Group Theory Ideas With a TI-84 CE

Timothy W. Jones

August 19, 2025

Abstract

We give some central ideas of abstract algebra in a motivated manner starting with the construction of the integers with straight edge and compass, extrapolating axioms for these integers, finding a finite version of integers that obey these same axioms, and comparing this result with a permutation group via a Cayley table constructed using a TI84 program. Along the way we show how Lagrange, Euler, and Fermat theorems can be motivated and proven as natural results of the development. The need for and the essence of abstraction in mathematics we hope emerges.

$\mathbb{Z}$ and $3\mathbb{Z}$

Use a straight edge to draw a straight line, use a compass to define a unit length, label 0, and make tick marks of this length to the left and right of 0. You have constructed a set and using induction you can infer all integers can be constructed.

Note that elements from this set under addition are closed and associative. Further 0 acts as an identity and for every $x \in \mathbb{Z}$ there exists an inverse x^{-1} such that $x + x^{-1} = 0$: here $x^{-1} = -x$. These four axioms also work for $3\mathbb{Z}$, the set of all integers multiplied by 3. It is natural to say that this subset is a subgroup of the larger group of all integers.

These are both infinite groups. Are they really different? Notice that we can define a one-to-one and onto function that preserves addition. It is just

$$f(a) = 3a.$$

It is easy to immediately see that $f(a+b) = 3(a+b) = 3a+3b = f(a)+f(b)$. Such a function is called a one to one and onto homomorphism, in short an isomorphism. Even though the sets are not equal, in some aspects (the existence of this isomorphism) they seem the same. Pop quiz: what is the domain and range of this function?

There is one way in which $\mathbb{Z}$ and $3\mathbb{Z}$ are clearly different. We can't construct or find a length of 2 using compass tick marks of radius 3. This is the sense in which geometry is trumped by algebra: what could tax humanity's geometric ingenuity (squaring a circle) for a long time (millenia) can be reduced to an obvious element (π) is in or not in a set, as we see from this easy example. To quote Aristotle *algebra rocks, geometry sucks!*.

Easy Finite Cases

$\equiv_4, +$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Table 1: Classes modulo 4 Cayley Table.

We've made a couple of infinite groups. Can we come up with a finite group that obeys the four axioms: **c**losed, existence of **i**dentity, **a**ssociative, and existence of **i**nverses (CIA I for short).

Given any n we note that given any other m (both in $\mathbb{Z}^+$) we can do a division and get a remainder of $0, \ldots, n-1$. A clock shows this. Consider a four hour clock consisting of $0, 1, 2, 3$. Using modulo 4 classes (sets of numbers with the same remainders), make a table, using addition. Notice that the set $\{0, 2\}$ forms a subgroup. In general, divisors of the groups order can sometimes form such subgroups. Thus a 12 hour clock has subgroups consisting of $\{0, 2, 4, 6, 8, 10\}$, $\{0, 3, 6, 9\}$, $\{0, 4, 8\}$, and $\{0, 6\}$.

Pop quiz: Which class is 13 in, in this regular mod 12 case? That's right 1. In the mod 4 case? In the mod 5 case? Just do the divisions and get the remainders. Can your TI84 calculator do this for you?

Now back to it: Can we say that all groups are such that subgroups will exist with orders all divisors of the group order? Stay tuned.

What goes wrong with our axioms if we switch to multiplication using modulo 4 again? The answer is 0 doesn't have an inverse that gives 1 which must be the identity under multiplication. Let's just drop 0 and consider $\{1, 2, 3\}$ under multiplication modulo 4. What goes wrong here? It isn't closed: $2 \times 2 \equiv 0$, not in the set. What about just $\{1, 3\}$? That works: $3 \times 3 = 9 \equiv 1$ mod 4. Might it be that sets of numbers relatively prime to a given n make a group? Later.

We notice that n times any class from the group $(\equiv_n, +)$, the group of integers modulo n under addition, always gives the unit, 0. The equivalent of this under multiplication is exponents of the order of the group should deliver the unit for such groups, 1. We notice that for primes, all numbers less than the prime are relatively prime to it. Let's look at $(\equiv_p, *)$ when $p = 5$. That will have 4 elements, order 4: $1^4 \equiv 1$ mod 5, $2^4 = 16 \equiv 1$ mod 5, $3^4 = 81 \equiv 1$ mod 5 and $4^4 = 256 \equiv 1$ mod 5. Amazing. Why does this work? It must follow from the axioms of a group directly. We don't want to look at specific cases, but to get all the specific cases by doing proofs just using the axioms. So for example, can we say

$$a^{\phi(n)} \equiv 1 \text{ mod n},$$

where $\phi(n)$ is the number of numbers relatively prime to n, like our mod 4 and mod 5 cases.

For the record: we have hit on (suggested) three theorems might be true: LaGrange (the order of subgroups divides the order of the group); Fermat ($a^{p-1} \equiv$ a mod p); and Euler ($a^{\phi(n)} \equiv 1$ mod n) [2].

Groups of Order 6

We can make two groups with the same order: 6. Make a table for $(\equiv_6, +)$ and $(RP(\equiv_{18}), *)$, the group of numbers less than 18 and relatively prime to it using multiplication mod 18. There are 6 such numbers: $\{1, 5, 7, 11, 13, 17\}$. The first table, $(\equiv_6, +)$ is going to be easy: Table 2. Note that with the convention of always making the identity the first in the list of a group's elements in these tables, we can drop the far left column and top row. With a calculator this convention (drop 'em) makes the going a lot easier. Speaking of calculators, the code and print out for generating $(RP(\equiv_{18}), *)$ is given in Figure 1, left. You need to initialize the matrix $[B]$ with dimensions 6×6 for this code to work.

Here's where you can start to grasp the nature of the puzzles posed by group theory. If I quite arbitrarily label the elements of $(\equiv_6, +)$ with m_i and

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Table 2: Cayley Table for integers mod 6.

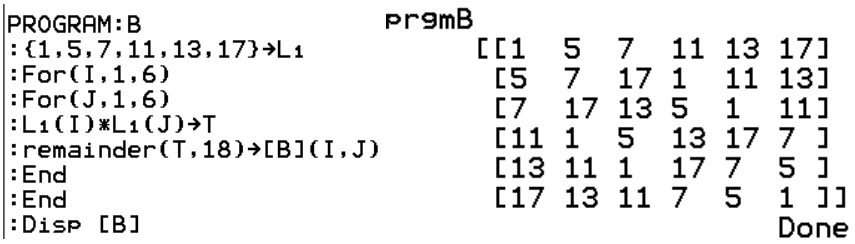

Figure 1: The TI84's remainder function and matrix capabilities do the trick fast.

those of $(RP(\equiv_{18}), *)$ with r_i with $1 \leq i \leq 6$ and define $f : (\equiv_6, +) \rightarrow (RP(\equiv_{18}), *)$ with $f(m_i) = r_i$ will I have an isomorphism? Hmm!? How about $f(m_6 + m_6) = f(m_5)$, aka $f(4)$; that should be $r_5 = 13$. It isn't. Notice the notation is $f(m_i + m_j) = f(m_i) * f(m_j)$ – the operator symbol changes. Can we conclude that the two groups are not isomorphic? We've just tried one function. If we could find subgroups of each, their number and orders that might help. If things don't match, can we conclude that the groups are not isomorphic?

Pop quiz: What are the remainders of 13^6, 11^6, and 5^6 when it is divided by 18?

Harder Finite Case

Just for fun it might be interesting to look at all the binary operations generally mentioned in a high school algebra book. Blitzer's Algebra and Trigonometry, 3rd or any edition will do. In the first chapter the natural, whole, rational, and irrational numbers are designated with $\mathbb{N}$, $\mathbb{W}$, $\mathbb{Q}$, and $\mathbb{I}$. The real

numbers and the complex numbers are given with $\mathbb{R}$ and $\mathbb{C}$. Generally all functions map the reals to the reals as in polynomials with integer coefficients; complex number tend to come up only as roots of polynomials – like quadratics. They have inverses and an identity: CIA I applies. In Chapter 7, Section 5 (Complex Numbers in Polar Form: DeMoivre's Theorem) we discover that nth roots of unity make a set under multiplication that seems very much like $(\equiv_n, +)$: $(RU_n, *)$, another finite group. The infinite sets that are closed under addition and multiplication are $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$.

A little more out of the main stream are functions (Chapter 2) and matrices (Chapter 8). Functions under composition and matrices under multiplication have identities and inverses (restrictions apply). Associativity isn't a problem, but closure requires some further refinements to arrive at groups. The lack of commutativity isn't a problem. That isn't one of the axioms required for a group. We certainly can immediately suspect that the easiest groups to create for these two will be infinite.

As with $(\mathbb{Z}, +)$ and $(\equiv_n, +)$, we can ask if there is a way to get finite sets of functions and matrices that are groups.

For matrices we can make the dimensions small 2×2 and we can use $\equiv_n, +$ for the elements. Matrices under addition shouldn't be a problem. We need a restriction for the existence of inverses when matrix multiplication is used. Our interest is more with functions.

For functions a good idea is to look at restricting the domain and range to finite sets. If one tried to determine if all linear forms $mx+b$s forms a group, you might succeed but given m and b are real numbers that's an infinite number of lines. Taking $\{1, 2, 3\}$ as the domain and f as a function on this domain, we are left with determining $\{f(1), f(2), f(3)\}$, the range. Functions don't have to be defined on numbers; we can define functions on sets or anything else. If we define a set of functions that take this finite set to all its permutations that might work. We can start with $f_0(\{1, 2, 3\}) = \{1, 2, 3\}$, an identity function? Say $f_1(123) = 321$, where we have abbreviated the permutations to three digit numbers, what is $f_0(f_1(123))$? It's 321, so $(123) \circ (321) = (321)$ when we further abbreviate composition to the usual $\circ$ operator. What permutation function corrects the typo *teh* and makes it *the*? How about a flip the second and third: $(132) \circ (teh) = the$. We are further abbreviating things.

Let's check our axioms and see if the permutation functions on $\{1, 2, 3\}$ is a group. Table 3 gives all the permutations. Permutations are a topic covered in Blitzer's Chapter 11, Section 6. One can evolve a mental algorithm for finding the composition of any two of the these functions. So, for example, $(321)(132)$ begets the thought sequence: 1 goes to 3 and 3 goes

	1	2	3
1	1	2	3
2	1	3	2
3	2	1	3
4	2	3	1
5	3	1	2
6	3	2	1

Table 3: The 3! permutations of three objects taken three at a time.

to 2; write $(2$; continue: 2 goes 2 and 2 goes to 3; add 3 to what you've written: $(23$; continue: 3 goes to 1 and 1 goes to 1; add 1 to what you've written: (231). The proof is by observation: if you have three different books and you do any sequence of orderings you will still have three books in some order. Its closed. Similarly reasoning yields it has an identity (don't do anything, that's a permutation), its associative and inverses exist (you can always get back to 123). It's a group; call it $Perms(\{1, 2, 3\})$ or, in general, $Perms(\{1, 2, \ldots, n\})$ or just $Perms_n$.

We note that it is not commutative: $(321)(132) = (231) \neq (132)(321) = (312)$. Blitzer mentions and gives an example of how function composition is not commutative, so one shouldn't be surprised.

We'd like a Cayley Table. This will be a 6 rows by 6 columns affair and will not be anywhere as easy as the previous tables. A TI-84 CE calculator with its programming and matrix capabilities comes to the rescue. As a quick proof of concept, we can put $Y_1 = (x = 1)3 + (x = 2)2 + (x = 3)1$ and $Y_2 = (x = 1)1 + (x = 2)3 + (x = 3)2$ into the calculator and then do a composition of these two with $Y_3 = Y_2(Y_1(x))$; see Figure 2, left. This is $(321)(132)$. Using the TI-84 table feature we can read of the result; it should be (231); see Figure 2, right.

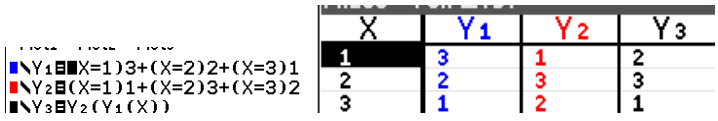

Figure 2: Zero is returned or 1, depending on X; TI-84's Table feature gives details.

The catch with this idea is we aren't going to get a completed 6x6 table any time soon. We want to use the calculators programming with its matrix features. It is going to be blissfully easy to make the table. Make a 6×3 table with the permutations; see Figure 3, left. Also make the $[B]$ matrix 6×6. Then create a program using the code in Figure 3, middle. Run the code and print matrix $[B]$, Figure 3, right.

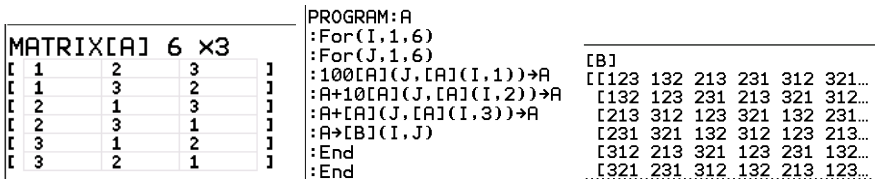

Figure 3: The TI84 allows for nesting in matrices; three digit numbers are used.

Just as a check, we note that, according to the this Table the left column's (132) on the second row there multiplied, so to speak, by the top row, 6th column's (321) is (312), row 2, column 6. Likewise $(321)(132) = (231)$ is confirmed.

Flattening Groups

We have three groups of order six: Figure 5. They look different, but are they? What the elements are called shouldn't matter: element 2 (aka 1) times element 2 is element 3 (aka 2) in $(\equiv_6, +)$; element 2 times element 2 is element 3 (aka 7) in $RP(\equiv_{18}, *)$; element 2 times element 2 is element 1 (aka 123, the identity) in $Perms\{1, 2, 3\}$. We could relabel these three groups with one through six and then look at them. This is just some busy work which you could make a program to do, but *by hand* works fine. The program in Figure 4 converts a group table $[B]$ into a flattened, as I call it, table $[C]$. It will work for any $[B]$ with positive integer values, not $(\equiv_6, +)$ with its 0 entries.

```
VAR NAME: AAAA

Ø01  Matr▸list([B],1,L₂)
Ø02  dim(L₂)→N
Ø03  max(L₂)→M
Ø04  M→dim(L₁)
Ø05  Fill(Ø,L₁)
Ø06  For(X,1,N)
Ø07  X→L₁(L₂(X))
Ø08  End
Ø09  {N,N}→dim([C])
Ø1Ø  For(I,1,N)
Ø11  For(J,1,N)
Ø12  L₁([B](I,J))→[C](I,J)
Ø13  End
Ø14  End
```

Figure 4: The first row of group table $[B]$ is moved to L_2 and L_2 initializes L_1 indexes $[B]$ with $[C]$.

0	1	2	3	4	5
1	2	3	4	5	0
2	3	4	5	0	1
3	4	5	0	1	2
4	5	0	1	2	3
5	0	1	2	3	4

```
prgmB
     [[1  5  7  11 13 17]
      [5  7  17 1  11 13]
      [7  17 13 5  1  11]
      [11 1  5  13 17 7 ]
      [13 11 1  17 7  5 ]
      [17 13 11 7  5  1 ]]
                     Done
```

```
[B]
[[123 132 213 231 312 321…
 [132 123 231 213 321 312…
 [213 312 123 321 132 231…
 [231 321 132 312 123 213…
 [312 213 321 123 231 132…
 [321 231 312 132 213 123…
```

Figure 5: Three groups of order six. Are they really different?

Pop Quiz: Does each row and column have one of each element? Prove that this must be true for groups? Can you identify subgroups in each? Prove that each column and row will have a copy of all the elements in a group.

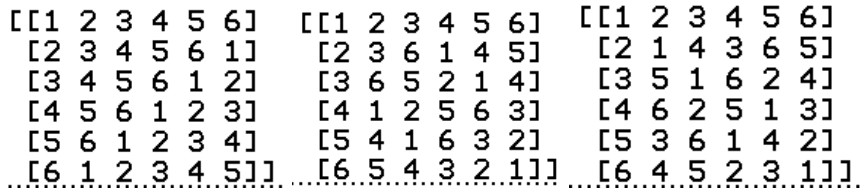

Figure 6: Left: $(\equiv_5, +)$; Middle: $RP(\equiv_{18}, *)$; Right: $Perms(\{1, 2, 3\})$.

We can create a isomorphism between the original versions of these groups and these flattened versions. The harder question is whether or not we can create an isomorphism between any two? There is also the notion of an automorphism. That is an isomorphism from a given group to itself. The existence of such a mapping would allow a relabeling of the elements that preserves the same structure.

Do you notice anything familiar about the three groups in Figure 6? They are all permutations of 6 things $\{1, 2, 3, 4, 5, 6\}$ taken 6 at a time. We should find each row (and column) in a table giving the $6! = 720$ such permutations. As we know such a beast is a group (720 rows by 720 columns) we should find these three groups as subgroups within it. It is a little much to work with $6!$, but not to worry after we look at some more examples, we will consider groups of order 4; $4!$ is just 24 and we can find our groups of order 4 all of them. Hopefully you are finding all this intriguing. All groups of any order n are subgroups of $Perms_n$. Is that enough for us to definitely differentiate different groups? Later.

More Examples

Consider the two groups $(\equiv_2, +)$ and $(\equiv_3, +)$. We can form ordered pairs from each and get six elements: $(\equiv_3, +) \times (\equiv_2, +)$; see the top row (and left column) of Table 4. We deeply suspect that $(\equiv_3 \times \equiv_2, +)$ is isomorphic to $(\equiv_6, +)$. But the flattened tables don't look the same.

We can so make subgroups out of such products of existing groups. In this product group the constituent groups are cyclic and hence commutative (or Abelian - fancy way of saying commutative). Can we go the other way and say all Abelian groups are products of such cyclic groups. This question is answered in Herstein's Section 13 (Direct Products) and Section 14 (Finite Abelian Groups). A related question: when is the converse of Lagrange true? Given the existence of a subgroup of G, we know its order is a divisor of the

		1	2	3	4	5	6
		$(0,0)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$
1	$(0,0)$	1	2	3	4	5	6
2	$(0,1)$	2	3	1	5	6	4
3	$(0,2)$	3	1	2	6	4	5
4	$(1,0)$	4	5	6	1	2	3
5	$(1,1)$	5	6	4	2	3	1
6	$(1,2)$	6	4	5	3	1	2

Table 4: The group $(\equiv_3, +) \times (\equiv_2, +)$ flattened.

order of G. If n divides the order of G when can we say that we know a subgroup of order n exists? Herstein partially answers that one in Section 12 (Sylow's Theorems): there are subgroups of prime power orders if that prime power divides a given group's order. What about composite divisors? Can we find a counter example? A group with a composite divisor that does not have a subgroup of that composite order? Later. Let's now pull back the lens.

It's a zoology

Plants and animals exist. We can think of groups as kinds of flora and fauna that we for various purposes (eating) might like to know about. Animals commute. They have organs. Groups have subgroups of various sizes – always divisors of a finite group size. We can see the organs of the different groups if we have a body of tricks (insights as given by theorems) with which to reason out the existence or non-existence of subgroups for a given group. We need to evolve a taxonomy or physiology for the corpses (sorry) that are on (in) these Cayley Tables.

A peek at Wikipedia's ideas on groups reveals that they do give for smaller groups details that does suggest somebody does think along the lines we do.

Can we prove something as simple as there is no possible isomorphism between two groups, necessarily of the same order but with one Abelian and one not? Well if G_{na} is the non-Abelian group, then two elements exist a and b in G_{na} such that $ab \neq ba$, so, if f is any isomorphism from G_{na} to G_a,

the Abelian group, then $f(ab) \neq f(ba)$, because this would imply $ab = ba$ by the one-to-one property of f. But $f(a)$ and $f(b)$ are in the Abelian group, so, $f(a)f(b) = f(b)f(a)$, but the homomorphism part of our isomorphism f then gives $f(ab) = f(ba)$, a contradiction.

Well okay, but why do mathematician brains like these groups so much? It might be because we tend to achieve tasks by finding the right order to do thinks and such *orders of doing things* are permutations of steps. To be candid, I use to frequently dress in the wrong order: shoes before socks, belt before pants and I would have to undress and dress through all the permutations before I would get it right. Then I studied group theory at Caltech with Foote the teacher with Peter Shor (quantum computing guy with droopy socks at the time) as a fellow student. By some kind of osmosis of the two I started getting the dressing order right. I've been properly clothed with minimal effort for years now. You can be too!

Orders of Groups

We left off with groups of order 6. We now have four: $(\equiv_6, +)$, $RP(\equiv_{18}, *)$, $Perms(\{1, 2, 3\})$, and 3×2. After some research, we are authoritatively told that there are just two groups of order 6: one Abelian, one non-Abelian. We know that $Perms_6$ is non-Abelian, so it must be that $(\equiv_6, +)$, $RP(\equiv_{18}, *)$ and 3×2 are isomorphic. How could we establish that?

Every element taken to consecutive powers will have to cycle back to the identity and define a *cyclic* subgroup: if $a \in G$, a group, let (a) denote the elements in this cyclic subgroup. It can be, it will be the case that prime order groups will have elements which have the same prime order as the group – that's implied by Lagrange. These elements, their cyclic subgroup will *generate* the group. As a quick check, consider $(\equiv_5, +)$; (1) generates the group. How about 2? Consider $2 + 2 = 4$; $2 + 2 + 2(6) \equiv 1 \bmod 5$; $2 + 2 + 2 + 2(8) \equiv 3 \bmod 5$, and $2 + 2 + 2 + 2 + 2(10 \equiv 0 \equiv \bmod 5$, so *yes* $(2) = \{0, 1, 2, 3, 4\}$, a generator.

We can create a program that will take powers and multiples of all the elements in $RP(\equiv_{18}, *)$ and $(\equiv_6, +)$. If we find generators g_1 and g_2, then $\phi : RP(\equiv_{18}, *) \rightarrow (\equiv_6, +)$ defined by $\phi(g_1) = g_2$ should be an isomorphism. We can reconfigure our tables for these groups so they are identical. We might also suspect that the various non-generators will have the same orders as well.

The TI-84 family of calculators has nice list features that make crunching powers and multiples especially easy. Look at the code in Figure 7, Left.

After forming a list with the elements of $RP(\equiv_{18}, *)$, we can take the power of the list in one step and also crunch remainders (the mod stuff) at the same time. We see that 5 and 11 are generators for $RP(\equiv_{18}, *)$ in the print out, Figure 7, Middle. The required isomorphism leaps out towards us in Figure 7, Right. In fact, we directly see $(\equiv_6, +)$ no staring at us. We have rearranged the order of the top column and left row to make things apparent.

Pop quiz: What are the elements and orders for the cyclic subgroups generated by $\{5, 7, 11, 13, 17\}$?

```
001 {1,5,7,11,13,17}→L1
002 Clear Entries
003 L1^Ø→L2:
004 List▸matr(L2,[A])
005 For(N,1,5)
006 remainder(L1^N,18)→L2
007 List▸matr(L2,[B])
008 augment([A],[B])→[A]
009 End
010 Disp [A]
```

```
[[1 1  1  1  1  1 ]
 [1 5  7  17 13 11]
 [1 7  13 1  7  13]
 [1 11 13 17 7  5 ]
 [1 13 7  1  13 7 ]
 [1 17 1  17 1  17]]
```

		1	5	7	17	13	11
		5^0	5^1	5^2	5^3	5^4	5^5
1	5^0	0	1	2	3	4	5
5	5^1	1	2	3	4	5	0
7	5^2	2	3	4	5	0	1
17	5^3	3	4	5	0	1	2
13	5^4	4	5	0	1	2	3
11	5^5	5	0	1	2	3	4

Figure 7: Left: Code for powers of the elements of $RP(\equiv_{18}, *)$; Middle: Rows give 0 to 5 power of $\{1, 5, 7, 11, 13, 17\}$ mod 18; Right: $\phi(5^n) = n$ shows $(\equiv_6, +)$.

We can generalize from this specific group to any flattened group. It would be rather nightmarish to calculate all the orders of $Perms_3$ for example. But given the flattened version we can write code to crunch the orders of the elements, now just $\{1, 2, 3, 4, 5, 6\}$. A TI84-CE can prompt for a matrix; not shown. You must navigate the matrix menu to specify the matrix (flattened group) you wish to crunch. Figure 8, Left shows the breathtakingly simple code that finds the orders of all elements of the standardized (better word than flattened) $Perms_3$ group, Figure 8, Right. There are three flips (order 2) and one rotation (order 3). As no element is of order 6, we can conclude that this group is not cyclic.

We should see elements of order 6 with the $RP(\equiv_{18}, *)$ group. Indeed, Figure 9 shows that 5 and 11 are generators of the order of the group; this group is cyclic.

A natural question to ask is whether or not all $RP(\equiv_n, *)$ are cyclic. We'll just dangle that proposition and move on.

Automorphisms

With these standardized groups we can immediately generate (witness, see) all one-to-one and onto mappings from a group to another group, including from a group to the same group. Not all will be isomorphisms (different

```
Disp 1
For(Y,2,6)
[C](Y,Y)→X:1→N
While (X≠1)
N+1→N:[C](X,Y)→X
End
Disp N+1
End
```

```
prgmAAORDER
1
2
2
3
3
2
Done
```

Figure 8: Left: the code just subs in the result of consecutive lookups; Right: the order of the orders indexes the original group.

```
prgmAAORDER
1
6
3
6
3
2
Done
```

Figure 9: With $[B]$ containing the standardized version of $RP(\equiv_{18}, *)$, the orders of each element are crunched.

range group) or automorphisms (same *range* group). Certainly, a mapping from a group generator to a non-group generator will not make the grade. To give the idea succinctly, consider the simple group of order 4 consisting of the powers of the complex number i: $i^0 = 1$, i, $i^2 = -1$, and $i^3 = -i$. We relabel these with the set $\{1, 2, 3, 4\}$ and make a Table for the standardized version (it's isomorphic to $(\equiv_4, +)$; all the permutations of these 4 objects taken 4 at a time are all the one-to-one and onto maps (bijections, for short). Suppose $\phi(x)$ is such a map given by $\phi : 1234 \rightarrow 2134$. This has the generator i going to -1, a non-generator. It shouldn't be an automorphism. A real automorphism is given by 1432.

We can demonstrate these ideas with a couple of TI-84 CE programs. In Figure 10, the matrix $[A]$ gives the group $|(\equiv_4, +)|$. The absolute value parallel lines indicate it's the standardized version. An automorphism, f is a bijection with the property that $f(xy) = f(x)f(y)$ where $x, y \in \{1, 2, 3, 4\}$. Thus $[A]$ the *clean* left side $f(xy)$ where 1234 is used, the identity map. All be have to do for the $f(xy)$ side where $f(x)$ is a permutation is find and swap per one of the $4!$ permutations. The code in Figure 11 does this per L_1, a list that the user provides that gives the permutation.

The left hand side of $f(xy) = f(x)f(y)$ can be generated by hand:

```
[A]
                [[1 2 3 4]
                 [2 3 4 1]
                 [3 4 1 2]
                 [4 1 2 3]]
```

Figure 10: $i^0 \to 1$; $i^1 \to 2$; $i^2 \to 3$; $i^3 \to 4$.

```
001 Prompt L₁
002 For(I,1,4)
003 For(J,1,4)
004 For(K,1,4)
005 If ([A](I,J)=K)
006 Then
007 L₁(K)→[B](I,J)
008 End
009 End
010 End
011 prgmAUTO
```

```
001 For(I,1,4)
002 For(J,1,4)
003 [A](L₁(I),L₁(J))→[C](I,J)
004 End
005 End
006 Disp ([C]=[B])
```

```
prgmAUTO2
L₁={1,4,3,2}
                                  1
                               Done
[B]
                [[1 4 3 2]
                 [4 3 2 1]
                 [3 2 1 4]
                 [2 1 4 3]]
```

Figure 11: Left: $f(xy)$ is a find and replace using L_1 and stores the result in matrix $[B]$; Middle (prgmAUTO): $f(x)f(y)$ uses $[A]$ and L_1 to *lookup* values and stores the result in $[C]$; Right: The 1 indicates $[C] = [B]$ and the permutation gives an automorphism.

given the permutation $abcd$ make all 1s as, all 2s bs, all 3s cs, and all 4s ds. Use Figure 10 and the permutation 1432 to arrive at Figure 11, Right. The permutation 2143 doesn't yield a automorphism. The lookup procedure for this permutation is given in Figure 12. Figure 13 shows the results of the TI program.

	2	1	4	3
2	(2,2)	(2,1)	(2,4)	(2,3)
1	(1,2)	(1,1)	(1,4)	(1,3)
4	(4,2)	(4,1)	(4,4)	(4,3)
3	(3,2)	(3,1)	(3,4)	(3,3)

	2	1	4	3
2	3	2	1	4
1	2	1	4	3
4	1	4	3	2
3	4	3	2	1

Figure 12: Left: The ordered pairs are used to locate (row,column) values in matrix $[A]$; Right: the result of this lookup.

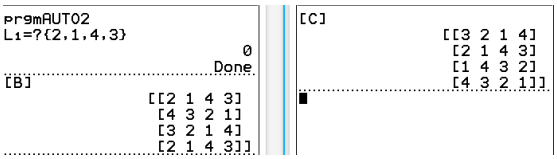

Figure 13: This permutation does not deliver a automorphism.

Homomorphisms

We have seen that every element of a group generates a cyclic subgroup. Sometimes the subgroup generated is the whole group; in which case, the group is itself a cyclic group. When an element doesn't generate the whole group, there are some elements in $G \setminus H$ (that's a set minus). For the record, H is generally a subgroup in this document. To make things more concrete, remember how $RP(\equiv_{18}, *)$ had two generators, 5 and 11, the rest of its elements have different orders and remnants in G. Why are we going on and on about subgroups under the heading *homomorphisms*?

Give me a chance! These isomorphisms and automorphisms are all homomorphisms. We have seen that one way to establish an isomorphism between two groups is to map a *generator* to a generator and see if it delivers an isomorphism. If it does the groups are really the same *up to isomorphism*. If we use a non-generator element what happens? We might get a homomorphism and that in turn might yield information about the image set in the *range* group and, here it is, the image set is likely a subgroup. We can use homomorphism to find subgroups of groups, to classify them by order and commutative or non-commutative. Is this enough of the DNA of a group to declare a unique species. Table x gives the framework we seek. The program might become (its a page turner) that we can generate automatically generators and then we might be able to get the subgroups to generate somehow something from a combination of a non-generator cyclic group with the remnants not in it. The whole thing starts to resemble an autopsy. You'll see. Let's keep going, shall we?

	T_1	T_2	T_3
G_1	$\#_{T_1}$	$\#_{T_2}$	$\#_{T_3}$
G_2	$\#_{T_1}$	$\#_{T_2}$	$\#_{T_3}$

Table 5: Three different types of subgroups; frequencies $\#$ in two groups.

If the number rows match are the groups isomorphic. Consider $H = (7) = \{1, 7, 13\}$ of $RP(\equiv_{18}, *)$. The remnant of this subgroup is $\{5, 11, 17\}$. We discover that $5H = 11H = 17H$ and that $1H = 7H = 13H = H$ by closure of a subgroup. We can make a new group $\{H, 5H\}$ of order 2.

Conclusion

These few programs should provide a stimulating introduction to group theory.

References

[1] Blitzer, R. (2010). *Algebra and Trignometry*, 3rd ed., Pearson.

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