Roots, Symmetries, and Galois

Linxuan Ma

April 20, 2022

This exploratory question paper is inspired by IB Mathematics' paper 3 and its chapter on complex number. This question paper aims to demonstrates some observations regarding polynomials and roots as an extension to the respective topics in IB Math, and in the end, helps the reader gain some intuition towards Galois theory and abstract algebra in general.

Exercises marked with * are optional; the understanding of them are not necessary to progress in this paper, but nonetheless they might be good practices.

1 Fields

As Yink once said, "mathematics is the constant discovery of new objects". Indeed, we've covered numerous mathematical constructs in high school math, but can we generalize those constructs under some common attributes?

Exercise 1.1. Calculate the following expressions and state what type of object (aka. construct) their results are:

a. $5 + 3$

b. $[2, 7, 3] \times [2, 2, 1]$

c. $\frac{1}{2} * \frac{3}{5}$

What are some observations? Well, it seems that the type of the answers to the above expressions are of the same type as their constituent components, e.g. 8 is a natural number, and as is 5 and 3 in $5 + 3$.

This is the idea of a closure; intuitively, a closure states that "I have some elements of the same type, imma do some operations on them, and the result is also gonna be of that same type".

Definition 1.1. A set A forms a *closure* over $f : (A, \dots, A) \to A$. This generalizes the aforementioned binary operations as a binary operator $\otimes$ is just a fuction $\otimes : (A, A) \to A$.

Exercise 1.2. Give 3 more examples of closure.

Definition 1.2. A *rational number* is a number that can be expressed in the form $\frac{p}{q}$ where $p, q \in \mathbb{N}$, $q \neq 0$.

Exercise 1.3. Does the rational numbers $\mathbb{Q}$ form a closure under division? Proof or provide a counter-example.

Exercise 1.4. Does the natural numbers $\mathbb{N}$ form a closure under subtraction? Proof or provide a counter-example.

***Exercise 1.5.** Let $M(m, n)$ denote the set of matrices of size $m \times n$. Under what condition for m and n does $M(m, n)$ form a closure over matrix multiplication?

It is evident that not all operators preserve the type of the operands, such as division in the set of natural numbers. However, we notice that most mathematical construct that we've learned thus far has some sort of "addition" and "multiplication".

Take vectors for example. Vectors form a closure over addition. Moreover, we can define its multiplication as element-wise multiplication. Now, observe that the addition of vectors satisfies the following properties:

1. $\vec{a} + \vec{b} = \vec{b} + \vec{a}$
2. $(\vec{a} + \vec{b}) + \vec{c} = \vec{a} + (\vec{b} + \vec{c})$
3. $\vec{a} + \vec{0} = \vec{0} + \vec{a} = \vec{a}$
4. $\vec{a} + (-\vec{a}) = \vec{0}$

Exercise 1.6. If we replace additions in the above equation with the aforementioned element-wise multiplication, which rules still hold? For the ones that do not hold, what are some edits that we can make to make them hold while retaining the general structure of the rule?

The properties described above are so prevalent in mathematics that we assigned objects that satisfy the above criteria a special name. If addition and multiplication are defined (in a certain way; see below) for a type of object, then we call it a *field.*

Definition 1.3. A *field* $(A, \oplus, \otimes)$ consists of a set A, an addition operation $\oplus : (A, A) \to A$ and a multiplication operation $\otimes : (A, A) \to A$ such that $\oplus$ and $\otimes$ satisfies:

1. **Commutativity:** $a \oplus b = b \oplus a$ and $a \otimes b = b \otimes a$ for all $a, b \in A$.
2. **Associativity:** $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ and $(a \otimes b) \otimes c = a \otimes (b \otimes c)$ for all $a, b, c \in A$.
3. **Identity:** There exists an identity element $0 \in A$ such that $\forall x \in A,\ 0 \oplus x = x$. The same applies for the multiplication operation, except that the multiplicative identity is often referred to as 1.
4. **Identity:** For all $x \in A$ there exists an additive $-x$ such that $x \oplus (-x) = 0$. Similarly, for all $x \in A$ there exists a multiplicative inverse x^{-1} such that $x \otimes x^{-1} = 1$.
5. **Distributivity:** $\otimes$ is distributive over $\oplus$: $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$.

Exercise 1.7. Proof that vectors in $\mathbb{R}^n$ for any $n \in \mathbb{N}$ is a field under vector addition and element-wise multiplication.

Exercise 1.8. Vector cross product is distributive over addition. However, vector under addition and cross product does *not* form a field. Explain why.

Note that the above definition also covers subtraction and division, as they are just inverses of addition and multiplication respectively.

From this point on, unless explicitly specified, the addition and multiplication of all mentioned fields default to the ordinary $+$ and $*$ respectively.

The benefit of forming a field is that we can now define polynomials with a set. To illustrate, in the case of $\mathbb{Q}$, we can define a polynomial like:

$$f(x) = \frac{69}{x^2} + 69x^2 + \frac{1}{69}x + 69$$

Note that all coefficients are elements of $\mathbb{Q}$. In addition, don't get thrown off by variables as denominators in a fraction; they are simply x to negative powers!

So, $\mathbb{Q}$ is a field. That means we can do whatever operations on its member, and the result will still end up inside $\mathbb{Q}$ (due to closure), right? While this is the case for $+$ and $*$, there are some operations that do not form a closure over $\mathbb{Q}$. The most notable example is the square root function.

1.1 Field Extensions

Exercise 1.9. Proof that $\sqrt{2}$ is not a rational number, i.e. cannot be expressed in the form $\frac{p}{q}$ for some $p, q \in \mathbb{N}$, $q \neq 0$ (hint: try proving by contradiction).

Uh oh, as nice as the rational numbers are, they do not include certain numbers such as $\sqrt{2}$. However, we can still squeeze $\sqrt{2}$ in there if we really wanted. Nothing can go wrong, right? Addition and multiplication still preserve their properties even when $\sqrt{2}$ is introduced, so there is no reason why we can't extend our "rational number" field to include just this one irrational number $\sqrt{2}$. This is the idea of *field extensions*.

Definition 1.4. The field $(F, \oplus_F, \otimes_F)$ is an extension to the field $(E, \oplus_E, \otimes_E)$ if the two fields satisfy:

1. $E \subseteq F$
2. $\oplus_E$ is simply $\oplus_F$ restricted to E, i.e. $\oplus_F$ over the stricter domain E instead of the original domain F
3. $\otimes_E$ is simply $\otimes_F$ restricted to E

By squeezing $\sqrt{2}$ into the elements of the rational number field, we obtain a field over the rational numbers and $\sqrt{2}$, whose elements are of the form $a + b\sqrt{2}$ where $a, b \in \mathbb{Q}$. This field extension of $\mathbb{Q}$ with $\sqrt{2}$ is denoted as $\mathbb{Q}[\sqrt{2}]$.

Exercise 1.10. Proof that the elements of $\mathbb{Q}[\sqrt{2}]$ is closed under addition and multiplication.

Exercise 1.11. Hence or otherwise, proof that $\mathbb{Q}[\sqrt{2}]$ is a field.