

Ramón Fernández

MAE 501 Notes from 9/4/08.

Some Preliminaries on sets.

A set is a well defined collection of objects. Such objects are called elements of the set. By well defined we mean that for any given object, whether or not it is on the set or it must be unambiguous. For example, if a set contains all the tables of the classroom for MAE 501, then any object in the room can be determined as being either in the set or not in the set. If the room had no table/s, the set would be called the empty, or null set.

Some of the sets that we are to be constantly working in this class are:

- \mathbb{N} The set of natural numbers.
- \mathbb{Z} The set of all integers.
- \mathbb{Q} The set of all rational numbers.
- \mathbb{R} The set of all real numbers. Within \mathbb{R} we have the Irrationals, \mathbb{I} , and the Rationals.
- \mathbb{C} The set of all complex numbers: $a+ bi$ such that $a, b \in \mathbb{R}$ and $\sqrt{-1} = i$.

Within the set of irrational numbers, there is a specific irrational that has been of interest to mathematicians, philosophers, physicists, architects, artists, musicians and even humanists. This number is called the golden ratio, also referred to as the golden mean, the golden section, the golden cut and the divine proportion. It has a value of approximately 1.61803..., and is usually designated by the Greek letter tau, τ . The golden ratio is expressed as $(a+\sqrt{b})/2$, where $a=1$, $b=5$ and $c=2$. We showed in class a motivation of the golden ratio coming from a rectangle. I will like to motivate one based on sequences. Let us look at the additive sequence $A_{n+2} = A_{n+1} + A_n$. This sequence requires two seed values, which in the simplest case are $A_0 = 0$ and $A_1 = 1$, which produces the values ... -8, 5, -3, 2, -1, 1, 0, 1, 1, 2, 3, 5, 8, ... let us look at the geometric sequence $A_{n+1} = \alpha A_n$, where α is some constant factor. "Consider for example the possibility that a sequence could be both additive and geometric; that is, the terms would satisfy both $A_{n+2} = A_{n+1} + A_n$, and $A_{n+1} = \alpha A_n$, these two equations could be combined to give the constraining relations for α $A_{n+2} = \alpha A_{n+1} = \alpha^2 A_n$ ". Equating $\alpha^2 A_n = \alpha A_n + A_n$ and dividing by A_n we get the equation $\alpha^2 - \alpha - 1 = 0$. This is known as the Fibonacci equation and the two roots satisfying it are $\alpha_1 = (1+\sqrt{5})/2$ and $\alpha_2 = (1-\sqrt{5})/2$, which has as solution the golden ratio, which by definition is an algebraic number". For the acquisition of this number from the rectangles see Lisa's email.

Closed sets are different from sets closed under an operation, they should not be confused. A set is said to be **closed** when it contains its boundaries, $0 \leq x \leq 1 = [0, 1]$ is a closed set. A set S is said to be **closed under an operation** $*$, if the operation $*$ applied to members of S produces a member of S . Let us see for example the set of integers with the operation of addition. Let a, b be any two integers, then $a+b$ is just the sum of two integers, which is indeed an integer, therefore the set of integers is closed under addition.

We discussed in class what would be a natural way of learning sets of number and agreed in that it should be: $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$; the irrational and rational numbers are included within the real numbers. In this part of the notes we are to define the set of complex numbers. Please note that there are other ways of defining the set of complex numbers. Let us pass to the definition and motivation of the complex numbers and i .

The set of complex numbers may be defined as pairs of real numbers, $\mathbb{C} = \{ (x, y) : x, y \in \mathbb{R} \}$ containing the operations of addition $(x, y) + (a, b) = (x + a, y + b)$ and multiplication $(x, y) \times (a, b) = (xa - yb, xb + ya)$. If this definition seems to be vague, a good argument to believe in it is that the set of complex numbers is an extension of the real numbers and so these two binary operations are embedded in the complex numbers. For example take the complex number $(x, 0) + (y, 0) = (x+y, 0)$ and $(x, 0) \times (y, 0) = (xy, 0)$. We can readily see that in this form the complex numbers behave just like the real. From here we can add that the real numbers are those complex numbers whose second coordinate is zero. Motivated by this definition, let us think of any complex number (x, y) as a linear combination of $(1, 0)$ and $(0, 1)$ with the coefficients $x, y \in \mathbb{R}$. Let us think of the complex number $(1, 0)$ as the real number 1. Then we can write the ordered pair $(x, y) \in \mathbb{R}^2$ as $(x, 0) + (0, y) \in \mathbb{C}$. Looking at $(0, 1) \times (y, 0) = (0, y)$ we can rewrite the ordered pair (x, y) as $(x, 0) + (0, 1) \times (y, 0)$. To motivate the idea of i as being a complex number, let us remember that $\sqrt{-1} = i$ and $i^2 = -1$. Take the number $(0, 1)$ to be i , then using the definition of multiplication at the beginning, $i^2 = (0, 1) \times (0, 1) = (-1, 0)$. Thinking as the complex number $(-1, 0)$ as a real number with second coordinate zero, we can see that indeed, $i^2 = -1$. Keeping this definition in mind we can then rewrite the coordinate pair $(x, y) = (x, 0) + (0, 1) \times (y, 0)$ as $x + iy$. Most books denote this number as $z = x + iy$.

Using the previous notation, $z = x + iy$, we say that $\text{Re} z = x$, which means the real part of z is equal to x and $\text{Im} z = y$, meaning the imaginary part of $z = y$. When the x coordinates of z is zero, z is referred to as purely imaginary.

Algebraic and Transcendental Numbers.

A number a is algebraic, if \exists a non-zero polynomial with rational coefficients that has a as a root. i.e, if it satisfies a polynomial equation of the form: $x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n = 0$, where the coefficients a_i are all rational. If a is not algebraic, it is called transcendental.

Corollary: All rational numbers are algebraic.

Proof: Let x, y be any real numbers with x non-zero, then we can write x, y as y/x . We can always construct a polynomial of the form $x \cdot r - y = 0$. Clearly, y/x satisfies our polynomial, and since x and y were arbitrary, the proof is complete.

The converse of this corollary is not true, i.e. there exist irrational numbers that are algebraic. Just let a be $\sqrt{2}$, this is a root of the polynomial $x^2 - 2 = 0$, as required.

Group: a group is a set G closed under an operation $*$ satisfying the following properties:

- \forall elements $g, h, k \in G$, $(g*h)*k = g*(h*k)$ (associativity)
- $\exists e \in G$ called the identity or unit: $\forall g \in G$, $e*g = g*e = g$ (identity)
- $\forall g \in G$, \exists an element $g^{-1} \in G$ called the inverse: $g*g^{-1} = g^{-1}*g = e$. (inverses)

If \forall elements $g, h \in G$ the operation $*$ of a group G satisfies the commutative law $h*g = g*h$, then the group is called Abelian or equivalently commutative.

Theorem: For any group G , the identity element is unique. Also, for any element $g \in G$ there exists a unique element satisfying the condition of being its inverse.

Proof: Let us start with the identity.

Assume that e and r are both identity elements of a group G , then by definition

$$r = er = e$$

and the equality $r = er$ holds, since e is an identity, also the equality $e = re$ holds since r is an identity, thus by definition of our identity elements we have that $e = r$, so the identity is unique as required.

Now assume that given $g \in G$, m and n are both inverses of g . Then we will have that

$m = me = m(gn)$, since n is an inverse of G this equality holds. But since we are working on a group G , applying the associative law on this equation gives $m = me = m(gn) = (mg)n = en = n$, hence $m = n$, and the inverse of g is unique as required.

Examples of groups:ⁱⁱ

Groups of numbers.

We already proved that the integers were closed under the operation of addition. Let us show that \mathbb{Z} also satisfies all the properties of a group. For any elements $a, b, c \in \mathbb{Z}$, $(a+b)+c = a+(b+c)$ so \mathbb{Z} under addition is associative. There is an element $0 \in (\mathbb{Z} +)$ such that for any a in $(\mathbb{Z} +)$, $a+0 = 0+a = a$, so 0 is the identity of $(\mathbb{Z} +)$. For any element b of $(\mathbb{Z} +)$, $b+(-b) = 0 =$ identity, so $-b$ is the inverses of b , $\therefore (\mathbb{Z} +)$ is a group.

The real, rational and complex numbers all form groups under addition. In order to obtain a group under multiplication zero must be removed from these sets. Try proving this.

Groups of matrices.

Let $GL(2, \mathbb{R})$ be the group of all invertibleⁱⁱⁱ 2×2 matrices with real coefficients, under the operation of multiplication.

Multiplication of matrices is associative, as shown in class.

To find the inverse of a 2x2 matrix proceed as follows, Let A be

$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, the inverse of A can be found using the formula:

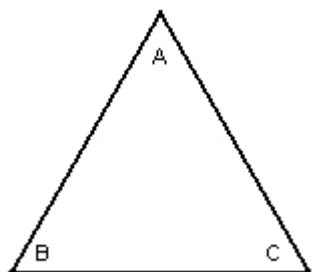
$$A^{-1} = \frac{1}{\det A} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix},$$

where the determinant of A = ad - bc, which is non-zero. So in $GL(2, \mathbb{R})$ every matrix has an inverse. In $GL(2, \mathbb{R})$ multiplying $(A^{-1} * A) = \text{Identity}$. $\therefore GL(2, \mathbb{R})$ under multiplication forms a group. We can also generalize this notions of groups to $GL(n, \mathbb{R})$, called the general linear group of all invertible nxn matrices with real coefficients.

The set of all upper-triangular matrices with both diagonal elements non-zero also forms a group under multiplication.

Groups of symmetries of the rigid motions of geometric figures.

Here we are to analyze the rigid motions of an equilateral triangle. There are many ways of picking up the triangle below and then setting it down again so that it looks the same as what we started with. We can accomplish this by performing rotations and reflections. In this case I am only going to work with rotations. The goal is to show that the rotations of the triangle below form a group. The elements of this group are going to be rotations by angles. Proof: identity. If we rotate the triangle by 360° then the rotation is equivalent to have done nothing to the triangle, giving us the identity. Existence of inverses: if we rotate the triangle by 60 degrees and then rotate again by 240 degrees we get back to the original triangle, which is the



identity.

If we perform one rotation followed by another rotation, we have just made a rotation equivalent to the sum of the angles of the individual rotations, which is also a rotation, so we get closure. To show associativity rotate fig 1 by 60 degrees followed by a rotation of 120 degrees followed by a rotation of 180 degrees, you get back to the identity. If now you reverse the order, apply a rotation of 180 degrees followed by a rotation of 120 degrees, followed by rotation of 60 degrees, we get to the identity, same result, so associativity holds.

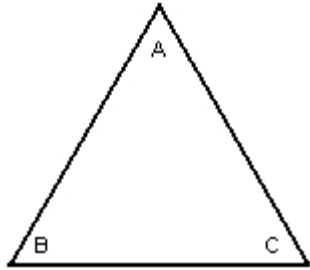


Fig (1)

So far we have studied sets with a single binary operation.^{iv} We will now introduce an algebraic structure^v that has two binary operations.

A **ring**^{vi} $[R, +, \cdot]$ is a set R with two operations $+$ and \cdot , called addition and multiplication such that R is closed under $+$ and \cdot , satisfying the following conditions:

1. The set R is Abelian under addition.
2. Multiplication is associative
3. $\forall a, b, c \in R$, the left and right distributive law holds, $(a+b)c = (ac) + (bc)$ and $a(b+c) = (ab) + (ac)$.

If in a ring multiplication is commutative, such ring is a **commutative ring**. A ring with multiplicative identity element is a **ring with unity**, and the multiplicative identity 1 is called **unity**.^{iii (p.172)} We mentioned in class that:

- There exists a multiplicative inverse.
- Not every element necessarily has multiplicative inverse, i.e. matrix under multiplication, polynomials with rational coefficients.

Corollary: Any subsets of the complex numbers that is a group under $+$ and happens to be closed under \cdot satisfies conditions 1-3, $\therefore \mathbb{Z}, (\mathbb{Q} \setminus 0), (\mathbb{R} \setminus 0), (\mathbb{C} \setminus 0)$ are all rings, as you should verify.

A multiplicative inverse of an element a in a ring R with unity $1 \neq 0$ is an element $a^{-1} \in R$ such that $a a^{-1} = a^{-1} a = 1$. If a multiplicative inverse for an element a in R exists it is unique. Proof:

Before we prove it we need to introduce the following definition.

Let R be a ring with unity $1 \neq 0$. An element u of R is a unit of R if it has a multiplicative inverse in R . If every non-zero element of R is a unit, then R is a division ring.

For our proof we need only the first definition. Assume that u is a unit in a ring R . Let $su = us = 1$ then s would be a multiplicative inverse for u . Assume also that $tu = ut = 1$, then t will also be a

multiplicative inverse for t . Now we have to show that $s = t$. The equation $s = s1$ is true; since we are in R associativity holds so $s = s1 = s(ut) = (su)t = 1t = t$. Hence $s=t$ as required.

References.^{vii}

ⁱ This section was acquired from : The Golden Ratio and Fibonacci Numbers. By Richard A. Dunlap.

ⁱⁱ These examples have been adapted from Numbers Groups and Codes 2nd Editions by J.F. Humphreys & M.Y. Prest.

ⁱⁱⁱ A matrix is said to be invertible if it has an inverse with respect to multiplication, equivalently, it has an inverse if its determinant is non-zero.

^{iv} A binary operation is a calculation that involves two operations.

^v An algebraic structure is a structure that consists of at least one set closed under at least one binary operation.

^{vi} The definitions presented here are mainly motivated from the book A First Course in Abstract Algebra by John B. Fraleigh 7th Edition. For an interesting historical Note see this book on page 168. Most of the definitions here are taken directly from the book. This material is still difficult for me and I did not want to jeopardize the learning of all of us in the class for which Most of the definitions in the section Rings here are taken directly from the book

^{vii} And of course, the core of the material comes from the notes we have all been constructing in class.