Nature of Algebraic Numbers

Zoe Daunt and Maitreyee Joshi

Northeastern University

25 April 2019

Abstract

We explore the behavior of algebraic numbers in relation to field theory, as well as the construction of relevant extension fields using quotient rings. We apply this method to gain a better understanding of splitting fields and Galois theory.

1 Introduction

In this project, we will be exploring the topic of Algebraic Numbers. In particular, we will be focusing on the behavior of algebraic numbers in fields and field extensions. A number is algebraic over a field F if it can be expressed as the solution to a polynomial equation with coefficients in F. If it cannot be expressed in that way, we call it transcendental over F. We examine how it is possible for a polynomial equation to have no solution in a field, yet have one or more solutions in an extension of that field. This occurs when a polynomial is irreducible over the original field. However, we can adjoin transcendental numbers to our field in order to create a field extension, over which that number is now algebraic. For example, π is not algebraic over Q (the field of rational numbers) but after extending Q to $Q(\pi)$, π becomes algebraic. We use ideas from ring theory to explore this topic in detail.

2 Motivation

When we were researching different possible topics for our extra credit project, we stumbled upon Algebraic/Transcendental Numbers. After reading more about them online and in our course textbook, we were both very interested in algebraic constructions.

This interest was sparked by wanting to investigate basic ideas obstructing polynomial roots. Both of us have studied relevant material in history of mathematics, and we were drawn to ideas such as the irrationality of $\sqrt{2}$.

Although these topics were not quite rigorous enough, they brought us on a journey that changed our focus from studying mathematical objects in isolation to a collection of mathematical objects. As we delved into the collections of mathematical objects, we began to look at their properties and chose to explore behavior of numbers algebraic in nature in regard to fields and field extensions. While we have taken courses relevant to this topic, we expected it to be quite rigorous and anticipated the need to study modern algebra in greater depth. Since a lot of the material covered in our number theory textbook was pretty straight-forward, the suggestion of applying the topic to a difficult area such as fields was appealing.

Over the course of this project, we hope to gain a deeper understanding of the characteristics of numbers across algebraic field extensions.

3 Definitions

Though we also define things throughout our paper, here are some definitions that we will reference.

- Field Axioms:
  - Associativity: addition $(a + b) + c = a + (b + c)$
    multiplication $(ab)c = a(bc)$.
  - Commutativity: addition $a + b = b + a$
    multiplication $ab = ba$.
  - Distributivity: addition $a(b + c) = ab + ac$
    multiplication $(a + b)c = ac + bc$.
  - Identity: addition $a + 0 = a = 0 + a + ac$
    multiplication $a * 1 = a = 1 * a$.
  - Inverses: addition $a + (-a) = 0 = (-a) + a$
    multiplication $aa^{-1} = 1 = a^{-1}a$ if $a \neq 0$.
- Ring Axioms:
  - Associativity: addition $(a + b) + c = a + (b + c)$
    multiplication $(ab)c = a(bc)$.
  - Commutativity: addition $a + b = b + a$
  - Distributivity: addition $a(b + c) = ab + ac$
    multiplication $(a + b)c = ac + bc$.
  - Identity: addition $a + 0 = a = 0 + a + ac$
  - Inverse: addition $a + (-a) = 0 = (-a) + a$
- We refer to Q as the field of rational numbers, or numbers of the form $\frac{m}{n}$, where m and n are integers.

4 Part I - What are Algebraic Numbers?

We began by defining algebraic numbers and briefly discussing extension fields.

Definition 1 A field K is said to be an extension field of a field F if F is a subset of K that satisfies all the field axioms with the same operations of K. We can also think of F as a subfield of K. We denote this extension as K/F.

As we stated in the introduction, we can consider a field F, and adjoin one or more elements that are solutions to an irreducible polynomial in F to construct an extension field. By adjoining elements that were not in the subfield F, some numbers that were not algebraic over F may be algebraic over its field extension, as in our $Q(\pi)$ example. This kind of extension field is more thoroughly defined in the following definition.

Definition 2 Let F be an extension field of K, and let $u_1, u_2, ..., u_n \in F$. The smallest subfield of F that contains K and $u_1, u_2, ..., u_n$ will be denoted by $K(u_1, u_2, ..., u_n)$. It is called the **extension field of K generated by** $u_1, u_2, ..., u_n$. Alternatively, $K(u_1, u_2, ..., u_n)$ is called the **extension field of K defined by adjoining** $u_1, u_2, ..., u_n$ to K.

We see this definition if we consider the extension field of the rationals.

Example 1 Say we have Q be the field of rational numbers. π is transcendental over Q, as in it cannot be defined as a solution to a polynomial with rational coefficients. However, if we adjoin π to Q, then we have $Q(\pi)$ as an extension field of Q over which π is transcendental.

As we explored these examples, we realized that there is a more general way of constructing these field extensions, which led us to polynomial rings. We were considering the field extension of the field Q that includes i, or $Q(i)$ which can also be described as the quotient ring $Q[x]/\langle x^2 + 1\rangle$.

Definition 3 A quotient ring is a ring that is the quotient of a ring A and one of its ideals a, denoted by A/a.

Definition 4 An ideal is a subset I of elements in a ring R that forms an additive group and has the property that, whenever x belongs to R and y belongs to I, then xy and yx belong to I.

For example, we could take ring A to be $\mathbb{Z}$ and the ideal to be $6\mathbb{Z}$. The quotient ring is $\mathbb{Z}_6 = \mathbb{Z}/6\mathbb{Z}$.

This method of constructing extension fields is efficient in that it ensures that the extension field still satisfies all the axioms of its subfield. Let's take a look at an example of this phenomenon.

Example 2 If we wanted to adjoin $\sqrt[3]{2}$ to Q, we would want to adjoin any root of the polynomial $x^3 - 2$. If we let u be any root of that polynomial, then $Q(u)$ is isomorphic to the quotient ring $Q[x]/\langle x^3 - 2\rangle$. This accounts for the roots of $x^3 - 2$ other than the obvious $\sqrt[3]{2}$. These would be of the form $\omega\sqrt[3]{2}$, where ω is a complex number that satisfies $\omega^3 = 1$. $x^3 - 1 = (x - 1)(x^2 + x + 1)$, so we can let ω be a root of $x^2 + x + 1$, so $\omega = \frac{-1}{2} + \frac{\sqrt{3}i}{2}$. Therefore $\omega^2 = \frac{-1}{2} - \frac{\sqrt{3}i}{2}$. From this we see that $\sqrt[3]{2}, \omega\sqrt[3]{2}$, and $\omega^2\sqrt[3]{2}$ are roots of $x^3 - 2$. Later we will see that this example can be used to describe a splitting field over Q.

A quotient ring equivalent to an extension field is more clearly described in the following proposition:

Definition 5 Let $\mathbb{F}$ be a finite field of characteristic p, and let $a \in \mathbb{F}$. A minimal polynomial for a is an irreducible polynomial $m(x) \in \mathbb{Z}_p[x]$ such that $m(a) = 0$.

Example 3 Let p be a prime, let $m(x) \in \mathbb{Z}_p[x]$ be an irreducible polynomial, and let $\mathbb{F}$ be a field

$$\mathbb{F} = \mathbb{Z}_p[x]/(m(x))$$

Let a denote the residue class of x modulo $m(x)$, i.e. the element of $\mathbb{F}$ corre-

sponding to x. Then $m(a) = 0$ in $\mathbb{F}$, so m is the minimal polynomial for a.
Proposition Let F be an extension field of K, and let $u \in F$.
If u is algebraic over K, then $K(u) \cong K[x]/\langle p(x)\rangle$, where $p(x)$ is the minimal polynomial of u over K.
Proof: (For the following proof, we rely on our background knowledge in group theory for understanding)
Define $\phi_u : K[x] \to F$ by $\phi_u(f(x)) = f(u)$, for all polynomials $f(x) \in K[x]$. This defines a ring homomorphism, and $ker(\phi_u)$ is the set of all polynomials $f(x)$ with $f(u) = 0$. The image of ϕ_u is a subring of F consisting of all elements of the form $a_0 + a_1u + ... + a_nu^n$, and it must be contained in every subring of F that contains K and u. In particular, the image of ϕ_u must be contained in $K(u)$.

If u is algebraic over K, then $ker(\phi_u) = \langle p(x)\rangle$, for the minimal polynomial $p(x)$ of u over K. In this case the fundamental homomorphism theorem for rings implies that the image of ϕ_u is isomorphic to $K[x]/\langle p(x)\rangle$, which is a field since $p(x)$ is irreducible. But then the image of ϕ_u must in fact be equal to $K(u)$, since the image is a subfield containing K and u. □

Knowing this proposition helps us to be able to thoroughly construct these extension fields and better understand them. As we became more familiar with this process we were introduced to splitting fields, and were very interested to see where they would take us.

5 Part II - Splitting Fields/Galois Theory

We say that a polynomial splits over F[X](or, more loosely, in F) if it is a product of polynomials of degree 1 in F[X]. Let F(α) be a simple field extension of a field F ,and let φ_n: F $\to \Omega$ be a homomorphism from F into a second field Ω. More specifically, if α is algebraic over F ,with minimum polynomial f(X), then the map $\varphi \mapsto \varphi(\alpha)$ defines a one-to-one correspondence $\{$extension φ: F[α] $\to \Omega$ of φ_0 $\} \leftrightarrow \{$roots of $\varphi_0 f$ in Ω $\}$. In particular, the number of such maps is the number of distinct roots of $\varphi_0 f$ in Ω.
Definition 6: Let f be a polynomial with coefficients in F . A field E containing F is said to split f if f splits in E[X]:

$$f(X) = a\prod_{i=1}^{m}(X - \alpha_i)$$

with all $\alpha_i \in$ E.
If E splits f and is generated by the roots of f ,

$$E = F[\alpha_1, ..., \alpha_m]$$

then it is called a splitting or root field for f .
Note that $\prod f_i(X^{m_i})(m_i \geq 1)$ and $\prod f_i(X)$ have the same splitting fields. Note also that f splits in E if it has $deg(f) - 1$ roots in E because the sum of the roots off lies in F.

Example 4: As seen in the example in the section above $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$ are the roots of $x^3 - 2$. Thus we obtain the splitting field as $\mathbb{Q}(\omega, \sqrt[3]{2})$. We claim that the degree of the splitting field over $\mathbb{Q}$ is 6. Since, $x^3 - 2$ is irreducible over $\mathbb{Q}$, we have $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. The polynomial $x^2 + x + 1$ is irreducible over $\mathbb{Q}$ and stays irreducible over $\mathbb{Q}(\sqrt[3]{2})$ since it has no root in that field. The degree of $x^2 + x + 1$ is not a divisor of $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$. Since ω is a root of $x^2 + x + 1$, this implies $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2})] = 2$.
Example 5:Let $f(X) = X^3 + aX^2 + bX + c \in \mathbb{Q}[X]$ be irreducible, and let $\alpha_1, \alpha_2, \alpha_3$ be its roots in C. Then $\mathbb{Q}[\alpha_1, \alpha_2, \alpha_3] = \mathbb{Q}[\alpha_1, \alpha_2]$ is a splitting field for f(X). Note that $[\mathbb{Q}[\alpha_1] : \mathbb{Q}] = 3$ and that $[\mathbb{Q}[\alpha_1, \alpha_2] : \mathbb{Q}[\alpha_1, \alpha_2]] = 1$ or 2, and so $[\mathbb{Q}[\alpha_1, \alpha_2] : \mathbb{Q}] = 3$ or 6. So splitting field of $X^3+10X+1$ has degree 6 over $\mathbb{Q}$.

Does a splitting field always exists?
Definition 7 Let f be a monic irreducible polynomial in $F[X]$. A pair (E, α) consiting of an extension E of F and an $\alpha \in E$ is called **a stem field for** f if $E = F[\alpha]$ and $f(\alpha) = 0$
Proposition: Every polynomial $f \in F[X]$ has a splitting field E_f, and $[E_f : F] \leq (deg\, f)$
Proof: Let $F_1 = F[\alpha_1]$ be a stem field for some monic irreducible factor of f in $F[X]$. Then $f(\alpha_1) = 0$, and we let F_2=$F_1[\alpha_2]$ be a stem field for some monic irreducible factor of $f(X)/(X - \alpha_1)$ in $F_1[X]$. As so forth, we arrive at the splitting field E_f. Let $n = \deg f$.
Then $[F_1 : F] = \deg g_1 \leq n, [F_2 : F_1] \leq n - 1, ...$, and so $[E_f : F] \leq n!$ □

What is a Galois Group?
Let F ⊂ K be a field extension. The Galois group of K over F is the group of all automorphisms of K which preserve F. The Galois group of a polynomial is defined as the Galois group of its splitting field. It is denoted by G(K/F).

Properties of Splitting Field
Let f(x) be an irreducible polynomial of degree n over a field F of characteristic 0. If f(x) is reducible over F, it will have roots in the existing field, and therefore not be a splitting field. Let K be the splitting field for f(x). Then the following facts hold:
a) All roots of f(x) in K are distinct, we can denote them by $x_1, ..., x_n$
b) The Galois group G(K/F) acts on the set $\{x_1, ..., x_n\}$ by permutations.
c) An automorphism $\varphi \in$ G(K/F) is completely determined by its values on the roots $\varphi(x_1), ..., \varphi(x_n)$, so G(K/F) is isomorphic to a subgroup of S_n.
d) The size of the Galois group equals the degree of the splitting field: $|G(K/F)| = [K : F]$.
e) The action of G(K/F) on the set of roots is transitive, that is, has one orbit.
Example 6: Consider again the polynomial $f(x) = x^3 + x + 1$ over Q. As explained above, its splitting field K has degree 6, so $|G(K/Q)| = 6$. On the other hand, G(K/Q) is a subgroup of S3 and $|S3| = 6$. Therefore G(K/Q) = S3. This is the first example of a non-commutative Galois group.

Constructing Splitting Fields
Since ancient times, Greeks finding roots of polynomial equation has been in the spotlight, but some polynomials such as x^2+1 over R do not have solutions. But by constructing a splitting field for such a polynomial we can find the roots of this polynomial in the new field. When K is a field and $f(T)/inK[T]$ is non-constant, there is a field extension $K\prime/K$ in which $f(T)$ picks up a root, say α. The $f(T) = (T-\alpha)g(T)$ where $g(T) \in K\prime[T]$ and $\deg g = \deg f - 1$. By applying the same process to $g(T)$ and continuing in this way finitely many times, we reach an extension L/K in which $f(T)$ splits into linear factors: in $L(T)$,

$$f(T) = c(T-\alpha_1)...(T-\alpha_n)$$

This field $K(\alpha_1, ..., \alpha_n)$ that is generated by the roots of $f(T)$ over K is a splitting field of $f(T)$ over K.

Steps for construction
Let F be a field and $g(x)$ be a polynomial in the polynomial ring of $F[X]$ of degree n. So now we construct a sequence of fields $F = K_0, K_1, .., K_{r-1}, K_r = K$ such that K_i is an extension of K_{i-1} which contains new root of $g(x)$. This construction will give us at most n extensions which is also the maximum number of roots of $g(x)$.

1. Factorize $g(x)$ over K_i into irreducible factors $f_i(X)f_2(X)..f_k(X)$.
2. Choose any non-linear irreducible factor $f(X) = f_i(X)$
3. Construct the field extension of K_{i+1} of K_i as the quotient ring $K_{i+1} = K_i[X]/f(X)$ where $f(X)$ denotes the ideal in $K_i[X]$ generated by $f(X)$
4. Repeat the process for K_{i+1} until $g(X)$ completely factors.

Example 7 A splitting field of T^2+1 over $\mathbb{R}$ is $\mathbb{R}(i,-i) = \mathbb{R}(i)$=$\mathbb{C}$
Example 8 A splitting field of T^2-2 over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2})$, since we pick up two roots in the field generated by just one of the roots.
Example 9 In $\mathbb{C}[T]$, a factorization of T^4-2 is $(T-\sqrt[4]{2})(T+\sqrt[4]{2})(T-i\sqrt[4]{2})(T+i\sqrt[4]{2})$. A splitting field of T^4-2 over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i)$. (Conrad)
While exploring ways of constructing these splitting fields, it seemed important to note that the splitting field of a polynomial is a bigger extension, in general, than the extension generated by a single root. For example, $\mathbb{Q}(\sqrt[4]{2}, i)$ is bigger than $\mathbb{Q}(\sqrt[4]{2})$.

6 Conclusion

Throughout the process of this project we were met with challenges. One was that we were both at different levels of understanding with regard to rings and fields. This hindered our learning process as we had to clear up confusion

with regards to groups and further related axioms for fields and rings before continuing to splitting fields and such. Another obstacle was that most of this was very new material for us, as we have not taken any courses on rings and fields yet. Because of this we had trouble sorting out the most important parts of the material. This project is important to us because by researching and recording what we find to be important in a way that we can comprehend can help others to understand the material as well. While we ended up straying away from discussing algebraic numbers in general, we feel that it was appropriate to let our path change, as the splitting field material allowed us to focus in on some of the building blocks of finite extensions.

Overall, we wish we could have spent more time with the topic and learned more about it, but also feel like we got the basics down and would be able to explain the important parts to someone with some experience in abstract algebra. One if the most gratifying aspects, however, is that delving into this topic exposed us to the study of rings and fields in mathematics, which sparked both of our interests. We hope to take that course eventually and possibly return to this topic with fresh eyes in the future.

7 Bibliography

- Artin, Michael (2011), *Algebra*, Pearson Education.
- Beachy, J. and Blair, W. (2006), *Abstract Algebra*, Waveland Press Inc: Illinois.
- Milne,J.S (2018),*Fields and Galois Theory*, www.jmilne.org/math/CourseNotes/FT.pdf.
- Conrad, Kieth, *Splitting Fields* kconrad.math.uconn.edu/blurbs/galoistheory/splittingfields.pdf.