# AN INTRODUCTION TO ALGEBRAIC NUMBERS AND ALGEBRAIC INTEGERS

MATIAS RELYEA

Abstract. In this brief introduction to algebraic numbers and algebraic integers, we will explore some properties of finite-dimensional vector spaces, and through the language of algebraic numbers and algebraic integers, state and prove several fundamental results in field theory and ring theory; namely that the set of algebraic numbers forms a field and that the set of algebraic integers forms a ring. These structures are related to and stem from their respective algebraic number fields, known as $\mathbb{Q}$ modules and $\mathbb{Z}$ modules respectively.

## Contents



## Introduction

Algebraic numbers and algebraic integers form a significant part of the study of Algebraic Number Theory, beginning with algebraic number fields (of which we mention very briefly in this paper), continuing with algebraic properties in particular domains and structures, the extent to which properties of unique or non-unique factorization are satisfied, and so on. What we cover in this paper is only a brief and elementary introduction to algebraic numbers and algebraic integers, as well as some algebraic background for the formulation and structure of certain mathematical objects.

*Date*: Summer 2022.

We will first introduce vector spaces, which form the foundation of linear algebra. Then we will proceed by defining the algebraic number fields in study: namely $\mathbb{Q}$ modules and $\mathbb{Z}$ modules. These will guide us through our study of fields of algebraic numbers and rings of algebraic integers. We will then prove their respective properties, and prove another significant result surrounding the nature of $\mathbb{Q}[x]$ and $\mathbb{Q}(x)$, which are the ring of polynomials with rational coefficients and the set of rational polynomials respectively.

To gain a better understanding of how these results are related to number theory, and how they follow into more advanced topics of algebraic number theory, [IRR90] is a fantastic source for a rigorous introduction and broad coverage. To study linear algebra, [Axl15] is a great place to start, as it begins with an informative and detailed introduction to vector spaces and algebraic structures. There are also numerous other sources that contain irrefutably interesting and integral material, but I will not list them here as they lie beyond the scope of this paper.

## 1. Preliminaries

### 1.1. **Vector Spaces.** We will begin by defining vector spaces.

**Definition 1.1** (Vector Space)**.** We define a vector space to be a set $V$ with an addition and scalar multiplication on $V$ that satisfies the following:

(1) $u + v = v + u$ for all $u, v \in V$ (commutativity),
(2) $(u + v) + w = u + (v + w)$ and $(\alpha\beta)z = \alpha(\beta v)$ for all $u, v, w \in V$ and $\alpha, \beta \in \mathbb{C}$ (associativity),
(3) $\alpha(u + v) = \alpha u + \alpha v$ and $(\alpha + \beta)v = \alpha v + \beta v$ for all $u, v \in V$ and $\alpha, \beta \in \mathbb{C}$ (distributivity),
(4) the existence of an additive identity $0 \in V$ such that $v+0 = v$ for all $v \in V$,
(5) the existence of an additive inverse such that for every $v \in V$ there exists some $w \in V$ where $v + w = 0$,
(6) the existence of a multiplicative identity $1 \in V$ such that $1v = v$ for all $v \in V$.

Note that the scalars $\alpha, \beta \in \mathbb{C}$ defined above can in fact be elements of any field; in this paper, we will use the complex number field $\mathbb{C}$ for the sake of simplicity in the construction of algebraic numbers and algebraic integers, but it very well may be extended to $\mathbb{R}$ or something similar. The following properties are not difficult to prove.

**Lemma 1.2.** *A vector space has a unique additive identity and inverse.*

**Lemma 1.3.** $0v = v$ *for every* $v \in V$.

**Lemma 1.4.** $\alpha 0 = 0$ *for every* $\alpha \in \mathbb{C}$.

**Lemma 1.5.** $(-1)v = -v$ *for every* $v \in V$.

We will now define a subspace.

**Definition 1.6** (Subspace)**.** A subset $U \subset V$ is defined as a subspace if $U$ is also a vector space.

It is not difficult to show that a subset of $V$ is a subspace. In order to do so, we need only check that it possesses an additive identity, and is closed under addition and multiplication.

**Definition 1.7** (Linear Combination)**.** For some list of vectors $(v_1, v_2, \ldots, v_n) \in V$, its linear combination is a vector of the form

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$$

where $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$.

**Definition 1.8** (Span)**.** We define the span of a list of vectors $(v_1, v_2, \ldots, v_n) \in V$ to be the set of all linear combinations. We write this as

$$\text{span}(v_1, v_2, \ldots, v_n) = \{\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n \mid \alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}\}.$$

**Definition 1.9** (Finite-Dimensional Vector Space)**.** We say that a vector space $V$ is finite-dimensional if there exists some finite list of vectors in $V$ such that its span is equivalent to the vector space. This list of vectors is known as a spanning list of $V$.

We say that a vector space that does not contain a finite list of vectors that spans the vector space is an **infinite-dimensional vector space**. We will not explore this concept in this paper, but it can be proven that if the dimension of the vector space is indeterminable, then the vector space is infinite-dimensional.

**Definition 1.10** (Linear Independence)**.** A list of vectors $(v_1, v_2, \ldots, v_n) \in V$ is linearly independent if the only way for its linear combination to be 0 is for all scalars multiples to be 0. In other words,

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0$$

is possible if and only if $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$.

**Definition 1.11** (Basis)**.** We define the basis of a finite-dimensional vector space $V$ to be a list of vectors that both spans $V$ and is linearly independent in $V$.

These will be useful later.

1.2. **Algebraic Numbers and Algebraic Integers.** We now introduce the algebraic numbers and algebraic integers. They are the focus of this paper, but what concerns us the most, on an elementary scale, is their algebraic structures, and how they can be used to prove certain properties across other algebraic structure. At the end of this subsection we will prove an important property regarding the algebraic integers that allows us to solve polynomial equations.

**Definition 1.12** (Algebraic Number)**.** An algebraic number is a complex number that is the root of some polynomial

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n,$$

where $a_0, a_1, a_2, \ldots, a_n \in \mathbb{Q}$. We will denote the set of all algebraic numbers as $\bar{\mathbb{Q}}$.

We may say, for instance, that $\sqrt{2}/2$ is an algebraic number, as it is a root of another polynomial.

**Definition 1.13** (Algebraic Integer)**.** Naturally, an algebraic integer is thus the root of some monic polynomial

$$x^n + b_1x^{n-1} + b_2x^{n-2} + \cdots + b_{n-1}x + b_n,$$

where $b_1, b_2, \ldots, b_n \in \mathbb{Z}$. We will denote the set of all algebraic integers as $\bar{\mathbb{Z}}$.

We may say, for instance, that $\sqrt{2}$ is an algebraic integer, as it is a root of the monic irreducible polynomial $x^2 - 2$.

Numbers that are neither algebraic numbers nor algebraic integers are known as **transcendental** numbers. For example, $e$ and $\pi$ are both transcendental, as they are not roots of polynomial equations with either rational or integer coefficients.

**Theorem 1.14.** *A rational number $r \in \mathbb{Q}$ is an algebraic integer if and only if it is a rational integer.*

*Proof.* To prove the backward direction, consider some $r \in \mathbb{Z}$. Then $r$ is clearly a root of the monic polynomial $x - r = 0$, so $r$ is an algebraic integer.

To prove the forward direction, suppose that $r \in \mathbb{Q}$, and that it is an algebraic integer. Then, by the definition of an algebraic integer, it satisfies the monic polynomial equation

$$x^n + b_1x^{n-1} + b_2x^{n-2} + \cdots + b_{n-1}x + b_n = 0, \tag{1}$$

where $b_1, b_2, \ldots, b_n \in \mathbb{Z}$. We let $r = c/d$ for $c, d \in \mathbb{Z}$ and $\gcd(c, d) = 1$. Allowing $r$ to be a root of (1), we substitute it for $x$ to obtain

$$\begin{aligned}\left(\frac{c}{d}\right)^n + b_1\left(\frac{c}{d}\right)^{n-1} + b_2\left(\frac{c}{d}\right)^{n-2} + \cdots + b_{n-1}\left(\frac{c}{d}\right) + b_n &= 0\\ d^n(c^n + b_1c^{n-1}d + b_2c^{n-2}d^2 + \cdots + b_nd^{n-1}) &= 0\\ c^n + b_1c^{n-1}d + b_2c^{n-2}d^2 + \cdots + b_nd^{n-1} &= 0.\end{aligned}$$

If we subtract $c^n$ from both sides, and factor out a $d$ from the resulting left-hand-side, we can easily see that $d \mid c^n$. However, since we were originally given the condition that $\gcd(c, d) = 1$, the only possibility for both to be valid is if $d = \pm 1$. Since $d = \pm 1$, $r$ thus must be a rational integer. It is the root of (1), so it is also an algebraic integer, and we are done. ∎

This theorem may also be known as the Rational Root Theorem, and it has applications in the solving of single-variable polynomial equations. The method described in the proof can be used to calculate the roots of any polynomial equation.

1.3. $\mathbb{Q}$ **modules and** $\mathbb{Z}$ **modules.** Although the $\mathbb{Q}$ module and $\mathbb{Z}$ module are examples of algebraic number fields, they are not the only examples of such.

**Definition 1.15** ($\mathbb{Q}$ module)**.** We define some subset $V \subset \mathbb{C}$ of the complex number field to be a $\mathbb{Q}$ module if its satisfies three conditions:

(1) For any $\gamma_1, \gamma_2 \in V$, is is true that $\gamma_1 + \gamma_2 \in V$ and $\gamma_1 - \gamma_2 \in V$. In other words, $V$ is closed under $+$.
(2) For some $\gamma \in V$ and $r \in \mathbb{Q}$, it is true that $r\gamma \in V$. In other words, $V$ has a scalar multiplication over $\mathbb{Q}$.
(3) There exist $\gamma_1, \gamma_2, \ldots, \gamma_n \in V$ such that every $\gamma \in V$ may be written as a linear combination of each $\gamma_1, \gamma_2, \ldots, \gamma_n$, or

$$\gamma = \sum_{i=1}^{n} r_i \gamma_i \text{ where } r_i \in \mathbb{Q}.$$

The first property asserts closure, the second illustrates a scalar multiplication, and the third asserts that there exists a finite list of vectors in $V$ such that their span equates to $V$. Thus it is not difficult to see that $V$ forms a finite-dimensional vector space over $\mathbb{Q}$.

**Definition 1.16** ($\mathbb{Z}$ module)**.** We define some subset $W \subset \mathbb{C}$ of the complex number field to be a $\mathbb{Z}$ module if it satisfies two conditions:

(1) For any $\omega_1, \omega_2 \in W$, it is true that $\omega_1 \pm \omega_2 \in W$.
(2) There exist $\omega_1, \omega_2, \ldots, \omega_m \in W$ such that every $\omega \in W$ may be written in the form

$$\omega = \sum_{i=1}^{m} q_i \omega_i \text{ where } q_i \in \mathbb{Z}.$$

Notice that unlike the $\mathbb{Q}$ module, $\mathbb{Z}$ does not form a finite-dimensional vector space over $\mathbb{Z}$ as it does not have a scalar multiplication. Also, a $\mathbb{Z}$ module does not need to contain a basis as it is not possible to produce a linearly independent list of vectors. However, we can see that it forms a finitely-generated abelian group.

**Definition 1.17** (Finitely-Generated Group)**.** We say that a group $G$ is **finitely-generated** if there exists a finite set $W \subset G$ such that every element of $G$ may be written as a linear combination of the finite set $W$.

Furthermore, a $\mathbb{Z}$ module is abelian because by definition, it is a subset of the complex field $\mathbb{C}$, which itself maintains commutativity and closure under $+$ and $\times$.

In general, modules are a generalization of a vector space, where the field of scalars seen in a vector space is confined by a ring rather than a field.

## 2. Sets of Algebraic Numbers and Algebraic Integers

Now that we are equipped with the necessary devices with which to communicate the following results, we can begin.

2.1. **The algebraic numbers form a field.** We will first prove a lemma that will assist in the proof of our theorem.

**Lemma 2.1.** *Suppose that $V \subset \mathbb{C}$ is a $\mathbb{Q}$ module. We will denote this $\mathbb{Q}$ module as $[\gamma_1, \gamma_2, \ldots, \gamma_n]$, where $\gamma_1, \gamma_2, \ldots, \gamma_n \in V$ forms a basis of $V$. Next, suppose that $\alpha \in \mathbb{C}$. If*

$$\alpha V \subset V,$$

*then $\alpha$ is an algebraic number, or $\alpha \in \bar{\mathbb{Q}}$.*

*Proof.* Let us take the basis $(\gamma_1, \gamma_2, \ldots, \gamma_n)$. Suppose that

$$\alpha\gamma_i = \sum_{j=1}^{n} a_{ij}\gamma_j \text{ where } a_{ij} \in \mathbb{Q}.$$

We can rewrite this as a system of equations of square matrix elements as follows:

$$\begin{aligned}
\alpha\gamma_1 &= a_{11}\gamma_1 + a_{12}\gamma_2 + \cdots + a_{1n}\gamma_n \\
\alpha\gamma_1 &= a_{21}\gamma_1 + a_{22}\gamma_2 + \cdots + a_{2n}\gamma_n \\
\alpha\gamma_1 &= a_{31}\gamma_1 + a_{32}\gamma_2 + \cdots + a_{3n}\gamma_n \\
&\vdots \\
\alpha\gamma_1 &= a_{n1}\gamma_1 + a_{n2}\gamma_2 + \cdots + a_{nn}\gamma_n.
\end{aligned}$$

We may rewrite this as a determinant

$$\det(\alpha I - A) = 0$$

where

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \cdots & a_{nn} \end{bmatrix}$$

and

$$I = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}.$$

Since the determinant is the characteristic polynomial of $A$, it is an $n$th degree polynomial equation. Thus it is clear that $\alpha$ is an algebraic number, and we are done. ∎

With this proven, we can assert that scalar multiples of $\alpha \in \mathbb{C}$ and any element of $V$ remains within $V$, and this will be incredibly useful for the final proof.

**Theorem 2.2.** *$\bar{\mathbb{Q}}$ is a field.*

*Proof.* Before we may proceed, let us recall the conditions of a field: there is closure under $+$ and $\times$, and the existence of an additive inverse and multiplicative inverse (the uniqueness of inverses is trivial). Thus we must prove that for algebraic numbers $\alpha_1, \alpha_2 \in \bar{\mathbb{Q}}$, it is true that

(1) for every $\alpha_1 \in \bar{\mathbb{Q}}$ there exists $\alpha_2 \in \bar{\mathbb{Q}}$ such that $\alpha_1 + \alpha_2 = 0$, which is also the additive identity in the field,
(2) for every $\alpha_1 \in \bar{\mathbb{Q}}$ there exists $\alpha_2 \in \bar{\mathbb{Q}}$ such that $\alpha_1\alpha_2 = 1$, which is also the multiplicative identity in the field,
(3) $\alpha_1 \pm \alpha_2 \in \bar{\mathbb{Q}}$,
(4) $\alpha_1\alpha_2 \in \bar{\mathbb{Q}}$.

The statements of (1) and (2) are relatively easy to see. To prove (1), let $\alpha$ satisfy $f(x) = 0$. Then it is true that $-\alpha$ satisfies $f(-x) = 0$, so we have an additive inverse. To prove (2), suppose that we have the polynomial

$$a_0\alpha^n + a_1\alpha^{n-1} + a_2\alpha^{n-2} + \cdots + a_n = 0,$$

where $a_i \in \mathbb{Q}$. Multiply the left-hand-side and right-hand-side of this polynomial by $\alpha^{-n}$ to obtain

$$\begin{aligned}
(\alpha^{-n})a_0\alpha^n + a_1\alpha^{n-1} + a_2\alpha^{n-2} + \cdots + a_{n-1}\alpha^{n-(n-1)} + a_n &= 0(\alpha^{-n}) \\
a_n\alpha^{-n} + a_{n-1}\alpha^{-n+((n-(n-1))} + a_{n-2}\alpha^{-n+((n-(n-2))} + \cdots + a_0 &= 0 \\
a_n\alpha^{-n} + a_{n-1}\alpha^{-(n-1)} + a_{n-2}\alpha^{-(n-2)} + \cdots + a_0 &= 0 \\
a_n\left(\frac{1}{\alpha}\right)^n + a_{n-1}\left(\frac{1}{\alpha}\right)^{n-1} + a_{n-2}\left(\frac{1}{\alpha}\right)^{n-2} + \cdots + a_0\left(\frac{1}{\alpha}\right)^0 &= 0.
\end{aligned}$$

Since $1/\alpha$ is a root of this polynomial, it is thus an algebraic number.

To prove (3) and (4), consider two polynomial equations

$$\alpha_1^n + r_1\alpha_1^{n-1} + r_2\alpha_1^{n-2} + r_n = 0$$

and

$$\alpha_2^n + s_1\alpha_2^{n-1} + s_2\alpha_2^{n-2} + s_m = 0,$$

where $r_i, s_i \in \mathbb{Q}$. We allow $V$ to be the $\mathbb{Q}$ module formed by considering all $mn$ linear combinations of the elements $\alpha_1^i\alpha_2^j$, where $0 \leq i \leq n$ and $0 \leq j \leq m$, which span $V$. Since $\alpha_1$ and $\alpha_2$ are defined by the two polynomials to be algebraic numbers, it must be true that, for some $\gamma \in V$,

$$\alpha_1\gamma \subset V \text{ and } \alpha_2\gamma \subset V,$$

by Lemma **2.1**. In the context of Lemma **2.1**, this is equivalent to stating that $\alpha_1 V \subset V$ and $\alpha_2 V \subset V$. Thus we may write

$$(\alpha_1 + \alpha_2)V \subset V \text{ and } (\alpha_1\alpha_2)V \subset V,$$

thus proving that $\alpha_1 + \alpha_2, \alpha_1\alpha_2 \in \bar{\mathbb{Z}}$, hence proving that $\bar{\mathbb{Z}}$ is a ring. Thus we are done. ∎

2.2. **The algebraic integers form a ring.** Much like the proof that $\bar{\mathbb{Q}}$ forms a field, the proof that $\bar{\mathbb{Z}}$ forms a ring involves proving a complementary lemma, and then proving the final result. We will omit the absolute details, but it is important to recall that a $\mathbb{Z}$ module forms a finitely-generated abelian group.

However, in order to further understand the relationship between the field of algebraic numbers and ring of algebraic integers, we must further understand how certain structures operate. Previously, when proving Theorem **2.2**, we showed that the set of algebraic numbers is a field if it has an additive and multiplicative inverse, which were denoted as 0 and 1 respectively. However, in the context of rings, it is not necessary to have those two types of inverses for each element. Furthermore, it is not necessary for a ring to be commutative. However, a commutative ring is a field if and only if every nonzero element in the ring has a multiplicative inverse, and we call this ring a **monoid**. We will not use monoids in our final proof, but it is important to notice that although fields and rings are definitively different, they still exist under two binary operations, and are equivalent in special cases. We may interpret a ring with two binary operations as a group under addition that satisfies some multiplicative axioms, and a field as a group under both addition and multiplication. As an example of the variability of a ring, we say that a ring that does not possess an identity element is an "rng".

The proof of Theorem **2.2** and Theorem **2.4** are vastly similar, as we focus on proving closure under $+$ and $\times$.

Furthermore, note that if we are able to prove this theorem, then it is evident that

$$\mathbb{Z} \subset \bar{\mathbb{Z}} \subset \bar{\mathbb{Q}}.$$

Now we can prove the aforementioned complementary lemma.

**Lemma 2.3.** *Suppose that some $W \subset \mathbb{C}$ is a $\mathbb{Z}$ module. We allow the finite set $\{\omega_1, \omega_2, \ldots, \omega_n\}$ to generate the group $W$, where $\omega_1, \omega_2, \ldots, \omega_n \in W$. Next, suppose that $\beta \in \mathbb{C}$. If*

$$\beta W \subset W,$$

*then $\beta$ is an algebraic integer, or $\beta \in \bar{\mathbb{Z}}$.*

*Proof.* Let $\{\omega_1, \omega_2, \ldots, \omega_n\}$ generate $W$. Suppose that

$$\beta\omega_i = \sum_{j=1}^{n} a_{ij}\omega_j \text{ where } a_{ij} \in \mathbb{Z}.$$

Similarly, we write this as a system of equations of square matrix elements:

$$\begin{aligned}
\beta\omega_1 &= a_{11}\omega_1 + a_{12}\omega_2 + \cdots + a_{1n}\omega_n \\
\beta\omega_1 &= a_{21}\omega_1 + a_{22}\omega_2 + \cdots + a_{2n}\omega_n \\
\beta\omega_1 &= a_{31}\omega_1 + a_{32}\omega_2 + \cdots + a_{3n}\omega_n \\
&\vdots \\
\beta\omega_1 &= a_{n1}\omega_1 + a_{n2}\omega_2 + \cdots + a_{nn}\omega_n.
\end{aligned}$$

Again, we write this as a determinant

$$\det(\beta I - B)$$

where

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \cdots & a_{nn} \end{bmatrix}$$

and

$$I = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}.$$

The characteristic polynomial of $B$ produces an $n$th degree monic polynomial equation, so $\beta$ is an algebraic integer, and we are done. ■

**Theorem 2.4.** *$\bar{\mathbb{Z}}$ is a ring.*

*Proof.* The proof is analogous to the proof that the set of algebraic numbers forms a field. We need only prove that $\beta_1 + \beta_2$ and $\beta_1\beta_2$ are in $\bar{\mathbb{Z}}$ for $\beta_1, \beta_2 \in \bar{\mathbb{Z}}$.

To do so, consider two monic polynomial equations

$$\beta_1^n + t_1\beta_1^{n-1} + t_2\beta_1^{n-2} + \cdots + t_n = 0$$

and

$$\beta_2^n + u_1\beta_2^{n-1} + u_2\beta_2^{n-2} + \cdots + u_n = 0,$$

where $t_i, u_i \in \mathbb{Z}$. We let $W$ be the $\mathbb{Z}$ module formed by considering all $kl$ linear combinations of the finite set of elements $\beta_1^i\beta_2^j$, where $0 \le i \le k$ and $0 \le j \le l$, which finitely generate $W$. Since the two polynomials above provide the conditions for $\beta_1$ and $\beta_2$ to be algebraic, it is true that, for some $\omega \in W$,

$$\beta_1\omega \subset W \text{ and } \beta_2\omega \subset W,$$

by Lemma **2.3**. In the context of Lemma **2.3**, this is equivalent to stating that $\beta_1 W \subset W$ and $\beta_2 W \subset W$. Thus we may write

$$(\beta_1 + \beta_2)W \subset W \text{ and } (\beta_1\beta_2)W \subset W,$$

thus proving that $\beta_1 + \beta_2, \beta_1\beta_2 \in \bar{\mathbb{Q}}$ by Lemma **2.3**, hence proving that $\bar{\mathbb{Z}}$ is a ring. Thus we are done. ■

## 3. Additional Results

We will conclude this paper with several interesting properties of algebraic numbers. So as to not confuse sets of algebraic numbers and algebraic integers with their field and ring counterparts, we will denote the field of algebraic numbers as $\Gamma$ and the ring of algebraic integers as $\Omega$.

However, before we proceed, we must reconsider two properties of a ring $k[x]$, elements of which are polynomials with coefficients from some field $F$. As in the ring of $\mathbb{Z}$, there is an analog for $k[x]$; namely the gcd and linear combination. However, in order to convey our results, we must use ring-theoretic language. Thus, for some $f_1, f_2, \ldots, f_n \in k[x]$, we denote $(f_1, f_2, \ldots, f_n)$ to be the **ideal** generated by $f_1, f_2, \ldots, f_n$, written as

$$f_1h_1 + f_2h_2 + \cdots + f_nh_n,$$

where $h_1, h_2, \ldots, h_n \in k[x]$. We may now proceed.

**Lemma 3.1.** *Let two polynomials $f(x), g(x) \in k[x]$. Then there exists some polynomial $d(x) \in k[x]$ such that $(f(x), g(x)) = (d(x))$. In other words, there exist two polynomials $f(x), g(x) \in k[x]$ such that the ideal generated by $f(x)$ and $g(x)$ is equivalent to the ideal generated by another polynomial $d(x) \in k[x]$.*

*Proof.* In the set $(f(x), g(x))$, let $d(x)$ be the element of least degree. Clearly, we have that $(d(x)) \subseteq (f(x), g(x))$. Thus, in order to prove the equivalence of these two ideals, we must show the reverse inclusion.

To do this, consider some $c(x) \in (f(x), g(x))$. If we assume $d(x) \nmid c(x)$, then by the division algorithm in $k[x]$, there exist polynomials $q(x), r(x)$ such that $c(x) = q(x)d(x) + r(x)$, where $\deg r(x) < \deg d(x)$. Since $c(x), d(x) \in (f(x), g(x))$, we may rewrite

$$r(x) = c(x) - q(x)d(x).$$

Now it is clear that $r(x) \subseteq (f(x), g(x))$. However, we originally assumed $d(x)$ to be the polynomial of least degree in the ideal $(f(x), g(x))$, yet the fact that $r(x)$ is in the same ideal and is of lesser degree suggests otherwise. Thus we have reached a contradiction, and $d(x) \mid c(x)$, so that $c \in (d(x))$, proving that $(f(x), g(x)) \subseteq (d(x))$. Thus we are done. ■

We say that this polynomial $d(x)$ of least degree is the **greatest common divisor** of $f(x)$ and $g(x)$ if $d(x)$ divides both $f(x)$ and $g(x)$ and every common divisor of

$f(x)$ and $g(x)$ divides $d(x)$. Again, referring to the analogue, if $d(x) = 1$, then $f(x)$ and $g(x)$ are relatively prime. We prove the following lemma.

**Lemma 3.2.** *Let $f(x), g(x) \in k[x]$. Then there is a $d(x) \in k[x]$ such that $(f(x), g(x)) = (d(x))$, where $d(x)$ is a greatest common divisor of $f(x)$ and $g(x)$.*

*Proof.* By Lemma **3**, it is clearly true that $f(x), g(x) \in (d(x))$, so $d(x) \mid f(x)$ and $d(x) \mid g(x)$. Let there exist some $h(x) \in k[x]$. Suppose that $h(x) \mid f(x)$ and $h(x) \mid g(x)$. Then $h(x)$ divides every polynomial of the form $f(x)l(x) + g(x)m(x)$ for $l(x), m(x) \in k[x]$. This implies that $h(x) \mid d(x)$, so $d(x)$ is clearly the greatest common divisor of $f(x)$ and $g(x)$, so we are done. ■

Now that we are equipped with these preliminary results, we may proceed.

Consider some $\alpha \in \Gamma$. Let $\mathbb{Q}[x]$ denote the ring of polynomials with rational coefficients. If we consider some nonzero polynomial $f(x) \in \mathbb{Q}[x]$ of smallest degree for which $\alpha$ is a root, then $f(x)$ must be irreducible. We will now prove a lemma that will further extend this and prove another property regarding divisibility of polynomials in $\mathbb{Q}[x]$.

**Lemma 3.3.** *If $\alpha \in \Gamma$, then $\alpha$ is the root of a unique monic irreducible polynomial $f(x) \in \mathbb{Q}[x]$. Furthermore, if there exists some other $g(x) \in \mathbb{Q}[x]$ with $\alpha$ as a root, then $f(x) \mid g(x)$.*

*Proof.* If $\alpha$ is a root of $f(x)$, then we can allow $f(x)$ to be any monic irreducible with the property that $f(\alpha) = 0$. We must prove uniqueness. However, we will first prove the second statement. We let $g(x)$ be a polynomial with the property that $g(\alpha) = 0$.

Assume that $f(x) \nmid g(x)$. Then $(f(x), g(x)) = 1$ by the statement following Lemma **3**. By the proof of Lemma **3.2**, we may write this as a linear combination of $f(x)$ and $g(x)$:

$$f(x)h(x) + g(x)t(x) = 1$$

for $h(x), t(x) \in \mathbb{Q}[x]$. If $\alpha$ is a root, then

$$\begin{aligned} f(\alpha)h(\alpha) + g(\alpha)t(\alpha) &= 1 \\ 0(h(\alpha)) + 0(t(\alpha)) &= 1 \\ 0 + 0 = 0 &\neq 1, \end{aligned}$$

which is a contradiction. Thus it must be true that $f(x) \mid g(x)$. Thus it is clear that $f(x)$ is unique. ■

We define this unique monic irreducible polynomial mentioned above to be the **minimal polynomial** of $\alpha$. If we allow this particular polynomial to be $f(x)$ and set $\deg f(x) = n$, then we say that $\alpha$ is the **algebraic number of degree** $n$. If $f(x)$ is irreducible and $\deg f(x) = n$, then $f(x)$ is the minimal polynomial for each of its $n$ roots by the Fundamental Theorem of Algebra.

We these results now equipped, we are prepared to prove the final result. If $\mathbb{Q}[\alpha]$ is the ring of polynomials over the field $\mathbb{Q}$ i.e. with rational coefficients, then

we define $\mathbb{Q}(\alpha)$ to be the field of complex numbers of the form $g(\alpha)/h(\alpha)$, where $g(x), h(x) \in \mathbb{Q}[x]$ are polynomials. The theorem we are about to prove is that if $\alpha$ is an algebraic integer, then $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$.

**Theorem 3.4.** *If $\alpha \in \Omega$, then $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$.*

*Proof.* Before we begin, notice that $\mathbb{Q}[\alpha] \subset \mathbb{Q}(\alpha)$. This is because the the integer 1 is a function, and we may write it as $h(x) = 1$, which is a polynomial of $\deg h(x) = 0$. Thus every element in $\mathbb{Q}[\alpha]$ exists in $\mathbb{Q}(\alpha)$.

Recall that $h(\alpha) \in \mathbb{Q}[\alpha]$. Assume that $h(\alpha) \neq 0$ (which guarantees that no polynomial in $\mathbb{Q}(\alpha)$ is indeterminate). By the negation of Lemma **3.3**, there exists some monic irreducible minimal polynomial $f(x) \in \mathbb{Q}[x]$ such that $f(x) \nmid h(x)$. It is true that $f(x)$ is the minimal polynomial of $\alpha$, as it is the polynomial of least degree in $\mathbb{Q}[x]$ such that $f(\alpha) = 0$ for $\alpha \in \Omega$.

Thus it is true that $f(x)$ and $g(x)$ are analogously relatively prime, so by the proof of Lemma **3.2**, we may write

$$f(x)s(x) + h(x)t(x) = 1$$

for $s(x), t(x) \in \mathbb{Q}[x]$. Let $x = \alpha \in \Omega$. Then since $f(\alpha) = 0$ but $h(\alpha) \neq 0$, we have

$$\begin{aligned} f(\alpha)s(\alpha) + h(\alpha)t(\alpha) &= 1 \\ 0(s(\alpha)) + h(\alpha)t(\alpha) &= 1 \\ h(\alpha)t(\alpha) &= 1. \end{aligned}$$

Thus we know that $t(\alpha) = 1/h(\alpha)$. Since we can assert that $t(\alpha) \in \mathbb{Q}[\alpha]$, it is thus true that $1/h(\alpha) \in \mathbb{Q}[\alpha]$. Let $\gamma \in \mathbb{Q}(\alpha)$. Then we may express it as a complex number

$$\gamma = \frac{g(\alpha)}{h(\alpha)} = g(\alpha)h(\alpha)^{-1}$$

for $g(x), h(x) \in \mathbb{Q}[x]$. Thus, by the above statement, it is clear that $\gamma \in \mathbb{Q}[\alpha]$. We may thus assert that $\mathbb{Q}(\alpha) \subset \mathbb{Q}[\alpha]$. By double inclusion, it follows that $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$, and we are done. ∎

## References

[Axl15] Sheldon Axler. *Linear Algebra Done Right*. Springer Cham, 2015.

[IRR90] Kenneth Ireland, Michael Ira Rosen, and Michael Rosen. *A classical introduction to modern number theory*, volume 84. Springer Science & Business Media, 1990.