Motivating Abstract
with Elementary Algebra

Timothy W. Jones

October 17, 2019

Abstract

There are natural lead ins to abstract algebra that occur in elementary algebra. We explore function composition and permutations as such lead ins to group theory and abstract algebra.

Introduction

You like math and are a math major. You've picked up a book on abstract algebra and are feeling a little bit queasy by what you see. Relax. This is a tutorial for you to make the transition from algebra 2, pre-calc, and the like to abstract less anxiety provoking. We'll motivate groups in particular.

Linear functions

Groups look at the properties that composition of functions have. You have noticed that functions can have inverses, for example, and that sometimes $f \circ g \neq g \circ f$. Consider linear functions, $y = f(x) = mx + b$ with $m \neq 0$. We will make this a set with $LF[x]$ and prove that $LF[x]$ is closed, meaning the composition of two elements is itself in the set.

Theorem 1. *$LF[x]$ is closed under function composition.*

Proof. Suppose $f_1(x) = m_1x + b_1$ and $f_2(x) = m_2x + b_2$ and m_1 and m_2 are not zero, i.e. $f_1, f_2 \in LF[x]$. Then

$$f_1(f_2(x)) = m_1(m_2x + b_2) + b_1 = m_1m_2x + m_1b_2 + b_1 \in LF[x]$$

□

Easy enough. We might mention that the slopes m are any non-zero reals. We could limit m to non-zero rationals or natural numbers and maintain this closure property. This is a common theme of abstract algebra. Change the coefficients involved and see what properties are maintained or lost. The next theorem gives a another property of $LF[x]$.

Theorem 2. *If $f(x) \in LF[x]$ then it has an inverse function and $f^{-1}(x) \in LF[x]$.*

Proof. We use the technique of interchanging x and y, solving for y, and substituting $f^{-1}(x)$ for the result. Suppose $f(x) = y = mx + b$, then switching

$$x = my + b$$

and solving for y gives

$$f^{-1}(x) = \frac{1}{m}x - \frac{b}{m}.$$

We confirm this result with

$$f(f^{-1}(x)) = m(\frac{1}{m}x - \frac{b}{m}) + b = x$$

and

$$f^{-1}(f(x)) = \frac{1}{m}(mx + b) - \frac{b}{m} = x.$$

□

This is more abstract than what you have encountered in previous algebra courses. Before you did have sets, like $\mathbb{N}$ and $\mathbb{Q}$, the natural and rational numbers and they did have such closure properties and, with the later, inverses. But now our set $LF[x]$ consists of functions, a more abstract idea than numbers. The unit or identity or one of the number sets now is x, the identity function, in $LF[x]$. The binary operations on sets of numbers, the arithmetic operations of addition, subtraction, multiplication, division is now reduced to just the operation of composition. Composition is associative, but it is not commutative, and distribution (using two operations) makes no sense with composition.

Applied

You may have done a section of your algebra two book involving variation problems. The set of functions $LF[x]$ has a subset that consists of direct variation functions, things of the form $y = kx$. This will be a subgroup of $LF[x]$, call it $DV[x]$, as in direct variation linear functions. It is commutative.

Knowing that inverses exists in $DV[x]$ one knows that the reverse problem of finding an x given a y value can be solved. Variation problems are big in physics. The function $F = ma$ says that acceleration varies directly with F. The universal law of gravitation is a variation problem, albeit involving joint and inverse variation; $e = mc^2$ is a variation problem with a square variation.

All of this points to real analysis. When can a set of functions cover or model a phenomenon. Fourier analysis uses a lot of trigonometric functions to expand what can be modeled. As it turns out polynomials, of which linear functions are an example, are potent, but limited. One needs infinite series, a thing studied first in calculus, to broaden the modeling range to include more complex phenomena of advanced physics.

Still with $LF[x]$ one gets the easiest means of contemplating in the abstract such questions.

Research

Look up what the evolution to the symbol $\mathscr{L}^2(\mu)$ in [**?**].

General polynomial functions

Note that quadratics, like $f(x) = ax^2 + bx + c$ will not be closed under composition and will not have inverses. $LF[x]$ is a group under composition because it has an identity, it is closed, it is associative, and its elements have inverses. Its a generalization of the integers under addition and the rationals under multiplication to more complex objects – from numbers to functions.

Solving polynomials

We can solve $x + 3 = 5$ in the integers and we can solve $3x - 5 = 7$ in the rational numbers. Which polynomials can we solve. We can solve the quadratics with integer coefficients with complex numbers. This is purport of the quadratic formula. Having contemplate the set $LF[x]$ how can we frame the general question of solving a polynomial. We need to specify the coefficients allowed, what set they are from, as well as where we will look for roots, where an x that solves $p(x) = 0$ is a root. In the case of the linear function $3x - 5 = 0$ the coefficients are from the integers and the roots are from the rationals. For the quadratic the coefficients can be from the integers, but the roots will be from the complex numbers. We have expand are coefficient set way up to get a quadratic's roots. What about the details of getting to a root for any polynomial? As we see with the linear and quadratic cases we insist that a finite number of steps involving algebraic manipulations are the means. Three sets: $polys$ through $means$ yields $roots$. The $means$ are a finite number of steps. How can we specify all the possible steps we allow? This is a major theme of abstract algebra.

The fast answer is to first note that a field has arithmetic operations we allow. Next a permutation of a finite set of these operations is the goal. Witness the algebraic steps necessary to solve $ax + b = 0$ and $ax^2 + bx + c = 0$ use field operations. The number of steps and the complexity of the operations goes up with the increasing degree, so we might expect that the problem gets harder and harder. Actually, there is a formula for the cubic, quartic, but the general quintic (degree 5) cases. One can get a real feel for how hard the problem gets by reverse engineering the situation from the solution back. Consider a factored polynomial and its relationship to its coefficients:

$$(x - r_1)(x - r_2)\ldots(x - r_n) =$$
$$x^n - \sum[1]x^{n-1} + \sum[2]x^{n-2} - \cdots \pm r_1 r_2 \cdots r_n,$$

where $[j]$ means products of roots taken j at a time. Try this with $n = 2$ and 3 to convince yourself of the general pattern. So to go from the coefficients back to the roots involves more and more work; the number of coefficients goes up and the number of sums and products goes up too. One might imagine that at some point it will be impossible to decode coefficients and get all the roots.

We've considered $LF[x]$ and its subgroup $DV[x]$. These are both infinite groups. Part of the puzzle of proving that $G5[x]$, greater than 5th degree polynomials with integer coefficients can't in general be solved requires learning about finite groups – permutations. You must likely studied permutations sometime in high school within a chapter on probability, so there is a natural door into making permutations functions. You'll see.

Permutations as functions

Are there finite groups which consist of functions? The functions would need to be one-to-one to insure that they have inverses. This is a limitation for real valued functions defined on $\mathbb{R}$. But remember those little diagrams giving examples of functions between two sets. These can be one-to-one and onto easily and we can compose with them. They will have inverses and as with all functions, with the right domains and ranges, are associative, there is hope.

Spelling corrections

Consider the misspelled version of ‘the’, say ’eht.’ The function $321(eht)$ corrects it: it moves the letter in the third position of its argument to the first, the letter in the second position stays in the second position, and the letter in the first position goes to the third position. Thus $321(eht) = the$. What’s the inverse of 321. Well what gives 123, the identity function. Well $321(321) = 123$. Permutations can be thought of as functions on strings of a given length; you rearrange or permute the letters making up the string; in the case of correcting a spelling typo to give the correct spelling. Table 1 gives the permutation of three objects – the objects t, h, and e. We generate all the typos for ‘the.’

123(the)	the
132(the)	teh
213(the)	hte
231(the)	hte
312(the)	eth
321(the)	eht

Table 1: The 3!=6 permutations of three objects considered as functions.

There seems little point in repeating the argument ‘123’. We can give a phrase that guides the function. This is done in Table 2. So when confronted with ‘teh’ we wish to flip the last two for ‘the’; ‘eth’ needs a conveyor belt 1 for ‘the‘. We could tell an editor for the last to transpose the first two letters and then transpose the resulting last two: ‘teh’ then ‘the.’ Are all permutations expressible as sequences of transposition? Yes. That’s in the group theory chapter of Herstein’s classic Topics in Algebra [2].

It is easy to see that a permutation of a permutation is a permutation. These functions are closed under composition. A flip of a flip is back to 123 and three rotations, 123 to 231 to 312 to 123, yields 123 as well. Each permutation function, henceforth just permutation, has an inverse. One can

123(123)	123	same
132(123)	132	flip last two f_1
213(123)	213	flip first two f_3
231(123)	231	conveyor belt 1 r_1
312(123)	312	conveyor belt 2 r_2
321(123)	321	flip outer f_2

Table 2: The flip function subscript gives which to hold constant. 'r' stands for rotate forward and wrap around to back.

see this group quickly by labeling a triangle's vertices with 1, 2, and 3 – label it from southwest going counter-clockwise. Flip vertex labels and rotate them and you get the three flips and rotations given in Table 2. Note the flips are their own inverses and form a subgroup of order 2. The rotations also this way, closed and with inverses, so that's another subgroup of order 3. The order of 3 subgroups is 2 and one is 3. Is it true that subgroups are divisors of the grand group? Yes. This is a named theorem in Herstein, Lagrange's theorem. Given a prime divides a group, is there necessarily a subgroup of that order? Yes. Subgroups of all possible divisor orders? No. Finite groups are as fascinating as prime numbers, maybe more so!

Permutation functions on a set of objects is a group: they are closed, have an identity, are associative (CIA) and also each has an inverse. We've seen three instances of groups: $LF[x]$, typo corrections, and call them rigid triangle transformations and these permutation groups. Cayley's theorem says that all finite groups are subgroups of permutation groups. You can see why; permutations give all possible functions, so naturally any set of functions that stays closed will have to be in these big sets of functions.

Abstract algebra

If you are about to take a course in abstract algebra you should take linear algebra first. The grand theme of abstract algebra is well anticipated by linear algebra. Linear algebra itself is well anticipated by solving linear equations taught in high school algebra. Blitzer has a chapter on matrices [1]. Linear algebra broadens the themes to consider the inverses of a matrix as well as how matrices give transformations. Transformations themselves allow for proving that two *spaces* are isomorphic. This theme of proving two spaces, think groups of one type and another, isomorphic is really about showing they are the same. So Cayley's theorem says all finite groups are isomorphic (the same) as a subgroup of some permutation group. Linear algebra is more concrete than group theory. Study it first.

Abstract algebra has as its grand goal proving that general fifth and greater degree polynomials over the rationals are not solvable by root taking. Root taking means all the arithmetic operations you are used to (add, subtract, multiple, and divide), plus powers and roots. There is no quadratic formula for polynomials over degree four. The proof of this requires groups, rings, fields, and vector spaces. It is a hard slog.

References

[1] R. Blitzer, *Algebra and Trigonometry*, 4th ed., Upper Saddle, NJ, 2010.

[2] I. N. Herstein, *Topics in Algebra*, 2nd ed., John Wiley, New York, 1975.

[3] W. Rudin, *Principles of Mathematical Analysis*, 3rd ed., McGraw-Hill, New York, 1976.