Scientific
Research
Publishing

Classifying Groups of Small Order

Gerard Thompson

Department of Mathematics and Statistics, The University of Toledo, Toledo, OH, USA
Email: gerard.thompson@utoledo.edu

Abstract

The classification of groups of order less than 16 is reconsidered. The goal of the paper is partly historical and partly pedagogical and aims to achieve the classification as simply as possible in a way which can be easily incorporated into a first course in abstract algebra and without appealing to the Sylow Theorems. The paper concludes with some exercises for students.

Keywords

Finite Group, Dihedral Group, Historical, Pedagogical

1. Introduction

This past semester I have been teaching an introductory course on abstract algebra. The question arises of how to reach an audience of a mixed background, for example, graduate and undergraduate students. My solution was to present the material in a very computational way rather than going the usual route of lots of Theorems and Propositions. More specifically, why not orient the course towards the problem of classifying groups of small order? In the present article I shall present a classification of groups of order less than 16. The ground rules are that we shall assume that students have covered the first four weeks of group theory. In Section 3 we present six "Elementary Facts" which students can treat as homework exercises. We shall also assume that we have known the classification of finite *abelian* groups. Maybe that is a lot to ask, however, it is easy to *understand* the structure of finite *abelian* groups: just keep in mind the groups $\mathbb{Z}_2 \times \mathbb{Z}_3$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$, the former is cyclic whereas the latter is not. Here $\mathbb{Z}_p$ denotes the set of integers $0, 1, 2, \cdots, p-1$ that are *added* modulo *p* so that it is perhaps better to write $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ rather than $\mathbb{Z}_2 \times \mathbb{Z}_3$. Many authors use the notation C_p to connote a cyclic group of order *p* to which of course $\mathbb{Z}_p$ is isomorphic. In particular in the sequel it is sometimes preferable to think of $\mathbb{Z}_2$ as being isomorphic to the group consisting of the integers $\{\pm 1\}$ under *multiplication*.

Probably the nicest way to obtain the structure for finite abelian groups is as Corollary to the structure Theorem for a finitely generated module over a principal ideal domain, which can be covered nicely in the second semester of the abstract algebra class: see for example [1]. Another pillar in the classification of finite

abelian groups is Sylow's Theorem or Theorems depending on how they are presented [2]. Important as these Theorems are, the proofs probably go over the heads of first semester abstract algebra students even though the statements of the theorems are not difficult and numerical examples come readily to hand. In Gallian's book [3] Sylow's Theorems are relegated to a section titled "Special Topics" and appear on page 399. We recommend [3] for all details not covered adequately in this short article. The author still enjoys the book by Herstein [4] from which he originally learned the subject. Another very nice book, among many others, is written by Rotman [5]. So that is the program: *classify groups of order less than* 16 *knowing the structure of finite abelian groups without using Sylow theory.*

In Section 3 we review some historical details about the emergence of the concept of an abstract group and some of the early results on the classification of groups of small order. In Section 4 we consider the action of conjugation of a group on itself and the class equation. In Section 5 we study properties of the dihedral group D_n of order *n*. In Section 6 we prove the main Theorem that identifies D_n in various cases. In Section 7 we take stock and see which values of $|G|$ have already been accounted for and then settle the remaining 4 cases. In Section 8 we draw a few conclusions and finally in Section 9 we present a few exercises for students.

We shall say a few words about notation: $H < G$ means that H is a subgroup of G and $H \triangleleft G$ means that H is a normal subgroup of G. The identity element in G will be denoted by e. We shall denote the center of the group $G = \{z \in G \mid xz = zx, \text{for all } x \in G\}$ by $Z(G)$ and the centralizer of an element $g \in G$, by $C_G(g)$, that is, $C_G(g) = \{x \in G \mid gx = xg\}$. We shall use the word *order* frequently with different meanings. Thus $|G|$ denotes the *order* of *G*, that is, the number of elements in *G*. We shall also use the same notation if merely $Y \subset G$. On the other hand, $o(g)$ is the *order* of an *element* $g \in G$, that is to say, the smallest positive power is *r* such that $g^r = e$. The reason for using the same word is that $o(g)$ is also the order of the cyclic subgroup generated by *g* and that cyclic subgroup will be denoted by $\langle g \rangle$. Another not very serious remark: I have consistently used numbers rather than writing numbers in words because there are a lot of them and I considered that to do so had a much of a more visual impact.

2. Some History

The development of group theory is a complicated historical and epistomological question that we cannot possibly do justice here. We shall not supply many of the historical references as they can be found in the excellent book by Rose [6] which can serve effectively as a text for a more advanced course on group theory. The theory was a gradual coalescence of ideas distilled from the areas of polynomial equations, number theory and geometry. Indeed the very concept of "geometry" itself was being expanded by Gauss, Riemann, Lobachevsky and Bolyai in the first part of the nineteenth century. Klein's Erlangen Program, which associates a group of symmetries to a particular flavor of geometry, dates from 1872. There had been numerous contributions to the theory of groups made by the likes of Lagrange and Cauchy (whose theorems in finite group theory we still celebrate today), Euler and Gauss himself, particularly in what we refer to nowadays as *abelian* groups and their relationship to modular arithmetic. Apparently Galois in 1831 had begun to grasp the notion of an abstract group, as opposed to a group of permutations, as too did Cayley in the 1850's although both men's work was years ahead of its time.

Eventually the abstract idea of a "group" emerged. A two volume book on algebra by Heinrich Weber "Lehrbuch der Algebra" appeared in 1895 and 1896 and the first edition of William Burnside's book [7] was published as long ago as 1897. These books were enormously influential. Meanwhile the Norwegian Ludwig Sylow's fundamental set of Theorems had appeared as early as 1872 [2]; it is interesting that his paper was written in French whereas Sophus Lie, Sylow's equally famous compatriot, wrote in German. Notice that Sylow refers again to "les groupes de substitutions", or *permutation group* in more modern language. Burnside [7] credits Sylow with laying the first real theoretical foundations of group theory. By 1870 Jordan had proved the Jordan-Hölder theorem for permutation groups and Hölder proved it for abstract groups in general in 1889. Furthermore, Hölder in 1893 was studying groups of order p^3, pq^2, pqr and p^4. In America in 1900 G. A. Miller and G. H. Ling [8] proved that there was no simple group of order between 1092 and 2001. In the negative direction, as late as 1908 Burnside was complaining to the London Mathematical Society about the lack of acceptance in Britain of group theory as a subject in its own right.

By 1930 Miller [9] was announcing the classification of all groups of order up 100. The most difficult case, as Miller's paper suggests, was $|G| = 64$. Apparently Miller's paper contained errors that were not corrected until

1964 by Marshall Hall and J K Senior [10]. From the 1960's onwards the quest for the classification of the finite *simple* groups was in full swing. Copious details may be found on the Wolfram website that do not need to be repeated here. We will be content simply to cite [11] [12] as more traditional references. Apparently the complete classification was not achieved in toto until 2004.

3. Elementary Facts

1) Groups of prime order are cyclic and unique up to isomorphism.
2) Conjugate elements have the same order.
3) If G is a group and $Z(G)$ is its center then the factor group $G/Z(G)$ cyclic implies that G is abelian.
4) If all elements of G except e are of order 2 then G is abelian.
5) If p is prime the number of elements of order p is a multiple of $p-1$.
6) If a group G is generated by two normal subgroups H and K (so that every $g \in G$ is of the form $h_1 k_1 h_2 k_2 \cdots h_p k_1 h_p$ for some finite p) and H and K are complementary in the sense that $H \cap K = \{e\}$, then $G \approx H \times K$, the direct product.

4. Conjugation and the Class Equation

4.1. Group Actions

Let G be a group and X a set. Then we say G *acts on X* if there is a group homomorphism ϕ from G to S_X, the latter set denoting the group of permutations of *X*. Here are three examples of group actions where the group acts on itself, that is, $X = G$.

- For $g \in X = G$ and $a \in G$ let $L_a(g) = ag$ (left translation)
- For $g \in X = G$ and $a \in G$ let $R_a(g) = ga^{-1}$ (right translation)
- For $g \in X = G$ and $a \in G$ let $\phi_a(g) = L_a \circ R_a(g) = aga^{-1}$ (conjugation): note $\phi_a(e) = e$ for $a \in G$.

Define $\{g(x) \mid g \in G\}$ to be the orbit $Orb(x)$ of x and define a relation on X according as elements belong to the same orbit. It is left as exercise to show that this relation is actually an equivalence relation. Define also $Stab(x)$ or G_x to be the stabilizer subgroup of x, that is, $G_x = \{g \in G \mid gx = x\}$. In the case of the first two actions defined above there is only one orbit for each $g \in G$, that is G itself; in that case we say that the action is *transitive*. Also, for each $g \in G$ we have $Stab(g) = \{e\}$. However, in the third example of the action of conjugation, the orbits are precisely the conjugacy classes of G and G_g is the *centralizer* $C_G(g)$ of g, that is, $C_G(g) = \{x \in G \mid gx = xg\}$. It is easy to show that $G_g < G$. Notice also that conjugation does nothing at all for abelian groups! In fact conjugation is a very special kind of action because G acts on itself not merely as a set but as a *group*; in other word the action maps not only to S_G but to $Aut(G)$, the group of automorphisms of G.

Theorem 1. *There is a one to one correspondence between elements of $Orb(x)$ and G/G_x, that is, the space of (left) cosets of G_x in G.*

Proof. Suppose that $y \in Orb(x)$; then there exists $g \in G$ such that $y = gx$. We obtain a map from $Orb(x)$ to G/G_x by mapping g to the left coset of gG_x in G. We leave the student to verify that this map is well-defined (the hardest part for students) and bijective. □

4.2. Example

The group D_6 or S_3 consists of the elements $\{e, x, x^2, y, xy, x^2 y\}$ subject to the relations $x^3 = y^2 = e, yx = x^2 y$. The last relation used repeatedly enables us to "twist" products of x and y to work all the x's to the front in a string of x's and y's and all the y's to the back. Then the other relations may be used to reduce any string to one of the 6 elements that constitute the group. The conjugacy classes of D_6 are $\{e\}, \{x, x^2\}, \{y, xy, x^2 y\}$ so that $Orb(x) = \{x, x^2\}$. Now $G_x = \{e, x, x^2\}$ and $yxy^{-1} = x^2$ so $G/G_x = \{e, x, x^2\} \cup y\{e, x, x^2\}$. Also

$Orb(y) = \{y, xy, x^2 y\}$ and $G_y = \{e, y\}$ and $x^{-1} yx = x^2 yx = x^2 x^2 y = xy$ and

$xyx^{-1} = xyx^2 = xx^2 yx = yx = x^2 y$ so $G/G_y = \{e, y\} \cup x\{e, y\} \cup x^2 \{e, y\}$.

4.3. Conjugation and Centralizers

The class equation expresses $|G|$ as a sum of the orders of the conjugacy classes. *Thus the order of a conjugacy class is the index of the centralizer of any element x in that conjugacy class*, that is, $\dfrac{|G|}{|C_G(x)|}$. In particular the order of a conjugacy class divides $|G|$. Notice that $z \in Z(G)$ if and only if $C_G(z) = G$ if and only if z comprises its own conjugacy class and that $|C_G(x)| \neq 1$ for $x \in G$ provided G is not the trivial group consisting of a single element. Hence on the right hand side of the class equation we will have as many 1's as appear in $Z(G)$ and sums of various proper divisors of $|G|$.

5. The Dihedral Group

The group D_{2n} of order $2n$ is generated by x and y subject to the relations $x^n = y^2 = e$ and $yx = x^{n-1}y$. We shall now determine the class equation for D_{2n}. Note that $yxy = x^{n-1}$ and $yx^2 y = x^{2(n-1)} = x^{n-2}$ and likewise $yx^3 y = x^{n-3}, \cdots, yx^{n-1}y = x$. If n is odd then $x \sim x^{n-1}, x^2 \sim x^{n-2}, \cdots, x^{\frac{n-1}{2}} \sim x^{\frac{n+1}{2}}$ whereas if n is even $x^{\frac{n}{2}}$ is a singleton and $\sim$ signifies "is conjugate to".

Now $x^{n-1}yx = x^{n-2}y$ and $x^{n-2}yx^2 = x^{-1}x^{n-2}yx = x^{n-3}x^{n-1}y = x^{n-4}y$. Continuing in this way we find that if n is odd $\{y, xy, \cdots, x^{(n-1)}y\}$ comprises a single conjugacy class, whereas if n is even $\{y, x^2 y, \cdots, x^{(n-4)}y, x^{(n-2)}y\}$ and $\{xy, x^3 y, \cdots, x^{(n-3)}y, x^{(n-1)}y\}$ constitute distinct conjugacy classes.

Assuming $n > 2$ so that D_{2n} is not abelian, as a result of the preceding calculations we see that, apart from $\{e\}$, the only other singleton conjugacy class is $\left\{x^{\frac{n}{2}}\right\}$ in the case where n is even. Thus if n is odd $Z(D_{2n}) = \{e\}$ whereas if n is even $Z(D_{2n}) = \left\{e, x^{\frac{n}{2}}\right\}$.

A few more elementary calculations convince one that if n is odd, the class equation for D_{2n} is

$$2n = 1 + 2 + 2 + \cdots + 2 + n$$

the number of 2's being $\dfrac{n-1}{2}$, whereas if n is even, the class equation for D_{2n} is

$$2n = 1 + 1 + 2 + 2 + \cdots + 2 + \frac{n}{2} + \frac{n}{2}$$

the number of 2's being $\dfrac{n-2}{2}$ this time.

Notice finally that if $n = 2r$ where r is odd then in fact $D_{2n} \approx Z_2 \times D_n$: indeed $Z(D_{2n}) = \{e, x^n\} \triangleleft D_{2n}$ and also $\{e, x^2, x^4, \cdots, x^{2n-2}, y, x^2 y, x^4 y, \cdots, x^{2n-2}y\} \triangleleft D_{2n}$ being a subgroup of index 2 that is isomorphic to D_n. Since the normal subgroups are complementary by Fact 6, it follows that $D_{2n} \approx Z_2 \times D_n$.

6. Theorem

Lemma 1. *If G is a non-abelian group of order pq where p and q are distinct primes then* $Z(G) = \{e\}$.

Proof. Since $Z(G) < G$ we must have that $|Z(G)|$ divides $|G|$ by Lagrange's Theorem and hence $|Z(G)|$ can only be one of $1, p, q, pq$. Now $|Z(G)| = pq$ if and only if G is abelian. If $Z(G) \neq \{e\}$ then $|Z(G)| = p$ or $|Z(G)| = q$. Now $Z(G) \triangleleft G$ and in either case the group $G/Z(G)$ is cyclic hence by Fact 3 G must be abelian. $\square$

Lemma 2. *If G is a group of order* p^m *where p is prime then* $Z(G) \neq \{e\}$.

Proof. If $Z(G) = \{e\}$ the class equation gives $p^m = 1 + \cdots$. Each of the terms on the right hand side except the first must be divisors of p^m since they are indexes of centralizers and cannot be 1 otherwise $Z(G) \neq \{e\}$ - contradiction and hence $Z(G) = \{e\}$ is impossible. $\square$

Theorem 2. *Suppose that G is a non-abelian group of order* $2n$ *where n is either an odd prime or 4 or 6. Suppose further that there exist* $x, y \in G$ *such that* $x^n = y^2 = e$ *and that* $y \neq x^{\frac{n}{2}}$. *Then* $G \approx D_{2n}$.

Proof. Clearly $\{e, x, x^2, \cdots, x^{n-1}\}$ are distinct as too are $\{y, xy, x^2 y, \cdots, x^{n-1}\underline{\,}y\}$. The only possibility for collapsing among these $2n$ elements is if y is a power of x and necessarily $y = x^2$, which case we are excluding. Now $C_G(x) = \langle x \rangle$: it certainly contains $\langle x \rangle$ and if $C_G(x) = G$ then $yx = xy$ and G would be abelian. Hence x belongs to a conjugacy class of 2 elements. Furthermore $yx = x^m y$ for some $1 < m < n$. Thus

$$yxy = x^m \quad \text{and} \quad x = y^2 xy^2 = yx^m y = (yxy)^m = (x^m)^m = x^{m^2}. \quad \text{Thus} \quad m^2 \equiv 1 \bmod m.$$

Suppose now that n is an odd prime. Then $m^2 \equiv 1 \bmod n$ has only the solution $m = n - 1$.

Suppose that $n = 4$. Then the only solution of $m^2 \equiv 1 \bmod n$ for $1 < m < 4$ is $m = 3$.

Suppose that $n = 6$. Then the only solution of $m^2 \equiv 1 \bmod n$ for $1 < m < 6$ is $m = 5$.

Hence $G \approx D_{2n}$ in all 3 cases covered by the Theorem. $\qquad\square$

Corollary 1. *Suppose that G is non-abelian and that* $|G| = 2p$ *where p is an odd prime. Then* $G \approx D_{2p}$.

Proof. By 1 $Z(G) = \{e\}$ and the only possibility for the class equation is $2p = 1 + 2 + 2 + \cdots + 2 + p$. Consider an element y in the conjugacy class of order p. Now $|C_G(y)| = 2$ and so $o(y) = 2$ since $y \neq e$. Turning to an element x in a conjugacy class of order 2 then $|C_G(x)| = p$. Since p is prime it follows that

$C_G(x) = \langle x \rangle$ is cyclic of order p. We cannot have $y = x^{\frac{p}{2}}$ for then $C_G(y) = G$ and $y \in Z(G)$ whereas $Z(G) = \{e\}$. Hence $G \approx D_{2p}$. $\qquad\square$

7. Case by Case Study

For each order bigger than 5 we are looking for a *non-abelian* group G. Since G is not abelian we have that $|Z(G)| \neq G$. Since groups of prime order are cyclic we do not need to consider the cases $|G| = 2, 3, 5, 7, 11, 13$. Furthermore Theorem 1 disposes of the cases $n = 6, 10, 14$ so it remains to study the cases 8, 9, 12, 15.

7.1. $|G| = 9$

It follows from Lemma 2 that $|Z(G)| \neq \{e\}$. Hence we can only have that $|Z(G)| = 3$. Now $|G/Z(G)| = 3$ and so $G/Z(G)$ is cyclic and hence G is abelian by Fact 3.

7.2. $|G| = 15$

By Lemma 1 $Z(G) = \{e\}$ and the class equation gives $15 = 1 + 3 + 3 + 3 + 5$. The elements of the conjugacy class of order 5 are themselves of order 3: they cannot be of order 5 because their centralizers are of order 3 whereas an element of order 5 has a centralizer of order at least 5. On the other hand each of the elements in the 3 conjugacy classes of order 3 must have order 5: indeed, if x is such an element then $|C_G(x)| = 5$ and x must generate $C_G(x)$. Now the total number of elements of order 5 must be 9, which contradicts Fact 5, since it would have to be multiple of 4. Hence there cannot exist G for which $|G| = 15$ and G is non-abelian.

7.3. $|G| = 8$

We know of course that D_8 is a non-abelian group of order 8. We investigate whether there are any others. According to Fact 4, G must have an element x of order 4. Suppose that $y \in G$ but that $y \notin \langle x \rangle$. Then according to Theorem 2, if G is not isomorphic to D_8 we may assume both that $y^4 = e$ and $x^2 = y^2$. It is then easy to see by cancelation that the elements of G must be $\{e, x, x^2, x^3, y, y^3, xy, yx\}$. Now $yx \neq xy$ or else G will be abelian. The only possibilities for $o(xy)$ are 2 or 4; however, if $(xy)^2 = e$ then $yx = x^3 y^3 = xy^5 = xy$ and again G would be abelian and so $o(xy) = 4$. Again by cancelation and elimination of all other possibilities we see that $yx = (xy)^{-1}$; furthermore $(xy)^2 = x^2 = y^2$ since xy has order 2. We will now rewrite the elements of G as $\{e, x^2, x, x^3, y, y^3, xy, (xy)^3\}$. Note that $yx = (xy)^3 = y^2 xy$ and hence $x = yxy$. Similarly $xyx = y$.

Finally we can replace e by 1, x^2 by -1 and x, y, xy by i, j, k, respectively, so as to obtain the quaternion group Q usually written as $\{\pm 1, \pm i, \pm j, \pm k\}$.

7.4. $|G| = 12$

We have since $Z(G) < G$ that $|Z(G)|$ could be 1, 2, 3, 4 or 6. We may reject the cases $|Z(G)| = 4$ or $|Z(G)| = 6$ because of Fact 4. Suppose next that $|Z(G)| = 3$. Then in the class equation we must have another

odd number, which can only be 3. Thus $12 = 1+1+1+3+\cdots$. Consider an element x in the conjugacy classes of order 3. Its centralizer is of order 4 and contains $Z(G)$ as a subgroup which is impossible since 3 does not divide 4. Thus $|Z(G)| = 1$ or 2.

Suppose then that $Z(G) = \{e, z\}$ where $z^2 = e$. Then again by Fact 4 we can only have that $G/Z(G) \approx D_6$. Now we know that D_6 contains a cyclic normal subgroup $\bar{N}$ of order 3. According to the correspondence theorem [4], which is really the deluxe version of the first isomorphism theorem, $\bar{N}$ engenders a normal subgroup N of order 6 in G that contains $Z(G)$. Since N itself has a non-trivial center it too must be cyclic. Suppose that $N = \langle x \rangle$. Since $N \triangleleft G$ there exists $y \in G$ such that $G = \langle x \rangle \cup y \langle x \rangle$ and furthermore $y^2 \in \langle x \rangle$.

Notice that $Z(G) = \{e, x^3\}$ since $Z(G) \subset N$ and if any other positive power of x were in $Z(G)$ then $|Z(G)| > 2$. Furthermore, $y^2 \in Z(G)$ since y^2 commutes with x and y so $y^2 = x^3$ or else $y^2 = e$ in which case $G \approx D_{12}$ by Theorem 2.

So in order to avoid having $G \approx D_{12}$ we must have $y^2 = x^3$. Evidently the group G can be written as $\{e, x, x^2, x^3, x^4, x^5, y, xy, x^2y, x^3y, x^4y, x^5y\}$. So which element is yx? Clearly, since $y \notin \langle x \rangle$, we have $yx \notin \langle x \rangle$ and $yx \neq y$. Moreover $yx \neq xy$ or else G would be abelian. If $yx = x^3y$ then $yx = yx^3$ since $x^3 \in Z(G)$ which would give $x^2 = e$ and so $yx \neq x^3y$. If $yx = x^2y$ then $(yx)^2 = yxyx = x^2y^2x = x^6 = e$. So $(yx)^2 = e$ and $yx \neq x^3$ so $G \approx D_{12}$ by Theorem 2. If $yx = x^4y$ then $(yx)^2 = x^4y^2x = x^8 = x^2$ so that $o((yx)^3) = 2$ and $(yx)^3 = yxx^2 = x^3y$. According to Theorem 2 we must have $G \approx D_{12}$ unless $x^3y = x^3$, which is of course impossible.

Thus the only way to avoid having $G \approx D_{12}$ is to have $y^2 = x^3$ and $yx = x^5y$ and of course $x^6 = y^4 = e$ and all the conditions for the existence of a group are now met. To recognize this group, introduce a new generator $w = x^2$ so that $w^3 = e$. The elements of G can be written as $\{e, y, y^2, y^3, w, wy, wy^2, wy^3, w^2, w^2y, w^2y^2, w^2y^3\}$. Now $w^2 = x^4 = yxy^2xy = y^3x^2y = y^3wy$ where we have used the fact that $y^2 \in Z(G)$. Hence $y^{-1}wy = w^2$. Thus the group Z_4 generated by y, acts on Z_3 generated by w via conjugation and engenders a group denoted by T that is a semi-direct product of Z_4 and Z_3. Although $G/Z(G) \approx D_6$ and in fact $G/Z_6 \approx Z_2$ neither of these extensions split: here $Z_6 \approx \langle x \rangle$.

In fact the group T belongs to a familiar class of finite groups of order $4n$ called the *dicyclic* groups and also known as the *binary dihedral* groups. Depending how one counts, the first such group is Z_4 and the second the group Q studied in subsection 6.3. For further details see [13] which is another nice reference for more advanced material.

Now suppose that $|Z(G)| = 1$. The class equation must contain another odd number which can only be 3. Hence we have the following cases:

- $12 = 1 + 3 + 2 + 2 + 2 + 2$
- $12 = 1 + 3 + 2 + 2 + 4$
- $12 = 1 + 2 + 3 + 3 + 3$
- $12 = 1 + 3 + 4 + 4$.

We consider the first three cases for which 2 appears in the class equation. We take x in one of the conjugacy classes of order 2. Then $|C_G(x)| = 6$. Since $C_G(x)$ has index 2 it is normal in G. Hence we may write $G = \langle x \rangle \cup \langle x \rangle y$ where $y^2 \in \langle x \rangle$. If y^2 is a positive power of x, it will be a central element. However, we are considering now only cases where $|Z(G)| = 1$ so the only possibility is $y^2 = e$. Now we can invoke Corollary 1 and conclude that $G \approx D_{12}$. Since for $G = D_{12}$ we have that $|Z(G)| = 2$ we conclude that none of the three cases for which 2 appears in the class equation actually do occur.

Now consider the last case of the class equation $12 = 1 + 3 + 4 + 4$. Each of the elements in the conjugacy classes of order 4 must have order 3 because their centralizers are of order 3. Elements in the conjugacy class of order 3 could have order 2 or 4 because each of their centralizers are of order 4; however, if the elements have order four their squares would have order 2 and there are no conjugacy classes left to accommodate them. Hence the elements in the conjugacy class of order 3 have order 2.

Let x and y be elements of order 2 and 3, respectively. Then yxy^2 and y^2xy are of order 2 since they are conjugate to x; if any two of x, yxy^2, y^2xy are equal we would have that $xy = yx$. In that case we have a cyclic subgroup of order 6 generated by xy and whose only element of order 2 is x. Now pick a second element of order 2 and appeal to Corollary 1 to conclude again that $G \approx D_{12}$ and again contradicting $|Z(G)| = 1$. Thus we may assume that x, yxy^2, y^2xy are distinct. Now xy and yx must be of order 3. It follows that $xyxy = y^2x$

and $yxyx = xy^2$. Besides e, x, yxy^2, y^2xy the remaining elements of G are $y, y^2, xy, yx, xyx, xy^2, yxy, y^2x$. Now obviously y and xyx and xy and yx, respectively, are conjugate. Furthermore, xy^2 and yxy and y^2x are conjugate. Now $xyxy = y^2x$ implies that $xy^2x = yxy$ and $yxyx = xy^2$ that $yxy = xy^2x$ so $y^2xyxy = y^2xxy^2x = yx$ and so xyx is conjugate to yx. Hence the conjugacy classes have to be $\{e\}$, $\{x, yxy^2, y^2xy\}, \{y, xy, yx, xyx\}, \{y^2, xy^2, y^2x, yxy\}$. It follows that $G \approx A_4$. We can obtain the usual presentation of A_4 by mapping x and y to the permutations (12) (34) and (123), respectively.

Finally, a more sophisticated approach is to note that the conjugacy class of order 3 together with e forms a normal subgroup $N \approx Z_2 \times Z_2$ of order 4: indeed the centralizer of an element x in the conjugacy class of order 3 is of order 4. Since elements in the two conjugacy class of order 4 are each of order 3, the only possibility is to obtain the normal subgroup N described above. It follows that $G/N \approx Z_3$. From there it is not difficult to argue that Z_3 acts on N as a semi-direct product and deduce that $G \approx A_4$. Of course N turns out to be the Sylow 2-subgroup.

8. Conclusions

We have classified all groups of order < 16 without using Sylow theory and assuming we have known the classification of finite abelian groups. It seems remarkable to the author that for $|G| < 16$ the classification of the non-abelian groups becomes almost routine and depends only on elementary facts: the case $|G| = 12$ is the only one that is at all challenging. So why stop at $|G| = 16$? In fact, it turns out that up to isomorphism there are 14 distinct such groups! As an exercise (see next Section) try to find 8 of them. In fact, the groups that are the hardest to classify are p-groups where the order of $|G| = p^m$ and p is prime and m is a positive integer. Sylow's powerful theorems tell us nothing for such groups. Furthermore, the smaller that p is, the harder are the groups to classify. Naively speaking, the smaller that p is the more combinatorial possibilities there are to satisfy the group axioms.

In [14] one can find descriptions of the non-abelian groups of order < 32 in terms of generators and relations. We should also mention the computer algebra system GAP that contains the "Small Groups Library". In that system groups of order up to 2000 are listed up to isomorphism with the exception of groups of order $1024 = 2^{10}$: apparently there are an 49,487,365,422 non-isomorphic 2-groups of order 1024. At the time of writing, according to Wolfram, all groups have been classified up to isomorphism up to order $2047 = 2^{11} - 1$. In addition to Wolfram the author has also gained a lot of information from Wikipaedia: search for "List of small groups". However, I am warned to add the usual disclaimers about referring to websites.

9. Exercises for the Student

- Supply proofs of the six Elementary Facts. As a hint for the sixth, note that it suffices to map generators to generators.
- Show that the orbits $Orb(x)$ defined in Section 4 according as elements belong to the same orbit actually is an equivalence relation.
- Show that for the stabilizer subgroup of $Stab(x)$ or G_x defined in Section 4, $G_x < G$.
- Finish the details of Theorem 4.1.
- Find 8 mutually non-isomorphic groups of order 16.
- Find generators and relations for the group A_4 starting from its definition as the subgroup of the symmetric group S_4 consisting of even permutations.
- Find an explicit isomorphism between D_{2n} and $Z_2 \times D_n$.

Acknowledgements

References

[1]   Hartley, B. and Hawkes, T. (1970) Rings, Modules and Linear Algebra. Chapman and Hall.

[2]   Sylow, L. (1872) Theoremes sur les groupes de substitutions. *Mathematische Annalen*, **5**, 584-594.
http://dx.doi.org/10.1007/BF01442913

[3]   Gallian, J.A. (2002) Contemporary Abstract Algebra. 5th Edition, Houghton-Mifflin, Boston.

[4]   Herstein, I.N. (1975) Topics in Algebra. 2nd Edition, Wiley, Hoboken.

[5]   Rotman, J.J. (1999) An Introduction to the Theory of Groups. Springer Graduate Text # 148.

[6]   Rose, J. (1978) A Course on Group Theory. Cambridge UP, Cambridge (Reprinted by Dover, New York, 1994).

[7]   Burnside, W. (1897) Theory of Finite Groups. Cambridge UP, Cambridge (Reprinted by Dover, New York, 1955).

[8]   Miller, G.A. and Ling, G.H. (1900) Proof that There Is No Simple Group whose Order Lies between 1092 and 2001. *American Journal of Mathematics*, **22**, 13-26. http://dx.doi.org/10.2307/2369764

[9]   Miller, G.A. (1930) Determination of All the Groups of Order 64. *American Journal of Mathematics*, **52**, 617-634.
http://dx.doi.org/10.2307/2370630

[10] Hall Jr., M. and Senior, J.K. (1964) The Groups of Order $2^n, (n \leq 6)$. Macmillan, New York.

[11] Gorenstein, D. (1985) The Enormous Theorem. *Scientific American*, **253**, 104-115.
http://dx.doi.org/10.1038/scientificamerican1285-104

[12] Solomon, R. (2001) A Brief History of the Classification of the Finite Simple Groups. *Bulletin of the American Mathematical Society New Series*, **38**, 315-352. http://dx.doi.org/10.1090/S0273-0979-01-00909-0

[13] Roman, S. (2011) Fundamentals of Group Theory: An Advanced Approach. Birkhaüser.

[14] Coxeter, H.S.M. and Moser, W.O.J. (1980) Generators and Relations for Discrete Groups. Springer, Berlin.
http://dx.doi.org/10.1007/978-3-662-21943-0