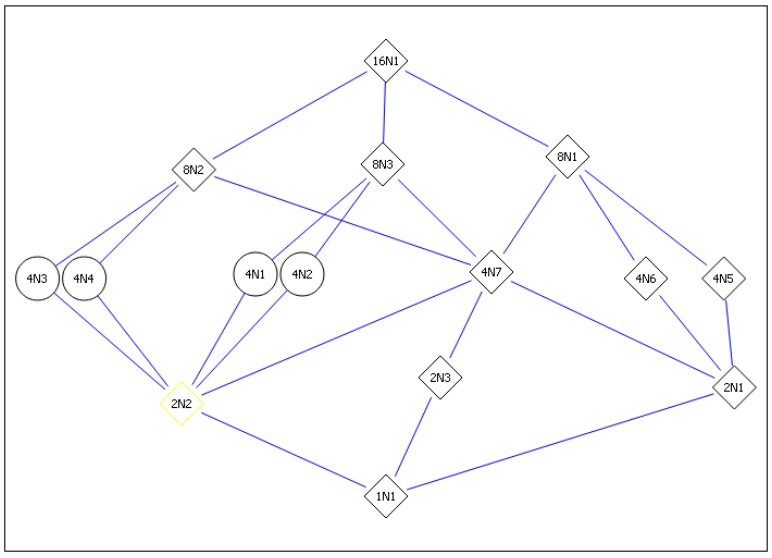


Figure 6: Subgroup diagram for $\mathbb{Z}_4 : \mathbb{Z}_4$.

subgroups are represented by diamonds). By the lattice isomorphism theorem, the subgroup diagram for $G/2N2$ is the diagram between $2N2$ and the whole group. The bijection preserves inclusions and normality, so it is effectively perfect. Since the subgroups $4N1$, $4N2$, $4N3$, and $4N4$ are not normal, $G/2N2$ is a group of order 8 with subgroups which are not normal. The only such group is D_4. Similarly, one can identify $G/2N3 \cong Q_8$ and $G/2N1 \cong \mathbb{Z}_4 \times \mathbb{Z}_2$. The three quotient groups are pairwise non-isomorphic.

In the same diagram, one might also consider the normal subgroup 4N7. The subgroup itself has three subgroups of order 2, so 4N7 $\cong V_4$. The quotient $G/4$N7 also has three subgroups of order 2 (represented by 8N1, 8N2, and 8N3). So, $G/4$N7 $\cong V_4$. Similarly, using skills for recognizing groups by their subgroup diagrams one can spot that 4N6 $\cong$ 4N7 $\cong \mathbb{Z}_4$ and $G/4$N6 $\cong \mathbb{Z}_4 \cong G/4$N7. This group has a very rich structure and illustrates what one can explore using technology with theorems from group theory.

[3]If H and K are subgroups of a group G, their join is the smallest subgroup of G containing both H and K.

4 Conjugation

The simplest way to look at conjugation with the Group Calculator is to select a group and an element of that group, and then click on *Close Under Conj.*; the conjugacy class of the element will be highlighted.

One can explore sizes of conjugacy classes further. First, we give some notation and the relevant theorem. Let G be a group and $g \in G$. The centralizer of $g \in G$ is $C_G(g) = \{x \in G \mid xg = gx\}$ and the conjugacy class of g is $Conj_G(g) = \{xgx^{-1} \mid x \in G\}$. These are related by

$$|Conj_G(g)| = [G : C_G(g)]. \tag{1}$$

We have described above how one can readily compute $Conj_G(g)$ with the group calculator. One can compute the centralizer from the group table by simply highlighting the element of interest and clicking on *Centralizer*.

For small groups, one can often determine $C_G(g)$ from the subgroup diagram. First note that any power of g commutes with g, so the cyclic subgroup $\langle g \rangle \subseteq C_G(g)$. Second, $C_G(g) = G$ if and only if g is in the center of G.

So, consider Figure 3, which gives the subgroup diagram for D_5. The subgroup 2N1 has order 2, so it is generated by an element of order 2 which we will call g. One can reason that g is not in the center of D_5.[4] So, by the considerations above, we have $C_G(g) = 2\text{N}1$. Then equation 1 tells us that the size of the conjugacy class of g is $[G : 2\text{N}1] = |G|/|2\text{N}1| = 10/2 = 5$. This can be confirmed from the group table by computing the conjugacy class directly. It is also consistent with the fact that 5 subgroups of order 2 are all conjugate since the 5 elements conjugate to g must all have order 2, so they generate subgroups of order 2 conjugate to $\langle g \rangle$.

5 Recognizing decompositions

There are two standard theorems for recognizing groups as products; the one for direct products is fairly standard for a beginning abstract algebra course while the one for semidirect products is standard for courses which cover that construction. We state versions of both here for reference.

Theorem 3 *Let G be a finite group, and H and K subgroups of G such that*

1. *$H \trianglelefteq G$ and $K \leq G$*
2. *$H \cap K = \{e\}$*
3. *$|H| \cdot |K| = |G|$*

Then $G \cong H \rtimes K$. If we also have $K \trianglelefteq G$, then $G \cong H \times K$.

[4] If g was in the center, it would commute with elements from the subgroup of order 5. That subgroup has prime order, so it is cyclic, hence abelian. The whole group is generated by the subgroup of order 5 and g, so if g was central, the group would be abelian.

All of the conditions are easy to verify by looking at a subgroup diagram in the Group Calculator. It allows the user to see the orders of subgroups, whether or not they are normal, and their intersection. Moreover, if the student has learned to recognize a small group by its order and subgroup diagram, then they can also see the isomorphism types of the candidate subgroups H and K.

For example, consider the subgroup diagram in Figure 4, a group of order 16. To see if it is a direct product, we would want to find either normal subgroups of orders 8 and 2 which intersect trivially, but there are none (the three subgroups of order 8 all contain the normal subgroup of order 2). Next we check to see if there are two normal subgroups of order 4 which intersect trivially, but there is only one normal subgroup of order 4. So, this group is not a direct product of proper subgroups.

If we check to see if it is a semidirect product of two subgroups of order 4, again no combinations work (all subgroups of order 4 contain a common subgroup of order 2). However, this group is a semidirect product of a subgroup of order 8 and a subgroup of order 2 in essentially 2 ways. For the subgroup of order 2 one can take 2N3, and for the subgroup of order 8 either 8N3 or 8N2. Recall $8N3 \cong \mathbb{Z}_8$ and $8N2 \cong Q_8$. So, this group is isomorphic to a group $\mathbb{Z}_8 \rtimes \mathbb{Z}_2$ and to a group $Q_8 \rtimes \mathbb{Z}_2$.[5]

References

[1] D. Kahneman, *Thinking, fast and slow*, Farrar, Straus and Giroux, 2011.

[2] Richard E Nisbett and Eugene Borgida, Journal of Personality and Social Psychology **32** (1975), no. 5, 932–943.

[5] We say *a* group because the two factors H and K in a semidirect product usually do not determine the isomorphism type of $H \rtimes K$.