Math From Scratch Lesson 9: Cosets and Cardinality

W. Blaine Dowler

November 29, 2010

Contents

1 Multiples

To this point, we have seen several algebras constructed out of objects which look nothing at all like the numbers we learned about as children, and yet we use those familiar natural and whole numbers to describe aspects of these groups and algebras through terms like cardinality and order. We will now define something which applies to those comfortable and familiar numbers, but not to reflections, rotations, or permutations.

Reflections, rotations and permutations all relate to each other through the operation of multiplication, as defined in each group through the symbol $\cdot$, or by simply writing the element adjacent to each other. However, as mentioned in lesson four, if the operation defining a group is commutative, then we call that group an *abelian group* and use the symbol $+$ to represent its operation. Let us explore the meaning of $+$.

In our intuitive understanding of addition is that it is the process of combining two or more groups of objects we can count into a single group. Formally,

addition is an operation which is commutative ($a + b = b + a$), associative ($(a + b) + c = a + (b + c)$), and has identity 0.

Definition Let $(G, +)$ be an abelian group. Let a and b be elements of G. If a has an inverse, then that inverse is written $-a$. We say that b is a *multiple* of a if, for some $n \in \mathbb{N}$ it is true that either

$$b = \underbrace{a + a + a + \ldots + a}_{n \text{ times}}$$

or

$$b = \underbrace{(-a) + (-a) + (-a) + \ldots + (-a)}_{n \text{ times}}$$

Notice in this definition that n must be a natural number: 0 is deliberately excluded. Notice also that the only multiple of 0 is 0, as 0+0+0+0+0+...+0 = 0 regardless of the number of instances of 0 appear on the left.

1.1 Factors

At this point, one may define a factor as well, as follows:

Definition If b is a multiple of a, corresponding to n repeated additions of a or $-a$, then we can say that a and n are *factors* of b. If $-a$ and $-n$ are defined in abelian group $(G, +)$, then they are also factors of b.

This definition will be the one we use for a while. However, we will eventually replace this definition with one that allows use to define factors when neither element a nor n is a natural number. In that situation, we will have factors without multiples, indicating the need to define one without referring to the definition of the other.

2 Exploring S_4

As you may recall from lesson six, S_4 is the group describing all permutations on four symbols. These permutations are written in terms of the changes produced. For example, the permutation (14) is the permutation which causes symbols 1 and 4 to trade places. The permutation (123) is the permutation which replaces 1 by 2, replaces 2 by 3, and replaces 3 by 1 in a cyclic fashion. There are 24

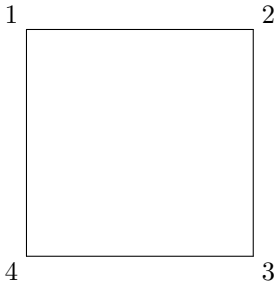

Figure 1: A square.

Permutation	**Corresponding transformation**
e	No transformation. (Identity)
(1234)	Rotation one quarter turn clockwise.
(13)(24)	Rotation by half a turn.
(1432)	Rotation three quarter turn clockwise.
(14)(23)	Reflection about horizontal axis of symmetry.
(12)(34)	Reflection about vertical axis of symmetry.
(13)	Reflection about diagonal joining points 2 and 4.
(24)	Reflection about diagonal joining points 1 and 3.

Table 1: Reflections and rotations of a square

possible such permutation, and eight of them correspond to the reflectional and rotational symmetries on a square. If our original shape looks like figure 1, then the eight permutations which leave the square as a square are those listed in table 1.

This subgroup of S_4 only contains eight elements out of 24 possible. We know that it is a subgroup; if we multiply elements of this subgroup by any other elements of this subgroup, we get elements within the subgroup. (For example, $(1234)(13) = (14)(23)$.) What happens if we multiply each element in this subgroup by an element of S_4 which is *not* in this subgroup?

Let us choose (14) as our random element of S_4 which is not in our existing subgroup. We multiply each of our elements by this element from the left, to obtain table 2.

This creates a new set of eight elements. There is no identity, so we see immediately that it cannot form a subgroup of its own. In fact, the only somewhat interesting observation at this point is that every element of this new set is distinct; no element appears on the list twice. Perhaps we can come up with a more interesting list by choosing another element. Let is choose, instead, element (23) and multiply by that from the left. We obtain table 3.

Original Element x	**Resulting element** $(14)x$
e	(14)
(1234)	(123)
(13)(24)	(1342)
(1432)	(243)
(14)(23)	(23)
(12)(34)	(1243)
(13)	(134)
(24)	(142)

Table 2: Symmetries of a square, multiplied by (14) from the left.

Original Element x	**Resulting element** $(23)x$
e	(23)
(1234)	(134)
(13)(24)	(1243)
(1432)	(142)
(14)(23)	(14)
(12)(34)	(1342)
(13)	(123)
(24)	(243)

Table 3: Symmetries of a square, multiplied by (23) from the left.

At first glance, this is no more interesting than the last set. In fact, it is *exactly* as interesting as the last set; they are completely identical! This is the interesting piece. In fact, this will be true no matter which of these eight elements we choose to start with, as seen in table 4.

It is important to keep in mind that all of these elements were produced by multiplication on the left by something in the righthand column of table 2. Had we chosen to multiply by any of the other eight elements in S_4, we would have ended up with a collection of those eight elements, as in table 5.

Similarly, had we multiplied by elements on the right instead of on the left, we would have had different cosets, as in table 6.

Although this set is different from that in table 2, it is identical to the table produced by multiplying on the right by any element in the righthand column of table 6, as the reader is encouraged to verify.[1]

Why is this? What do these sets mean? Why is this relevant at all? What

[1]Translation of common mathematical textbooks terms: "it is left as an exercise to the reader" means "this is a long, pedantic activity that's worth doing once to convince yourself it works, but doing it once is enough and the author had to do it as a student once already."

x	$(123)x$	$(1243)x$	$(134)x$	$(1342)x$	$(14)x$	$(142)x$	$(23)x$	$(243)x$
e	(123)	(1243)	(134)	(1342)	(14)	(142)	(23)	(243)
(1234)	(1342)	(142)	(1243)	(243)	(123)	(23)	(134)	(14)
(13)(24)	(243)	(23)	(142)	(14)	(1342)	(134)	(1243)	(123)
(1432)	(14)	(134)	(23)	(123)	(243)	(1243)	(142)	(1342)
(14)(23)	(142)	(1342)	(243)	(1243)	(23)	(123)	(14)	(134)
(12)(34)	(134)	(14)	(123)	(23)	(1243)	(243)	(1342)	(142)
(13)	(23)	(243)	(14)	(142)	(134)	(1342)	(123)	(1243)
(24)	(1243)	(123)	(1342)	(134)	(142)	(14)	(243)	(23)

Table 4: All combinations of multiplications.

x	$(34)x$
e	(34)
(1234)	(124)
(13)(24)	(1423)
(1432)	(132)
(14)(23)	(1324)
(12)(34)	(12)
(13)	(143)
(24)	(234)

Table 5: Symmetries of a square, multiplied by (34) from the left.

x	$x(14)$
e	(14)
(1234)	(234)
(13)(24)	(1243)
(1432)	(132)
(14)(23)	(23)
(12)(34)	(1342)
(13)	(143)
(24)	(124)

Table 6: Symmetries of a square, multiplied by (14) from the right.

does it have to do with multiples? The rest of this lesson answers those questions.

3 Cosets Defined

The sets created above are referred to as *cosets*. Formally defined:

Definition Let $(G, \cdot)$ define a group. Let $(A, \cdot)$ be a subgroup of $(G, \cdot)$. Let $x \in G$. We say B is a left coset of A if $B = xA$. In other words, each element of B is an element of A multiplied on the left by x. Similarly, C is a right coset of A if $C = Ax$. If $x \in A$, then clearly $xA = Ax = A$.

Okay, so we now have a definition. However, we still have no clear purpose. We'll get there; I promise. In our above example, we found that two different cosets were produced by taking sufficiently different elements. In other words, the cosets were either completely identical when produced by two different elements multiplied from the left (say, (23) and (14)) or completely unrelated ((14) and (34), for example). With technical terms, the cosets are *disjoint.* This was no accident.

Let $(G, \cdot)$ be a group, and $(A, \cdot)$ be a proper subgroup of $(G, \cdot)$. Choose $x, y \in G$ such that $x \in A$ and $y \in A$. Multiply x on the left by y, and label the product z such that $yx = z$. Now, either $z \in A$ or $z \notin A$. If $z \in A$, then by the fact that $(A, \cdot)$ is a group, meaning it is closed and contains inverses for all of its elements, then we also find that $zx^{-1} \in A$. However, by our definitions, $zx^{-1} = yxx^{-1} = y$. So, if $y \in A$, then $yx \in A \forall x \in A$, but if $y \notin A$ then $yx \notin A \forall x \in A$. In formal set notation, using the $\cap$ for intersections as defined in lesson two, we find that either $A \cap yA = A$ if $y \in A$ or $A \cap yA = \emptyset$ if $y \notin A$. Thus, the left cosets of a subgroup $(A, \cdot)$ of group $(G, \cdot)$ are a group of disjoint sets.

Furthermore, we can prove all left cosets have the same size, by noting that all possible products yx with fixed y have unique results within a group. Assume $yx = c$ and $yz = c$ are products within the group. Well, we can prove that $x = z$ in all cases, thereby proving that the products are unique for fixed y, as follows:

$$x = y^{-1}yx = y^{-1}c = y^{-1}yz = z$$

So, when building a left coset yA, we find that $o(A) = o(yA)$, as each product yx is unique for $x \in A$. We can repeat the last few paragraphs for right cosets instead of left cosets and obtain equivalent results. We are now equipped to discuss Lagrange's Theorem, which is the point of the entire lesson.

4 Lagrange's Theorem

Lagrange's Theorem relates the size (order, cardinality) of a subgroup to the size (order, cardinality) of its parent group. Let $(A, \cdot)$ be a subgroup of $(G, \cdot)$. We can find a collection of distinct cosets of A through appropriate choice of multiplicative elements x. Choose $x_1, x_2, \ldots x_n$ as necessary such that each x_i is distinct, and such that $x_i A \cap x_j A = \emptyset$ when $i \neq j$. Thus, using the union notation from before, we can find a set of x_n such that $G = x_1 A \cup x_2 A \cup \ldots \cup x_n A$. We know we can collect every element of G this way: choose x_1 at random and calculate $x_1 A$. If $A = G$, we are already done. If not, choose x_2 such that $x_2 \in G$ and $x_2 \notin x_1 A$. This produces a disjoint $x_2 A$. If there is an element $x_3 \in G$ such that $x_3 \notin x_1 A$ and $x_3 \notin x_2 A$, then calculate $x_3 A$. Continue the process; if any element of G has not been included in a coset $x_i A$ after each iteration, then calculate that one. In the case of infinite sets, the n subscript on the last x_n may not be finite, but the formalism still holds. Also, note that $o(x_1 A) = o(x_2 A) = \ldots = o(x_n A)$. With unique products yx for fixed x, and with distinct subgroups, all cosets must be of the same order as the original subgroup.

Definition Let $(A, \cdot)$ be a subgroup of $(G, \cdot)$ with cosets such that $G = x_1 A \cup x_2 A \cup \ldots \cup x_n A$ where $x_i \in G \forall i$. The *index* of A in G, denoted $[G : A]$, is equal to n.

This now gives us Lagrange's theorem: let $(A, \cdot)$ be a subgroup of $(G, \cdot)$. Then $o(G)$ is a multiple of $o(A)$. Given this much advance work, the proof is now trivial: $o(G) = [G : A]o(A)$ where $[G : A] \in \mathbb{N}$. In other words, if a group has order $o(G)$, then the order $o(A)$ of any possible subgroup A must be a factor of $o(G)$.

For finite sets, it is clear to see that the index defined through left cosets is the same as the index for the right coset: the cosets still have identical order, and the original group $(G, \cdot)$ has the same order, so the rest follows. To include infinite sets, one must formalize the proof. We have not yet formally studied the size of infinite groups. However, given the definition of bijective functions from lesson eight, it is not hard to see that, should a bijective function connect a left and right coset of A, then those two cosets must have the same size: every element in the left coset can be matched to an element in the right coset, and vice versa. This will be formally established when we deal with the sizes of infinite sets. In the meantime, should we need to apply Lagrange's Theorem, we will do so only with finite groups.

Lagrange's theorem also has implications for cyclic elements of $(G, \cdot)$. If $x \in G$ is a cyclic element of $(G, \cdot)$, then we know that $x^n = e$ for some $n \in \mathbb{N}$.

Thus, $o(x) = n$. Well, in that case, we can define a subgroup $(A, \cdot)$ of $(G, \cdot)$ as the group generated by x. In that case, $o(A) = o(x) = n$. As $o(A)$ must be a factor of $o(G)$, then $o(x)$ must *also* be a factor of $o(G)$. Therefore, the order of a cyclic element x within a group $(G, \cdot)$ is restricted to the factors of $o(G)$.

5 Upcoming Lessons

In our next lesson, we define the axioms of an algebraic ring. This will allow us to define the integers, which will lead to divisibility, factoring, and ultimately tell us exactly what kinds of restrictions Lagrange's Theorem produces in the formal sense, although most readers would have an intuitive grasp of that at this point. We will also use the definition of the integers to lead ourselves to the axiom of inequality, which brings us to an important piece of mathematical theory that the author has assumed for some of these examples: the unique representation of numbers to a given base.