Algebraic Number Theory

Dr. Anuj Jakhar

Indian Institute of Technology Bhilai

anujjakhar@iitbhilai.ac.in

August 2021

Motivation

- The origin of Algebraic Number theory is attributed to Fermat's Last Theorem which was conjectured by a French mathematician Pierre de Fermat in 1637.

Motivation

- The origin of Algebraic Number theory is attributed to Fermat's Last Theorem which was conjectured by a French mathematician Pierre de Fermat in 1637.
- It states that the equation $X^n + Y^n = Z^n$ has no solution in non-zero integers x, y, z, when n is an integer greater than 2.

Motivation

- The origin of Algebraic Number theory is attributed to Fermat's Last Theorem which was conjectured by a French mathematician Pierre de Fermat in 1637.
- It states that the equation $X^n + Y^n = Z^n$ has no solution in non-zero integers x, y, z, when n is an integer greater than 2.
- Fermat himself proved the case $n = 4$ of the theorem.
- If $n = pm$, then the relation $x^n + y^n = z^n$ implies that $(x^m)^p + (y^m)^p = (z^m)^p$ which gives a solution of the equation $X^p + Y^p = Z^p$.

Motivation

- The origin of Algebraic Number theory is attributed to Fermat's Last Theorem which was conjectured by a French mathematician Pierre de Fermat in 1637.
- It states that the equation $X^n + Y^n = Z^n$ has no solution in non-zero integers x, y, z, when n is an integer greater than 2.
- Fermat himself proved the case $n = 4$ of the theorem.
- If $n = pm$, then the relation $x^n + y^n = z^n$ implies that $(x^m)^p + (y^m)^p = (z^m)^p$ which gives a solution of the equation $X^p + Y^p = Z^p$.
- Since any integer greater than 2 is either a multiple of 4 or has an odd prime factor, for proving Fermat's Last Theorem it is enough to show that $X^p + Y^p = Z^p$ has no non-zero integer solutions for all odd prime exponents p.

- This celebrated theorem motivated a general study of the theory of algebraic numbers.
- History reveals that in 1770, Leonhard Euler used the field $\mathbb{Q}(\omega)$ with ω a complex cube root of unity to prove Fermat's Last Theorem for the case $n = 3$.

- This celebrated theorem motivated a general study of the theory of algebraic numbers.
- History reveals that in 1770, Leonhard Euler used the field $\mathbb{Q}(\omega)$ with ω a complex cube root of unity to prove Fermat's Last Theorem for the case $n = 3$.

- A complex number α is said to be an algebraic number if α is a root of a non-zero polynomial with coefficients from the field $\mathbb{Q}$ of rational numbers.

- This celebrated theorem motivated a general study of the theory of algebraic numbers.
- History reveals that in 1770, Leonhard Euler used the field $\mathbb{Q}(\omega)$ with ω a complex cube root of unity to prove Fermat's Last Theorem for the case $n = 3$.

- A complex number α is said to be an algebraic number if α is a root of a non-zero polynomial with coefficients from the field $\mathbb{Q}$ of rational numbers.
- A complex number which is not an algebraic number is called a transcendental number.

- This celebrated theorem motivated a general study of the theory of algebraic numbers.
- History reveals that in 1770, Leonhard Euler used the field $\mathbb{Q}(\omega)$ with ω a complex cube root of unity to prove Fermat's Last Theorem for the case $n = 3$.

- A complex number α is said to be an algebraic number if α is a root of a non-zero polynomial with coefficients from the field $\mathbb{Q}$ of rational numbers.
- A complex number which is not an algebraic number is called a transcendental number.
- Note that if α is an algebraic number, then the degree of the extension $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ is finite and vice versa.

Exercise. Prove that $\cos \frac{\pi}{12}$ is an algebraic number.

- The first major step towards a general proof of Fermat's Last Theorem was by a French woman Sophie Germain. In a letter dated May 12, 1819 to the greatest number theorist of that time Carl Friedrich Gauss, she explained her idea of the proof.

- The first major step towards a general proof of Fermat's Last Theorem was by a French woman Sophie Germain. In a letter dated May 12, 1819 to the greatest number theorist of that time Carl Friedrich Gauss, she explained her idea of the proof.

She proved that if p is an odd prime such that $q = 2kp + 1$ is also a prime for some number k satisfying the following conditions:

- $x^p \equiv p \mod q$ has no solution
- the set of pth powers modulo q contains no consecutive non-zero integers,

then the first case of Fermat's Last Theorem holds for the exponent p, i.e., the equation $X^p + Y^p = Z^p$ has no solution in integers x, y, z with p not dividing xyz.

- The first major step towards a general proof of Fermat's Last Theorem was by a French woman Sophie Germain. In a letter dated May 12, 1819 to the greatest number theorist of that time Carl Friedrich Gauss, she explained her idea of the proof.

She proved that if p is an odd prime such that $q = 2kp + 1$ is also a prime for some number k satisfying the following conditions:

- $x^p \equiv p \mod q$ has no solution
- the set of pth powers modulo q contains no consecutive non-zero integers,

then the first case of Fermat's Last Theorem holds for the exponent p, i.e., the equation $X^p + Y^p = Z^p$ has no solution in integers x, y, z with p not dividing xyz.

- In particular, for an odd prime p if $2p + 1$ is also a prime, then the first case of Fermat's Last Theorem holds for the exponent p. In this way she was able to show that the same holds for all odd primes $p \leq 197$.

In 1825, her method claimed its first complete success, when using her results,

- the famous mathematicians Peter Gustav Lejeune Dirichlet and Adrien-Marie Legendre working independently were able to prove the case $n = 5$ of Fermat's Last Theorem.

In 1825, her method claimed its first complete success, when using her results,

- the famous mathematicians Peter Gustav Lejeune Dirichlet and Adrien-Marie Legendre working independently were able to prove the case $n = 5$ of Fermat's Last Theorem.
- the French mathematician Gabriel Lamé proved the case $n = 7$ of the theorem (1839).

In 1825, her method claimed its first complete success, when using her results,

- the famous mathematicians Peter Gustav Lejeune Dirichlet and Adrien-Marie Legendre working independently were able to prove the case $n = 5$ of Fermat's Last Theorem.
- the French mathematician Gabriel Lamé proved the case $n = 7$ of the theorem (1839).

Her results related to Fermat's Last Theorem remained most important until the contribution of Eduard Kummer in 1847.

Ernst Eduard Kummer

- The German mathematician Ernst Eduard Kummer contributed a lot towards the subject.

[1] A prime p is said to be regular if the class number of the field $\mathbb{Q}(e^{2\pi\iota/p})$ is not divisible by p.

Ernst Eduard Kummer

- The German mathematician Ernst Eduard Kummer contributed a lot towards the subject.
- While trying to prove Fermat's Last Theorem, he was studying arithmetic of the ring $\mathbb{Z}[\zeta_p]$ where ζ_p is a primitive pth root of unity, p prime and realized that unique factorization into prime elements may not hold in such rings.

[1] A prime p is said to be regular if the class number of the field $\mathbb{Q}(e^{2\pi\iota/p})$ is not divisible by p.

Ernst Eduard Kummer

- The German mathematician Ernst Eduard Kummer contributed a lot towards the subject.
- While trying to prove Fermat's Last Theorem, he was studying arithmetic of the ring $\mathbb{Z}[\zeta_p]$ where ζ_p is a primitive pth root of unity, p prime and realized that unique factorization into prime elements may not hold in such rings.
- While tackling the above problem, he made a remarkable achievement discovering that the unique factorization property could be salvaged if we replace role of elements of $\mathbb{Z}[\zeta_p]$ by what he called ideal numbers.

- Richard Dedekind extended Kummer's work by using ideals in place of ideal numbers; in fact the concept of an ideal of a ring was thus born in the work of Kummer and Dedekind.

[1] A prime p is said to be regular if the class number of the field $\mathbb{Q}(e^{2\pi\iota/p})$ is not divisible by p.

Ernst Eduard Kummer

- The German mathematician Ernst Eduard Kummer contributed a lot towards the subject.
- While trying to prove Fermat's Last Theorem, he was studying arithmetic of the ring $\mathbb{Z}[\zeta_p]$ where ζ_p is a primitive pth root of unity, p prime and realized that unique factorization into prime elements may not hold in such rings.
- While tackling the above problem, he made a remarkable achievement discovering that the unique factorization property could be salvaged if we replace role of elements of $\mathbb{Z}[\zeta_p]$ by what he called ideal numbers.

- Richard Dedekind extended Kummer's work by using ideals in place of ideal numbers; in fact the concept of an ideal of a ring was thus born in the work of Kummer and Dedekind.
- By using the theory of ideal numbers, Kummer proved Fermat's Last Theorem for a wide range of prime exponents - the so called 'regular' primes[1].

[1] A prime p is said to be regular if the class number of the field $\mathbb{Q}(e^{2\pi\iota/p})$ is not divisible by p.

- In fact, a large part of classical number theory can be expressed in the framework of Algebraic Number Theory.

[2] This prize is named after the Norwegian Mathematician Niels Henrik Abel (1802-1829) and directly modeled after the Nobel Prize. It comes with a monetary award of 7.5 million Norwegian Kroner.

- In fact, a large part of classical number theory can be expressed in the framework of Algebraic Number Theory.
- This theory now has a wealth of applications to several topics in mathematics such as Diophantine equations, cryptography, factorizations into prime ideals, primality testing etc.

[2] This prize is named after the Norwegian Mathematician Niels Henrik Abel (1802-1829) and directly modeled after the Nobel Prize. It comes with a monetary award of 7.5 million Norwegian Kroner.

- In fact, a large part of classical number theory can be expressed in the framework of Algebraic Number Theory.
- This theory now has a wealth of applications to several topics in mathematics such as Diophantine equations, cryptography, factorizations into prime ideals, primality testing etc.
- It is this wider link that led to the final proof of Fermat's Last Theorem.

[2] This prize is named after the Norwegian Mathematician Niels Henrik Abel (1802-1829) and directly modeled after the Nobel Prize. It comes with a monetary award of 7.5 million Norwegian Kroner.

- In fact, a large part of classical number theory can be expressed in the framework of Algebraic Number Theory.
- This theory now has a wealth of applications to several topics in mathematics such as Diophantine equations, cryptography, factorizations into prime ideals, primality testing etc.
- It is this wider link that led to the final proof of Fermat's Last Theorem.

- After seven years of efforts, an English mathematician Andrew John Wiles completed a proof of Fermat's Last Theorem by May 1993.

[2] This prize is named after the Norwegian Mathematician Niels Henrik Abel (1802-1829) and directly modeled after the Nobel Prize. It comes with a monetary award of 7.5 million Norwegian Kroner.

- In fact, a large part of classical number theory can be expressed in the framework of Algebraic Number Theory.
- This theory now has a wealth of applications to several topics in mathematics such as Diophantine equations, cryptography, factorizations into prime ideals, primality testing etc.
- It is this wider link that led to the final proof of Fermat's Last Theorem.

- After seven years of efforts, an English mathematician Andrew John Wiles completed a proof of Fermat's Last Theorem by May 1993.
- He outlined the proof in three lectures in a conference held at Sir Issac Newton Institute in Cambridge in June 1993.

[2] This prize is named after the Norwegian Mathematician Niels Henrik Abel (1802-1829) and directly modeled after the Nobel Prize. It comes with a monetary award of 7.5 million Norwegian Kroner.

- In fact, a large part of classical number theory can be expressed in the framework of Algebraic Number Theory.
- This theory now has a wealth of applications to several topics in mathematics such as Diophantine equations, cryptography, factorizations into prime ideals, primality testing etc.
- It is this wider link that led to the final proof of Fermat's Last Theorem.

- After seven years of efforts, an English mathematician Andrew John Wiles completed a proof of Fermat's Last Theorem by May 1993.
- He outlined the proof in three lectures in a conference held at Sir Issac Newton Institute in Cambridge in June 1993.
- The title of Wiles' lecture series was "Modular forms, Elliptic curves and Galois representations".
- For solving this problem, he was knighted in 2000 and received other awards such as 2016 Abel[2] prize.

[2] This prize is named after the Norwegian Mathematician Niels Henrik Abel (1802-1829) and directly modeled after the Nobel Prize. It comes with a monetary award of 7.5 million Norwegian Kroner.

Theorem 1. The set of all algebraic numbers is a subfield of $\mathbb{C}$, the field of complex numbers.

Theorem 1. The set of all algebraic numbers is a subfield of $\mathbb{C}$, the field of complex numbers.

Proof. Suppose that α, β are algebraic numbers with $\beta \neq 0$.

We have to show that $\alpha \pm \beta$, $\alpha\beta$ and α/β are algebraic numbers.

Theorem 1. The set of all algebraic numbers is a subfield of $\mathbb{C}$, the field of complex numbers.

Proof. Suppose that α, β are algebraic numbers with $\beta \neq 0$.

We have to show that $\alpha \pm \beta$, $\alpha\beta$ and α/β are algebraic numbers.

- The extensions $\mathbb{Q}(\alpha)/\mathbb{Q}$ and $\mathbb{Q}(\beta)/\mathbb{Q}$ are finite, say of degree *m* and *n* respectively.

Theorem 1. The set of all algebraic numbers is a subfield of $\mathbb{C}$, the field of complex numbers.

Proof. Suppose that α, β are algebraic numbers with $\beta \neq 0$.

We have to show that $\alpha \pm \beta$, $\alpha\beta$ and α/β are algebraic numbers.

- The extensions $\mathbb{Q}(\alpha)/\mathbb{Q}$ and $\mathbb{Q}(\beta)/\mathbb{Q}$ are finite, say of degree m and n respectively.
- Since

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] \leq [\mathbb{Q}(\beta) : \mathbb{Q}] = n,$$

it follows from Tower theorem (cf. any field theory book) that

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] \leq mn.$$

Theorem 1. The set of all algebraic numbers is a subfield of $\mathbb{C}$, the field of complex numbers.

Proof. Suppose that α, β are algebraic numbers with $\beta \neq 0$.

We have to show that $\alpha \pm \beta$, $\alpha\beta$ and α/β are algebraic numbers.

- The extensions $\mathbb{Q}(\alpha)/\mathbb{Q}$ and $\mathbb{Q}(\beta)/\mathbb{Q}$ are finite, say of degree m and n respectively.
- Since
$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] \leq [\mathbb{Q}(\beta) : \mathbb{Q}] = n,$$
it follows from Tower theorem (cf. any field theory book) that
$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] \leq mn.$$
- As the elements $\alpha \pm \beta$, $\alpha\beta$ and $\dfrac{\alpha}{\beta}$ belong to $\mathbb{Q}(\alpha, \beta)$, therefore the degree of the extension obtained by adjoining any of these elements to $\mathbb{Q}$ is finite.
- This completes the proof of the theorem.

Theorem 2. The field $\mathbb{A}$ of all algebraic numbers is a countable set.

Theorem 2. The field $\mathbb{A}$ of all algebraic numbers is a countable set.

Proof. We know that a complex number α is an algebraic number if and only if it is a root of a non-zero polynomial with coefficients from $\mathbb{Z}$.

Theorem 2. The field $\mathbb{A}$ of all algebraic numbers is a countable set.

Proof. We know that a complex number α is an algebraic number if and only if it is a root of a non-zero polynomial with coefficients from $\mathbb{Z}$.

- For a non-constant polynomial $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0$ belonging to $\mathbb{Z}[X]$, we define the rank of $f(X)$ by

$$\text{rank}(f) = n + |a_n| + |a_{n-1}| + \cdots + |a_0|.$$

Theorem 2. The field $\mathbb{A}$ of all algebraic numbers is a countable set.

Proof. We know that a complex number α is an algebraic number if and only if it is a root of a non-zero polynomial with coefficients from $\mathbb{Z}$.

- For a non-constant polynomial $f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$ belonging to $\mathbb{Z}[X]$, we define the rank of $f(X)$ by
$$\text{rank}(f) = n + |a_n| + |a_{n-1}| + \cdots + |a_0|.$$
- Note that $\text{rank}(f) \geq 2$.

Theorem 2. The field $\mathbb{A}$ of all algebraic numbers is a countable set.

Proof. We know that a complex number α is an algebraic number if and only if it is a root of a non-zero polynomial with coefficients from $\mathbb{Z}$.

- For a non-constant polynomial $f(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_0$ belonging to $\mathbb{Z}[X]$, we define the rank of $f(X)$ by

$$\text{rank}(f) = n + |a_n| + |a_{n-1}| + \cdots + |a_0|.$$

- Note that $\text{rank}(f) \geq 2$.
- Also observe that for any given positive integer s, the number of polynomials with coefficients from $\mathbb{Z}$ having rank s is finite.

Theorem 2. The field $\mathbb{A}$ of all algebraic numbers is a countable set.

Proof. We know that a complex number α is an algebraic number if and only if it is a root of a non-zero polynomial with coefficients from $\mathbb{Z}$.

- For a non-constant polynomial $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0$ belonging to $\mathbb{Z}[X]$, we define the rank of $f(X)$ by

$$\text{rank}(f) = n + |a_n| + |a_{n-1}| + \cdots + |a_0|.$$

- Note that $\text{rank}(f) \geq 2$.
- Also observe that for any given positive integer s, the number of polynomials with coefficients from $\mathbb{Z}$ having rank s is finite.
- Consequently if P_s denotes the set of all those algebraic numbers which are roots of polynomials with integer coefficients having rank s, then P_s is a finite set.

Theorem 2. The field $\mathbb{A}$ of all algebraic numbers is a countable set.

Proof. We know that a complex number α is an algebraic number if and only if it is a root of a non-zero polynomial with coefficients from $\mathbb{Z}$.

- For a non-constant polynomial $f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$ belonging to $\mathbb{Z}[X]$, we define the rank of $f(X)$ by

$$\text{rank}(f) = n + |a_n| + |a_{n-1}| + \cdots + |a_0|.$$

- Note that $\text{rank}(f) \geq 2$.
- Also observe that for any given positive integer s, the number of polynomials with coefficients from $\mathbb{Z}$ having rank s is finite.
- Consequently if P_s denotes the set of all those algebraic numbers which are roots of polynomials with integer coefficients having rank s, then P_s is a finite set.
- Since $\mathbb{A} = \bigcup_{s=2}^{\infty} P_s$ and countable union of finite sets is countable, it follows that $\mathbb{A}$ is countable.

- Theorem 2 implies that the set of all transcendental numbers is uncountable.

- Theorem 2 implies that the set of all transcendental numbers is uncountable.
- It was Joseph Liouville who first constructed in 1853 a large number of transcendental numbers by proving that real algebraic numbers cannot be too well approximated by rationals.

- Theorem 2 implies that the set of all transcendental numbers is uncountable.
- It was Joseph Liouville who first constructed in 1853 a large number of transcendental numbers by proving that real algebraic numbers cannot be too well approximated by rationals.
- However the question whether some familiar real numbers were transcendental still persisted.
- The first success in this direction was by Charles Hermite.
- In 1873, Hermite proved that e is transcendental.

- Theorem 2 implies that the set of all transcendental numbers is uncountable.
- It was Joseph Liouville who first constructed in 1853 a large number of transcendental numbers by proving that real algebraic numbers cannot be too well approximated by rationals.
- However the question whether some familiar real numbers were transcendental still persisted.
- The first success in this direction was by Charles Hermite.
- In 1873, Hermite proved that e is transcendental.
- In 1882 Ferdinand Lindemann proved the transcendence of π.

- Theorem 2 implies that the set of all transcendental numbers is uncountable.
- It was Joseph Liouville who first constructed in 1853 a large number of transcendental numbers by proving that real algebraic numbers cannot be too well approximated by rationals.
- However the question whether some familiar real numbers were transcendental still persisted.
- The first success in this direction was by Charles Hermite.
- In 1873, Hermite proved that e is transcendental.
- In 1882 Ferdinand Lindemann proved the transcendence of π.
- In fact he proved that for any non-zero algebraic number α, e^{α} is transcendental, which implies that π is transcendental because $e^{\pi\iota} = -1$ is algebraic.

- Theorem 2 implies that the set of all transcendental numbers is uncountable.
- It was Joseph Liouville who first constructed in 1853 a large number of transcendental numbers by proving that real algebraic numbers cannot be too well approximated by rationals.
- However the question whether some familiar real numbers were transcendental still persisted.
- The first success in this direction was by Charles Hermite.
- In 1873, Hermite proved that e is transcendental.
- In 1882 Ferdinand Lindemann proved the transcendence of π.
- In fact he proved that for any non-zero algebraic number α, e^{α} is transcendental, which implies that π is transcendental because $e^{\pi\iota} = -1$ is algebraic.
- In 1934, working independently Alexander Gelfond and Theodor Schnieder proved that if α, β are algebraic numbers (real or complex) with $\alpha \neq 0, 1$ and β irrational, then each value of α^{β} is transcendental.

- A complex number α is said to be an algebraic integer if α is a root of a monic polynomial with integer coefficients.
- To avoid confusion, elements of $\mathbb{Z}$ will sometimes be called rational integers and a prime number will sometimes be referred to as a rational prime.

- A complex number α is said to be an algebraic integer if α is a root of a monic polynomial with integer coefficients.
- To avoid confusion, elements of $\mathbb{Z}$ will sometimes be called rational integers and a prime number will sometimes be referred to as a rational prime.

Example. $\sqrt{2}$ is an algebraic integer but $1/\sqrt{2}$ is not.

- A complex number α is said to be an algebraic integer if α is a root of a monic polynomial with integer coefficients.
- To avoid confusion, elements of $\mathbb{Z}$ will sometimes be called rational integers and a prime number will sometimes be referred to as a rational prime.

Example. $\sqrt{2}$ is an algebraic integer but $1/\sqrt{2}$ is not.

Theorem 3. A complex number α is an algebraic integer if and only if the minimal polynomial of α over $\mathbb{Q}$ has all its coefficients in $\mathbb{Z}$.

Proof of Theorem 3.

- Suppose that α is an algebraic integer and $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ is a monic polynomial with α as a root.

Proof of Theorem 3.

- Suppose that α is an algebraic integer and $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ is a monic polynomial with α as a root.
- Write $f(x) = f_1(x)f_2(x)\cdots f_r(x)$, where each $f_i(x)$ belonging to $\mathbb{Q}[x]$ is irreducible.

Proof of Theorem 3.

- Suppose that α is an algebraic integer and $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ is a monic polynomial with α as a root.
- Write $f(x) = f_1(x)f_2(x)\cdots f_r(x)$, where each $f_i(x)$ belonging to $\mathbb{Q}[x]$ is irreducible.
- Write

$$f_i(x) = d_i/b_i(g_i(x)), \quad d_i, b_i \in \mathbb{Z}^+, \; g_i(x) \in \mathbb{Z}[x] \text{ primitive.}$$

Proof of Theorem 3.

- Suppose that α is an algebraic integer and $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ is a monic polynomial with α as a root.
- Write $f(x) = f_1(x)f_2(x)\cdots f_r(x)$, where each $f_i(x)$ belonging to $\mathbb{Q}[x]$ is irreducible.
- Write

$$f_i(x) = d_i/b_i(g_i(x)), \quad d_i, b_i \in \mathbb{Z}^+, \ g_i(x) \in \mathbb{Z}[x] \text{ primitive.}$$

- Since

$$b_1 b_2 \cdots b_r f(x) = d_1 d_2 \cdots d_r g_1(x) g_2(x) \cdots g_r(x)$$

and product of primitive polynomials is primitive by Gauss Lemma, on taking contents, the above equation implies that $b_1 b_2 \cdots b_r = d_1 d_2 \cdots d_r$.

Proof of Theorem 3.

- Suppose that α is an algebraic integer and $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ is a monic polynomial with α as a root.
- Write $f(x) = f_1(x)f_2(x)\cdots f_r(x)$, where each $f_i(x)$ belonging to $\mathbb{Q}[x]$ is irreducible.
- Write

$$f_i(x) = d_i/b_i(g_i(x)), \quad d_i, b_i \in \mathbb{Z}^+, \ g_i(x) \in \mathbb{Z}[x] \text{ primitive.}$$

- Since

$$b_1b_2\cdots b_rf(x) = d_1d_2\cdots d_rg_1(x)g_2(x)\cdots g_r(x)$$

  and product of primitive polynomials is primitive by Gauss Lemma, on taking contents, the above equation implies that $b_1b_2\cdots b_r = d_1d_2\cdots d_r$.
- Since $f(x)$ is monic, the equality $f(x) = g_1(x)g_2(x)\cdots g_r(x)$ shows that the leading coefficient of each $g_i(x)$ belongs to $\{+1, -1\}$.

- Recall that α is a root of $f(x)$, so $g_i(\alpha) = 0$ for some i.

- Recall that α is a root of $f(x)$, so $g_i(\alpha) = 0$ for some i.
- But $g_i(x)$ is irreducible over $\mathbb{Q}$ and has coefficients in $\mathbb{Z}$ with leading coefficient ± 1.

- Recall that α is a root of $f(x)$, so $g_i(\alpha) = 0$ for some i.
- But $g_i(x)$ is irreducible over $\mathbb{Q}$ and has coefficients in $\mathbb{Z}$ with leading coefficient ± 1.
- Therefore the minimal polynomial of α over $\mathbb{Q}$ is $\pm g_i(x)$ which proves the desired assertion.
- The converse part is trivial (by definition).

The following theorem gives some more characterizations of an algebraic integer.

The following theorem gives some more characterizations of an algebraic integer.

Theorem 4.

For a complex number α, the following statements are equivalent:

(i) α is an algebraic integer.

The following theorem gives some more characterizations of an algebraic integer.

Theorem 4.

For a complex number α, the following statements are equivalent:

(i) α is an algebraic integer.

(ii) The subring $\mathbb{Z}[\alpha]$ of $\mathbb{C}$ generated by $\mathbb{Z}$ and α is a finitely generated $\mathbb{Z}$-module.

The following theorem gives some more characterizations of an algebraic integer.

Theorem 4.

For a complex number α, the following statements are equivalent:

(i) α is an algebraic integer.

(ii) The subring $\mathbb{Z}[\alpha]$ of $\mathbb{C}$ generated by $\mathbb{Z}$ and α is a finitely generated $\mathbb{Z}$-module.

(iii) There exists a non-zero finitely generated $\mathbb{Z}$-submodule M of $\mathbb{C}$ such that $\alpha M \subseteq M$.

Proof of Theorem 4.

- (i) $\Longrightarrow$ (ii).

Proof of Theorem 4.

- (i) $\Longrightarrow$ (ii).
- Let $g(X) \in \mathbb{Z}[X]$ be a monic polynomial satisfied by α.

Proof of Theorem 4.

- (i) $\implies$ (ii).
- Let $g(X) \in \mathbb{Z}[X]$ be a monic polynomial satisfied by α.
- Let $h(\alpha) \in \mathbb{Z}[\alpha]$ be any element with $h(X)$ belonging to $\mathbb{Z}[X]$.

Proof of Theorem 4.

- (i) $\Longrightarrow$ (ii).
- Let $g(X) \in \mathbb{Z}[X]$ be a monic polynomial satisfied by α.
- Let $h(\alpha) \in \mathbb{Z}[\alpha]$ be any element with $h(X)$ belonging to $\mathbb{Z}[X]$.
- By division algorithm, we can write $h(X) = g(X)q(X) + r(X)$ where $q(X), r(X) \in \mathbb{Z}[X]$ and $\deg r(X) < \deg g(X) = n$ (say).

Proof of Theorem 4.

- (i) $\implies$ (ii).
- Let $g(X) \in \mathbb{Z}[X]$ be a monic polynomial satisfied by α.
- Let $h(\alpha) \in \mathbb{Z}[\alpha]$ be any element with $h(X)$ belonging to $\mathbb{Z}[X]$.
- By division algorithm, we can write $h(X) = g(X)q(X) + r(X)$ where $q(X), r(X) \in \mathbb{Z}[X]$ and $\deg r(X) < \deg g(X) = n$ (say).
- So $h(\alpha) = g(\alpha)q(\alpha) + r(\alpha) = r(\alpha)$, which shows that $h(\alpha)$ is a linear combination of $1, \alpha, \dots, \alpha^{n-1}$ with coefficients from $\mathbb{Z}$.

Proof of Theorem 4.

- (i) $\Longrightarrow$ (ii).
- Let $g(X) \in \mathbb{Z}[X]$ be a monic polynomial satisfied by α.
- Let $h(\alpha) \in \mathbb{Z}[\alpha]$ be any element with $h(X)$ belonging to $\mathbb{Z}[X]$.
- By division algorithm, we can write $h(X) = g(X)q(X) + r(X)$ where $q(X), r(X) \in \mathbb{Z}[X]$ and $\deg r(X) < \deg g(X) = n$ (say).
- So $h(\alpha) = g(\alpha)q(\alpha) + r(\alpha) = r(\alpha)$, which shows that $h(\alpha)$ is a linear combination of $1, \alpha, \ldots, \alpha^{n-1}$ with coefficients from $\mathbb{Z}$.
- Thus $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a system of generators of $\mathbb{Z}[\alpha]$ as $\mathbb{Z}$-module.

Proof of Theorem 4.

- (i) $\implies$ (ii).
- Let $g(X) \in \mathbb{Z}[X]$ be a monic polynomial satisfied by α.
- Let $h(\alpha) \in \mathbb{Z}[\alpha]$ be any element with $h(X)$ belonging to $\mathbb{Z}[X]$.
- By division algorithm, we can write $h(X) = g(X)q(X) + r(X)$ where $q(X), r(X) \in \mathbb{Z}[X]$ and $\deg r(X) < \deg g(X) = n$ (say).
- So $h(\alpha) = g(\alpha)q(\alpha) + r(\alpha) = r(\alpha)$, which shows that $h(\alpha)$ is a linear combination of $1, \alpha, \ldots, \alpha^{n-1}$ with coefficients from $\mathbb{Z}$.
- Thus $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a system of generators of $\mathbb{Z}[\alpha]$ as $\mathbb{Z}$-module.
- (ii) $\implies$ (iii) is trivial.

Proof of Theorem 4, (iii) implies (i).

- Let $\{w_1, \ldots, w_n\}$ be a system of generators of a non-zero finitely generated $\mathbb{Z}$-module $M \subseteq \mathbb{C}$ such that $\alpha M \subseteq M$.

Proof of Theorem 4, (iii) implies (i).

- Let $\{w_1, \ldots, w_n\}$ be a system of generators of a non-zero finitely generated $\mathbb{Z}$-module $M \subseteq \mathbb{C}$ such that $\alpha M \subseteq M$.
- By hypothesis, $\alpha w_i \in M$ for each i. So there exist integers a_{ij} such that

$$\alpha w_i = a_{i1} w_1 + \cdots + a_{in} w_n, \; 1 \leq i \leq n.$$

Proof of Theorem 4, (iii) implies (i).

- Let $\{w_1, \ldots, w_n\}$ be a system of generators of a non-zero finitely generated $\mathbb{Z}$-module $M \subseteq \mathbb{C}$ such that $\alpha M \subseteq M$.
- By hypothesis, $\alpha w_i \in M$ for each i. So there exist integers a_{ij} such that

$$\alpha w_i = a_{i1} w_1 + \cdots + a_{in} w_n, \; 1 \leq i \leq n.$$

- On denoting the $n \times n$ matrix $(a_{ij})_{i,j}$ by A and the identity matrix by I, the above n equations can be rewritten as

$$(\alpha I - A) \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Proof of Theorem 4, (iii) implies (i).

- Let $\{w_1, \ldots, w_n\}$ be a system of generators of a non-zero finitely generated $\mathbb{Z}$-module $M \subseteq \mathbb{C}$ such that $\alpha M \subseteq M$.
- By hypothesis, $\alpha w_i \in M$ for each i. So there exist integers a_{ij} such that

$$\alpha w_i = a_{i1} w_1 + \cdots + a_{in} w_n, \; 1 \leq i \leq n.$$

- On denoting the $n \times n$ matrix $(a_{ij})_{i,j}$ by A and the identity matrix by I, the above n equations can be rewritten as

$$(\alpha I - A) \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

- Multiplying the above equation on the left by the transpose of the cofactor matrix of $(\alpha I - A)$, we obtain

Proof of Theorem 4, (iii) implies (i), Contd....

- $$\det(\alpha I - A) \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}. \tag{1}$$
- Since $\{w_1, w_2, \ldots, w_n\}$ generates M, (1) implies that $\det(\alpha I - A)M = \{0\}$.

Proof of Theorem 4, (iii) implies (i), Contd....

- $$\det(\alpha I - A)\begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}. \quad (1)$$
- Since $\{w_1, w_2, \ldots, w_n\}$ generates M, (1) implies that $\det(\alpha I - A)M = \{0\}$.
- As M is a non-zero submodule of $\mathbb{C}$, we conclude that $\det(\alpha I - A) = 0$ which proves that α satisfies the monic polynomial $\det(XI - A)$ with coefficients from $\mathbb{Z}$.

The following theorem relates the sets of algebraic numbers and algebraic integers.

The following theorem relates the sets of algebraic numbers and algebraic integers.

Theorem 5.

(i) The set of all algebraic integers is a subring of the field of all algebraic numbers.

The following theorem relates the sets of algebraic numbers and algebraic integers.

Theorem 5.

(i) The set of all algebraic integers is a subring of the field of all algebraic numbers.

(ii) If ξ is an algebraic number, then there exists an integer $c \neq 0$ such that $c\xi$ is an algebraic integer.

The following theorem relates the sets of algebraic numbers and algebraic integers.

Theorem 5.

(i) The set of all algebraic integers is a subring of the field of all algebraic numbers.

(ii) If ξ is an algebraic number, then there exists an integer $c \neq 0$ such that $c\xi$ is an algebraic integer.

(iii) The field of algebraic numbers is the quotient field of the ring of algebraic integers.

Proof of Theorem 5 (i).

- Suppose that α and β are algebraic integers which satisfy monic polynomials having degrees m and n over $\mathbb{Z}$.

Proof of Theorem 5 (i).

- Suppose that α and β are algebraic integers which satisfy monic polynomials having degrees m and n over $\mathbb{Z}$.
- We have to prove that $\alpha - \beta, \alpha\beta$ are algebraic integers.

Proof of Theorem 5 (i).

- Suppose that α and β are algebraic integers which satisfy monic polynomials having degrees m and n over $\mathbb{Z}$.
- We have to prove that $\alpha - \beta, \alpha\beta$ are algebraic integers.
- As shown in the proof of the previous theorem, we have

$$\mathbb{Z}[\alpha] = \mathbb{Z} + \mathbb{Z}\alpha + \cdots + \mathbb{Z}\alpha^{m-1}$$

and

$$\mathbb{Z}[\beta] = \mathbb{Z} + \mathbb{Z}\beta + \cdots + \mathbb{Z}\beta^{n-1}.$$

Proof of Theorem 5 (i).

- Suppose that α and β are algebraic integers which satisfy monic polynomials having degrees m and n over $\mathbb{Z}$.
- We have to prove that $\alpha - \beta, \alpha\beta$ are algebraic integers.
- As shown in the proof of the previous theorem, we have

$$\mathbb{Z}[\alpha] = \mathbb{Z} + \mathbb{Z}\alpha + \cdots + \mathbb{Z}\alpha^{m-1}$$

and

$$\mathbb{Z}[\beta] = \mathbb{Z} + \mathbb{Z}\beta + \cdots + \mathbb{Z}\beta^{n-1}.$$

- Therefore

$$\mathbb{Z}[\alpha, \beta] = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \mathbb{Z}\alpha^i \beta^j;$$

so $\mathbb{Z}[\alpha, \beta]$ is a finitely generated $\mathbb{Z}$-module.

Proof of Theorem 5 (i).

- Suppose that α and β are algebraic integers which satisfy monic polynomials having degrees m and n over $\mathbb{Z}$.
- We have to prove that $\alpha - \beta, \alpha\beta$ are algebraic integers.
- As shown in the proof of the previous theorem, we have

$$\mathbb{Z}[\alpha] = \mathbb{Z} + \mathbb{Z}\alpha + \cdots + \mathbb{Z}\alpha^{m-1}$$

and

$$\mathbb{Z}[\beta] = \mathbb{Z} + \mathbb{Z}\beta + \cdots + \mathbb{Z}\beta^{n-1}.$$

- Therefore

$$\mathbb{Z}[\alpha, \beta] = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \mathbb{Z}\alpha^i \beta^j;$$

so $\mathbb{Z}[\alpha, \beta]$ is a finitely generated $\mathbb{Z}$-module.
- Since $(\alpha - \beta)\mathbb{Z}[\alpha, \beta] \subseteq \mathbb{Z}[\alpha, \beta]$, it follows from assertion (iii) of the previous theorem that $\alpha - \beta$ is an algebraic integer.

Proof of Theorem 5 (i).

- Suppose that α and β are algebraic integers which satisfy monic polynomials having degrees m and n over $\mathbb{Z}$.
- We have to prove that $\alpha - \beta, \alpha\beta$ are algebraic integers.
- As shown in the proof of the previous theorem, we have

$$\mathbb{Z}[\alpha] = \mathbb{Z} + \mathbb{Z}\alpha + \cdots + \mathbb{Z}\alpha^{m-1}$$

  and

$$\mathbb{Z}[\beta] = \mathbb{Z} + \mathbb{Z}\beta + \cdots + \mathbb{Z}\beta^{n-1}.$$

- Therefore

$$\mathbb{Z}[\alpha, \beta] = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \mathbb{Z}\alpha^i \beta^j;$$

  so $\mathbb{Z}[\alpha, \beta]$ is a finitely generated $\mathbb{Z}$-module.
- Since $(\alpha - \beta)\mathbb{Z}[\alpha, \beta] \subseteq \mathbb{Z}[\alpha, \beta]$, it follows from assertion (iii) of the previous theorem that $\alpha - \beta$ is an algebraic integer.
- Arguing similarly, we see that $\alpha\beta$ is an algebraic integer.

Proof of Theorem 5 (ii).

- Since ξ is an algebraic number, it satisfies a polynomial $\frac{a_0}{b_0}X^s + \frac{a_1}{b_1}X^{s-1} + \cdots + \frac{a_s}{b_s}$ with a_i, b_i integers, a_0 non-zero.

Proof of Theorem 5 (ii).

- Since ξ is an algebraic number, it satisfies a polynomial $\frac{a_0}{b_0}X^s + \frac{a_1}{b_1}X^{s-1} + \cdots + \frac{a_s}{b_s}$ with a_i, b_i integers, a_0 non-zero.
- Clearing the denominators, we see that

$$c_0\xi^s + c_1\xi^{s-1} + \cdots + c_s = 0 \tag{2}$$

for some c_i's in $\mathbb{Z}$.

Proof of Theorem 5 (ii).

- Since ξ is an algebraic number, it satisfies a polynomial $\frac{a_0}{b_0}X^s + \frac{a_1}{b_1}X^{s-1} + \cdots + \frac{a_s}{b_s}$ with a_i, b_i integers, a_0 non-zero.
- Clearing the denominators, we see that

$$c_0\xi^s + c_1\xi^{s-1} + \cdots + c_s = 0 \tag{2}$$

  for some c_i's in $\mathbb{Z}$.
- Multiplying (1.2) by c_0^{s-1}, we have

$$(c_0\xi)^s + c_1(c_0\xi)^{s-1} + \cdots + c_s c_0^{s-1} = 0,$$

  which shows that $c_0\xi$ satisfies the monic polynomial $X^s + c_1X^{s-1} + \cdots + c_s c_0^{s-1}$ with integral coefficients.
- Hence (ii) is proved.

Assertion (iii) follows from (ii).

Definition (Algebraic Number Field). A subfield K of $\mathbb{C}$ is called an algebraic number field if K is a finite extension of $\mathbb{Q}$.

Definition (Algebraic Number Field). A subfield K of $\mathbb{C}$ is called an algebraic number field if K is a finite extension of $\mathbb{Q}$.

- For an algebraic number field K, we shall denote by $\mathcal{O}_K$ the set consisting of all algebraic integers belonging to K.
- In view of Theorem 5, $\mathcal{O}_K$ is a subring of K having quotient field K.

The following theorem gives an important property of the ring of algebraic integers.

The following theorem gives an important property of the ring of algebraic integers.

Theorem 6.

If a complex number α is a root of a monic polynomial whose coefficients are algebraic integers, then α is an algebraic integer.

The following theorem gives an important property of the ring of algebraic integers.

Theorem 6.

If a complex number α is a root of a monic polynomial whose coefficients are algebraic integers, then α is an algebraic integer.

Proof of Theorem 6. Let α be a root of the polynomial $P(X) = X^m + \alpha_1 X^{m-1} + \cdots + \alpha_m$ of degree m, where each α_i is an algebraic integer.

- Suppose that α_i satisfies a monic polynomial over $\mathbb{Z}$ of degree n_i for $1 \leq i \leq m$.

The following theorem gives an important property of the ring of algebraic integers.

Theorem 6.
If a complex number α is a root of a monic polynomial whose coefficients are algebraic integers, then α is an algebraic integer.

Proof of Theorem 6. Let α be a root of the polynomial $P(X) = X^m + \alpha_1 X^{m-1} + \cdots + \alpha_m$ of degree m, where each α_i is an algebraic integer.

- Suppose that α_i satisfies a monic polynomial over $\mathbb{Z}$ of degree n_i for $1 \leq i \leq m$.
- Then as shown in the proof of Theorem 4, we have

$$\mathbb{Z}[\alpha_i] = \mathbb{Z} + \mathbb{Z}\alpha_i + \cdots + \mathbb{Z}\alpha_i^{n_i-1}, \quad 1 \leq i \leq m.$$

The following theorem gives an important property of the ring of algebraic integers.

Theorem 6.
If a complex number α is a root of a monic polynomial whose coefficients are algebraic integers, then α is an algebraic integer.

Proof of Theorem 6. Let α be a root of the polynomial $P(X) = X^m + \alpha_1 X^{m-1} + \cdots + \alpha_m$ of degree m, where each α_i is an algebraic integer.

- Suppose that α_i satisfies a monic polynomial over $\mathbb{Z}$ of degree n_i for $1 \leq i \leq m$.
- Then as shown in the proof of Theorem 4, we have

$$\mathbb{Z}[\alpha_i] = \mathbb{Z} + \mathbb{Z}\alpha_i + \cdots + \mathbb{Z}\alpha_i^{n_i - 1}, \quad 1 \leq i \leq m.$$

- Therefore

$$\mathbb{Z}[\alpha_1, \alpha_2, \ldots, \alpha_m] = \sum_{j_1=0}^{n_1-1} \sum_{j_2=0}^{n_2-1} \cdots \sum_{j_m=0}^{n_m-1} \mathbb{Z}\alpha_1^{j_1}\alpha_2^{j_2} \cdots \alpha_m^{j_m}. \tag{3}$$

Proof of Theorem 6, Contd.....

- Note that α satisfies the monic polynomial $P(X)$ with coefficients from the ring $\mathbb{Z}[\alpha_1, \alpha_2, \ldots, \alpha_m] = R$ (say).

Proof of Theorem 6, Contd.....

- Note that α satisfies the monic polynomial $P(X)$ with coefficients from the ring $\mathbb{Z}[\alpha_1, \alpha_2, \ldots, \alpha_m] = R$ (say).
- Therefore arguing as in the starting of the proof of Theorem 4, we see that

$$R[\alpha] = R + R\alpha + \cdots + R\alpha^{m-1}.$$

Proof of Theorem 6, Contd.....

- Note that α satisfies the monic polynomial $P(X)$ with coefficients from the ring $\mathbb{Z}[\alpha_1, \alpha_2, \ldots, \alpha_m] = R$ (say).
- Therefore arguing as in the starting of the proof of Theorem 4, we see that

$$R[\alpha] = R + R\alpha + \cdots + R\alpha^{m-1}.$$

- It now follows from (3) and the above equation that

$$R[\alpha] = \sum_{j=0}^{m-1} \sum_{j_1=0}^{n_1-1} \cdots \sum_{j_m=0}^{n_m-1} \mathbb{Z}\alpha_1^{j_1} \cdots \alpha_m^{j_m} \alpha^j.$$

Proof of Theorem 6, Contd.....

- Note that α satisfies the monic polynomial $P(X)$ with coefficients from the ring $\mathbb{Z}[\alpha_1, \alpha_2, \ldots, \alpha_m] = R$ (say).
- Therefore arguing as in the starting of the proof of Theorem 4, we see that

$$R[\alpha] = R + R\alpha + \cdots + R\alpha^{m-1}.$$

- It now follows from (3) and the above equation that

$$R[\alpha] = \sum_{j=0}^{m-1} \sum_{j_1=0}^{n_1-1} \cdots \sum_{j_m=0}^{n_m-1} \mathbb{Z}\alpha_1^{j_1} \cdots \alpha_m^{j_m} \alpha^j.$$

- Thus $R[\alpha]$ is a finitely generated $\mathbb{Z}$-module with $\alpha R[\alpha] \subseteq R[\alpha]$.
- Therefore by Theorem 4(iii), α is an algebraic integer.

The next definition extends the notion of an algebraic integer.

Definition. Let R be an integral domain with quotient field F and let F' be an extension of F. We say that α belonging to F' is integral over R if α satisfies a monic polynomial with coefficients from R.

Arguing as for the proof of Theorems 4, 5, the following theorems can be easily proved.

Theorem 7.

Let α, R, F and F' be as in the above definition. Then the following statements are equivalent:

(i) α is integral over R.

(ii) $R[\alpha]$ is a finitely generated R-module.

(iii) There exists a non-zero finitely generated R-submodule M of F' such that $\alpha M \subseteq M$.

Theorem 8.

Let R be an integral domain with quotient field F and let F' be an extension of F. The following hold:

(i) The set of all elements of F' which are integral over R is a subring of F'.

(ii) If ξ belonging to F' is algebraic over F, then there exists a non-zero element r belonging to R such that $r\xi$ is integral over R.

(iii) If F'/F is an algebraic extension, then the quotient field of R' is F' where R' is the set of those elements of F' which are integral over R. The ring R' is called the integral closure of R in F'.

Definition. An integral domain R is said to be integrally closed if the integral closure of R in its quotient field coincides with R.

The following corollary is an immediate consequence of Theorems 5 and 6.

Corollary 9. For an algebraic number field K, if $\mathcal{O}_K$ denotes the ring of algebraic integers of K, then $\mathcal{O}_K$ is an integrally closed domain with quotient field K.

It may be pointed out that the analogue of Theorem 3 does not hold for an arbitrary integral domain, i.e.,

If R is an integral domain with quotient field F and α is an element of an extension of F such that α integral over R, then the minimal polynomial of α over F may not have coefficients in R.

For example, if $R = \mathbb{Z}[\sqrt{5}]$ and $\alpha = \dfrac{1+\sqrt{5}}{2}$, then α being a root of the polynomial $X^2 - X - 1$ is integral over R, but the minimal polynomial of α over F is $X - \alpha$, which does not belong to $R[X]$.

The following simple lemma shows that the analogue of Theorem 3 holds for integrally closed domains.

Lemma 10. If R is an integrally closed domain with quotient field F and α is an element of an extension of F such that α is integral over R, then the minimal polynomial of α over F has coefficients in R.

Proof. Let $f(X)$ be a monic polynomial belonging to $R[X]$ of which α is a root and $g(X)$ be the minimal polynomial of α over F.

- Since $g(X)$ divides $f(X)$, each root of $g(X)$ is integral over R.
- So the coefficients of $g(X)$, being elementary symmetric functions of the roots of $g(X)$, are also integral over R in view of Theorem 8(i).
- The lemma now follows as $g(X) \in F[X]$ and R is an integrally closed domain.

Norm and Trace

The definitions of norm and trace were first given by Richard Dedekind in his book *Über die Theorie der ganzen algebraischen Zahlen*, published in 1879. Its English translation is now available with the title *Theory of Algebraic Integers*.

Definition. Let K/F be a finite extension of fields, then K is a finite-dimensional vector space over F. For α belonging to K, consider the F-linear transformation T_α of K defined by $T_\alpha(\xi) = \alpha\xi$ for every $\xi \in K$. The characteristic polynomial of this linear transformation is called the characteristic polynomial of α relative to the extension K/F.
Thus if $\{v_1, v_2, \ldots, v_n\}$ is a (vector space) basis of the extension K/F and $\alpha v_i = \sum_{j=1}^{n} a_{ij} v_j$, $a_{ij} \in F$, then the characteristic polynomial of α relative to K/F is determinant of the matrix $(XI - A)$, where $A = (a_{ij})_{i,j}$ and I is the $n \times n$ identity matrix.

With notations as in the above definition,

Note: the characteristic polynomial of α relative to K/F is independent of the choice of the basis $\{v_1, v_2, \ldots, v_n\}$ of K/F.

- If $\{v_1', v_2', \ldots, v_n'\}$ is another basis of K/F, then the matrix $B = (b_{ij})_{i,j}$ of the linear transformation T_α with respect to $\{v_1', v_2', \ldots, v_n'\}$ defined by $\alpha v_i' = \sum\limits_{j=1}^{n} b_{ij} v_j'$ is similar to the matrix A.
- In fact,

$$B = PAP^{-1},$$

where P is the transition matrix from $\{v_1, v_2, \ldots, v_n\}$ to $\{v_1', v_2', \ldots, v_n'\}$, because

$$\begin{bmatrix} \alpha v_1 \\ \alpha v_2 \\ \vdots \\ \alpha v_n \end{bmatrix} = A \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix}, \begin{bmatrix} \alpha v_1' \\ \alpha v_2' \\ \vdots \\ \alpha v_n' \end{bmatrix} = B \begin{bmatrix} v_1' \\ v_2' \\ \vdots \\ v_n' \end{bmatrix}, \begin{bmatrix} v_1' \\ v_2' \\ \vdots \\ v_n' \end{bmatrix} = P \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix}$$

and hence

$$\begin{bmatrix} \alpha v_1' \\ \alpha v_2' \\ \vdots \\ \alpha v_n' \end{bmatrix} = P \begin{bmatrix} \alpha v_1 \\ \alpha v_2 \\ \vdots \\ \alpha v_n \end{bmatrix} = PA \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} = PAP^{-1} \begin{bmatrix} v_1' \\ v_2' \\ \vdots \\ v_n' \end{bmatrix}.$$

which shows that $B = PAP^{-1}$.

The following theorem gives an important property of the ring of algebraic integers.

Definition (Norm and Trace)

Let K/F be a finite extension of fields. For an element α of K, let T_α denote the F-linear transformation of K defined by $T_\alpha(\xi) = \alpha\xi$ for all $\xi \in K$. Let A be the matrix of T_α with respect to a fixed basis $\{v_1, v_2, \ldots, v_n\}$ of K/F.

The norm and trace of α with respect to K/F are defined to be the determinant of A and the trace of A; these will be denoted by $N_{K/F}(\alpha)$, $Tr_{K/F}(\alpha)$ respectively.

In view of above note, these are independent of the choice of a basis of K/F.

Some Simple Properties of Norm and Trace

Let K be an extension of degree n of a field F. Let α, β be in K and $a \in F$. Then the following hold:

(i) $Tr_{K/F}(a) = na$ and $N_{K/F}(a) = a^n$.

(ii) $Tr_{K/F}(\alpha + \beta) = Tr_{K/F}(\alpha) + Tr_{K/F}(\beta)$.

(iii) $N_{K/F}(\alpha\beta) = N_{K/F}(\alpha)N_{K/F}(\beta)$.

For a finite extension K/F, the mapping

$$\alpha \mapsto N_{K/F}(\alpha)$$

is a homomorphism of the multiplicative group $K^\times$ consisting of non-zero elements of the field K into the multiplicative group $F^\times$ and the mapping

$$\alpha \mapsto Tr_{K/F}(\alpha)$$

is an F-linear functional on K.

The following lemma will be used in the proof of the next theorem.

Lemma 11. Let $B_n = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ -c_0 & -c_1 & -c_2 & \cdots & -c_{n-2} & -c_{n-1} \end{pmatrix}$.

Then the characteristic polynomial of the matrix[3] B_n is $f(X) = c_0 + c_1X + \cdots + c_{n-1}X^{n-1} + X^n$.

[3] In Linear Algebra, the transpose of the matrix B_n is called the companion matrix of the polynomial $f(X)$.

Theorem 12. The characteristic polynomial $f_\alpha(X)$ of an element $\alpha \in K$ relative to the extension K/F is a power of the minimal polynomial of α over F.

Proof. Let $\phi_\alpha(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_0$ be the minimal polynomial of α over F. Then $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis of the extension $F(\alpha)/F$.

- Let $\{\theta_1, \theta_2, \ldots, \theta_r\}$ be a basis of $K/F(\alpha)$.
- Fix the basis
$$\{\theta_1, \alpha\theta_1, \ldots, \alpha^{n-1}\theta_1\,;\, \theta_2, \alpha\theta_2, \ldots, \alpha^{n-1}\theta_2\,;\, \ldots\,;\, \theta_r, \alpha\theta_r, \ldots, \alpha^{n-1}\theta_r\}$$
of the extension K/F.
- The matrix of the linear transformation T_α defined by $T_\alpha(\xi) = \alpha\xi$ with respect to this basis will be a block diagonal matrix with r blocks down the main diagonal, each block being equal to

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ -c_0 & -c_1 & -c_2 & \cdots & -c_{n-2} & -c_{n-1} \end{pmatrix}.$$

- So the characteristic polynomial of T_α is the rth power of the characteristic polynomial of A.
- By Lemma 11, the characteristic polynomial of the matrix A is $\phi_\alpha(X)$ and hence $f_\alpha(X) = \phi_\alpha(X)^r$.

The following simple result of field theory will be used in the sequel.

Lemma 13. Let $F(\theta)$ be a separable extension of a field F of degree n and $f(X) = (X - \theta^{(1)}) \cdots (X - \theta^{(n)})$ be the minimal polynomial of θ over F. If $g(X_1, \ldots, X_n)$ is a polynomial with coefficients in F such that $g(\theta^{(1)}, \ldots, \theta^{(n)})$ remains unchanged under all the permutations of $\theta^{(1)}, \ldots, \theta^{(n)}$, then $g(\theta^{(1)}, \ldots, \theta^{(n)}) \in F$.

The theorem stated below describes all roots of a characteristic polynomial.

Theorem 14. Let K/F be a separable extension of degree n and let $\tau_1, \tau_2, \ldots, \tau_n$ be all the F-isomorphisms of K into a normal extension of F containing K. Then the characteristic polynomial of an element $\alpha \in K$ relative to the extension K/F is $(X - \tau_1(\alpha)) \cdots (X - \tau_n(\alpha))$.

The following theorem and its corollary provide another definition of norm and trace.

Theorem 15. Let K/F be an extension of fields and let $\alpha \in K$ have characteristic polynomial $f_\alpha(X)$ relative to the extension K/F. Suppose that $f_\alpha(X)$ factors into linear factors as

$$f_\alpha(X) = (X - \alpha_1) \cdots (X - \alpha_n)$$

over an extension of K. Then

$$N_{K/F}(\alpha) = \alpha_1 \alpha_2 \cdots \alpha_n$$

and

$$Tr_{K/F}(\alpha) = \alpha_1 + \alpha_2 + \cdots + \alpha_n.$$

Proof of Theorem 15. Let A denote the matrix of linear transformation T_α defined on K by $T_\alpha(\xi) = \alpha\xi$ with respect to a fixed basis of K/F. Then

$$f_\alpha(X) = \det\left(XI - A\right) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \quad \text{(say)}.$$

- Substituting $X = 0$ in the above equation, we obtain

$$\det(-A) = a_0;$$

  consequently

$$N_{K/F}(\alpha) = \det A = (-1)^n a_0 = \alpha_1\alpha_2\cdots\alpha_n.$$

- When we expand the determinant of the matrix $(XI - A)$, the coefficient of X^{n-1} is $-\sum_{i=1}^{n} a_{ii}$. So

$$\alpha_1 + \alpha_2 + \cdots + \alpha_n = \sum_{i=1}^{n} a_{ii} = Tr_{K/F}(\alpha).$$

- This proves the theorem.

The corollary stated below follows immediately from the above theorem and Theorem 14.

Corollary 16. If K/F is a separable extension of degree n and $\tau_1, \tau_2, \ldots, \tau_n$ are all the F-isomorphisms of K into a normal extension of F containing K, then for every $\alpha \in K$, we have $Tr_{K/F}(\alpha) = \sum_{i=1}^{n} \tau_i(\alpha)$ and $N_{K/F}(\alpha) = \prod_{i=1}^{n} \tau_i(\alpha)$.

The following theorem is an immediate consequence of Theorem 12 and Theorem 15.

Theorem 16. Let K/F be an extension of degree n and α be an element of K with $[F(\alpha) : F] = d$. Let $\alpha_1, \alpha_2, \dots, \alpha_d$ be the roots of the minimal polynomial of α over F counting multiplicities (if any) in some extension of F. Then

$$Tr_{K/F}(\alpha) = \frac{n}{d}\sum_{i=1}^{d} \alpha_i = \frac{n}{d} Tr_{F(\alpha)/F}(\alpha)$$

and

$$N_{K/F}(\alpha) = \left(\prod_{i=1}^{d} \alpha_i\right)^{n/d} = \left(N_{F(\alpha)/F}(\alpha)\right)^{n/d}.$$

The corollary stated below follows immediately from Theorem 16 and Lemma 10.

Corollary 17. Let R be an integrally closed domain with quotient field F and K be a finite extension of F. If an element α of K is integral over R, then $Tr_{K/F}(\alpha)$ and $N_{K/F}(\alpha)$ belong to R.

The following special case of the above corollary will be used quite often.

Corollary 18. If α is an algebraic integer belonging to an algebraic number field K, then $Tr_{K/F}(\alpha)$ and $N_{K/F}(\alpha)$ belong to $\mathbb{Z}$.

We now prove the following theorem which asserts that norm and trace are transitive.

Theorem 19. Let $F \subseteq K \subseteq L$ be a tower of finite extensions. Then $Tr_{L/F}(\gamma) = Tr_{K/F}(Tr_{L/K}(\gamma))$ and $N_{L/F}(\gamma) = N_{K/F}(N_{L/K}(\gamma))$ for each element $\gamma \in L$.

Proof of Theorem 19. Let $\{w_1, w_2, \ldots, w_n\}$ and $\{\theta_1, \theta_2, \ldots, \theta_m\}$ be bases of the extensions K/F and L/K respectively.

- Let γ be an element of L. Write

$$\gamma\theta_i = \sum_{j=1}^{m} \alpha_{ij}\theta_j, \ \alpha_{ij} \in K, \quad \alpha_{ij} w_r = \sum_{s=1}^{n} a_{ijrs} w_s, \ a_{ijrs} \in F.$$

- By definition

$$\begin{aligned} Tr_{L/K}(\gamma) &= \alpha_{11} + \alpha_{22} + \cdots + \alpha_{mm}, \\ Tr_{K/F}(\alpha_{11}) &= a_{1111} + a_{1122} + \cdots + a_{11nn}, \\ Tr_{K/F}(\alpha_{22}) &= a_{2211} + a_{2222} + \cdots + a_{22nn}, \\ \vdots &= \vdots \qquad \vdots \qquad \vdots \\ Tr_{K/F}(\alpha_{mm}) &= a_{mm11} + a_{mm22} + \cdots + a_{mmnn}. \end{aligned}$$

- We compute the matrix of the F-linear transformation $T_\gamma : L \to L$ defined by $T_\gamma(\xi) = \gamma\xi$ with respect to the basis

$$\mathcal{B} := \{\theta_1 w_1, \ldots, \theta_1 w_n \; ; \; \theta_2 w_1, \ldots, \theta_2 w_n \; ; \; \ldots \; ; \; \theta_m w_1, \ldots, \theta_m w_n\}$$

of the extension L/F.

- Write the equation

$$T_\gamma(\theta_1 w_1) = \gamma\theta_1 w_1 = (\alpha_{11}\theta_1 + \alpha_{12}\theta_2 + \cdots + \alpha_{1m}\theta_m)w_1$$

as

$$T_\gamma(\theta_1 w_1) = \sum_{i=1}^{n} a_{111i}\theta_1 w_i + \sum_{j=1}^{n} a_{121j}\theta_2 w_j + \cdots + \sum_{r=1}^{n} a_{1m1r}\theta_m w_r.$$

- Similarly write

$$T_\gamma(\theta_1 w_2) = \gamma\theta_1 w_2 = (\alpha_{11}\theta_1 + \alpha_{12}\theta_2 + \cdots + \alpha_{1m}\theta_m)w_2 \quad as$$

$$T_\gamma(\theta_1 w_2) = \sum_{i=1}^{n} a_{112i}\theta_1 w_i + \sum_{j=1}^{n} a_{122j}\theta_2 w_j + \cdots + \sum_{r=1}^{n} a_{1m2r}\theta_m w_r.$$

- Continuing in this way, it can be seen that the matrix of T_γ with respect to the basis $\mathcal{B}$ is an $mn \times mn$ matrix given by

$$\begin{bmatrix} A_{11} & A_{12} & \cdots & A_{1m} \\ A_{21} & A_{22} & \cdots & A_{2m} \\ \vdots & \vdots & \vdots & \vdots \\ A_{m1} & A_{m2} & \cdots & A_{mm} \end{bmatrix},$$

where each A_{ij} is an $n \times n$ matrix with (r, s)th entry a_{ijrs}. So

$$Tr_{L/F}(\gamma) = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{iijj} = \sum_{i=1}^{m} Tr_{K/F}(\alpha_{ii}) =$$

$$Tr_{K/F}(\sum_{i=1}^{m} \alpha_{ii}) = Tr_{K/F}(Tr_{L/K}(\gamma))$$

and hence the first assertion of the theorem is proved.

Second assertion. We now prove that

$$N_{L/F}(\gamma) = N_{K/F}(N_{L/K}(\gamma)). \tag{4}$$

- Keeping in mind Theorem 15, it can be quickly seen that the left hand side of (4) equals $[N_{K(\gamma)/F}(\gamma)]^{[L:K(\gamma)]}$ and its right hand side equals $[N_{K/F}(N_{K(\gamma)/K}(\gamma))]^{[L:K(\gamma)]}$.
- So it is enough to prove (4) when $L = K(\gamma)$.
- Let $\{w_1, \ldots, w_n\}$ be a basis of K/F and m denote the degree of $K(\gamma)/F$.
- Consider the basis

$$\mathcal{B}' := \{w_1, \ldots, w_n \; ; \; \gamma w_1, \ldots, \gamma w_n \; ; \; \ldots \; ; \; \gamma^{m-1} w_1, \ldots, \gamma^{m-1} w_n\}$$

  of $K(\gamma)/F$.
- Let $X^m + \alpha_1 X^{m-1} + \cdots + \alpha_m$ denote the minimal polynomial of γ over K. Then by Theorem 15, $N_{K(\gamma)/K}(\gamma) = (-1)^m \alpha_m$.
- Let A_i denote the matrix of the F-linear transformation $T_{\alpha_i} : K \to K$ (which is multiplication by α_i) with respect to the basis $\{w_1, w_2, \ldots, w_n\}$.

- Then it can be easily verified that the $mn \times mn$ matrix M of the F-linear transformation $T_\gamma : K(\gamma) \to K(\gamma)$ defined by $T_\gamma(\xi) = \gamma\xi$ with respect to the basis $\mathcal{B}'$ is given by

$$M = \begin{bmatrix} O_{n\times n} & I_{n\times n} & O_{n\times n} & \cdots & O_{n\times n} \\ O_{n\times n} & O_{n\times n} & I_{n\times n} & \cdots & O_{n\times n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ -A_m & -A_{m-1} & -A_{m-2} & \cdots & -A_1 \end{bmatrix}.$$

- In order to evaluate determinant of M, interchange the first block of n columns of the matrix M with the second block of n columns; in the new matrix interchange second block of n columns with the third block of n columns.

- Repeating the process $m-1$ times, we see that

$$N_{K(\gamma)/F}(\gamma) = \det M = (-1)^{n(m-1)} \det \begin{bmatrix} I_{n\times n} & O_{n\times n} & O_{n\times n} & \cdots \\ O_{n\times n} & I_{n\times n} & O_{n\times n} & \cdots \\ \vdots & \vdots & \vdots & \vdots \\ -A_{m-1} & -A_{m-2} & -A_{m-3} & \cdots \end{bmatrix}$$

$$= (-1)^{n(m-1)} \det(-A_m) = (-1)^{nm} \det(A_m) = (-1)^{nm} N_{K/F}($$
$$= N_{K/F}((-1)^m \alpha_m) = N_{K/F}(N_{K(\gamma)/K}(\gamma)).$$

- This proves the second assertion of the theorem.

Exercises.

- Prove by induction on n that the determinant of the Vandermonde matrix
$$\begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{bmatrix}$$
equals $\prod_{1 \leq j < i \leq n} (\alpha_i - \alpha_j)$.
- If a complex number α is not an algebraic integer, then show that α^ϵ with ϵ a positive rational number can not be an algebraic integer.
- Prove that $\cos \frac{\pi}{12}$ is an algebraic number. Is it an algebraic integer? Justify your answer.
- Let $K = \mathbb{Q}(\theta)$ be an algebraic number field where θ is a root of $X^3 - X - 1$. Calculate $N_{K/\mathbb{Q}}(3\theta^2 - 1)$.

- Let $K = \mathbb{Q}(\theta)$ be an algebraic number field where θ is a root of $X^3 - X^2 - 2X - 8$. Calculate $N_{K/\mathbb{Q}}(3\theta^2 - 2\theta - 2)$.
- Let $F \subseteq K \subseteq L$ be a tower of finite extensions of degrees 3 and 2 respectively. Prove that $Tr_{L/F}(\gamma) = Tr_{K/F}(Tr_{L/K}(\gamma))$ for each $\gamma \in L$.
- Let $F \subseteq K \subseteq L$ be a tower of finite extensions of degrees 2 and 3 respectively. Given $\gamma \in L$, prove that $N_{L/F}(\gamma) = N_{K/F}(N_{L/K}(\gamma))$. (Hint: It is enough to prove the desired equality when $L = K(\gamma)$. Let $\{w_1, w_2\}$ be a basis of K/F. Compute the matrix of T_γ with respect to the basis $\{w_1, w_2; \gamma w_1, \gamma w_2; \gamma^2 w_1, \gamma^2 w_2\}$).