Introduction to Algebraic Number Theory

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 500

1. Number Fields
   - Algebraic Numbers
   - Minimal Polynomials
   - The Field of Algebraic Numbers
   - Number Fields
   - Integrality
   - The Ring of All Algebraic Integers
   - Rings of Integers of Number Fields

Subsection 1

Algebraic Numbers

Algebraic and Transcendental Numbers

Definition

A complex number α is said to be **algebraic** if it is the root of a polynomial equation with integer coefficients.
If α is not algebraic, it is **transcendental**.

Example: Every rational number $\frac{m}{n}$ is algebraic.

It is a root of $nX - m = 0$.

Also $\pm\sqrt{2}$ are roots of $X^2 - 2 = 0$. So $\pm\sqrt{2}$ are both algebraic.

- Every polynomial with integer coefficients of degree n will have n algebraic numbers as roots.
- Liouville (1844) was the first to construct an explicit example of a transcendental number.
- Hermite (1873) proved that e is transcendental
- Lindemann (1882) proved that π is transcendental.

Countability of Algebraic Numbers

- Write $\mathscr{A} \subseteq \mathbb{C}$ for the collection of all algebraic numbers.

Theorem (Cantor)

The set $\mathscr{A}$ is countable, i.e., there are only countably many algebraic numbers.

- Let
$$p(X) = c_0X^d + c_1X^{d-1} + \cdots + c_d = 0$$
be a polynomial equation, with all $c_i \in \mathbb{Z}$ and $c_0 \neq 0$.
Define the quantity
$$H(p) = d + |c_0| + \cdots + |c_d| \in \mathbb{Z}.$$
This process associates an integer to every polynomial with integer coefficients. Note that $\deg(p) = d < H(p)$.

Countability of Algebraic Numbers (Cont'd)

- Let H be any natural number.

  Then it is easy to see that there are only finitely many polynomials $p(X)$ which satisfy $H(p) \leq H$.

  Say that an algebraic number $\alpha \in \mathscr{A}$ is **of level** H if α is a root of some polynomial p with $H(p) \leq H$.

  We observe again that:

  - There are only finitely many polynomials with $H(p) \leq H$;
  - All of them have at most H roots (since the degree of such a polynomial is bounded by H).

  Thus, there are only finitely many algebraic numbers of level H, for any given H.

Countability of Algebraic Numbers (Cont'd)

- Conversely, every algebraic number is a root of such a polynomial.

  Thus, every algebraic number is of level H for some H.

  The collection of algebraic numbers can therefore be written as a union

  $$\mathscr{A} = \bigcup_{H=1}^{\infty} \{\alpha \in \mathscr{A} : \alpha \text{ is of level } H\}.$$

  We have observed that each set on the right-hand side is finite.

  Furthermore, the union is a countable union, as the indexing set consists of the natural numbers.

  Therefore, $\mathscr{A}$ is a countable union of finite sets.

  It is therefore countable.

  Now $\mathbb{C}$ is uncountable, and its subset $\mathscr{A}$ is countable.

  Hence, transcendental numbers exist and, moreover, the set of transcendental numbers is actually uncountable.

Liouville's Theorem

Theorem (Liouville)

Let α be a real algebraic number which is a root of an irreducible polynomial $f(X)$ over $\mathbb{Z}$ of degree $n > 1$. Then there is a constant c, such that for all rational numbers $\frac{p}{q}$,

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^n}.$$

- If $\left|\alpha - \frac{p}{q}\right| > 1$, choosing $c = 1$ covers these values.

  We consider the case $\left|\alpha - \frac{p}{q}\right| \leq 1$.

Liouville's Theorem (Cont'd)

- Apply the Mean Value Theorem to $f(X)$ at the points α and $\frac{p}{q}$.

  We deduce that there exists γ, strictly between α and $\frac{p}{q}$, such that

$$f'(\gamma) = \frac{f(\alpha) - f(\frac{p}{q})}{\alpha - \frac{p}{q}}.$$

  As α is a root of f, we have $f(\alpha) = 0$.

  As $f(X)$ is irreducible of degree $n > 1$, it has no rational roots.

  So $f(\frac{p}{q}) \neq 0$.

  But $f(X)$ has integer coefficients.

  So the denominator of $f(\frac{p}{q})$ must divide q^n.

  Hence, $q^n f(\frac{p}{q})$ is a non-zero integer. So $\left| f\left(\frac{p}{q}\right) \right| \geq \frac{1}{q^n}$.

Liouville's Theorem (Cont'd)

- Now $|\gamma - \alpha| < 1$ as α is strictly between α and $\frac{p}{q}$, and $|\alpha - \frac{p}{q}| \leq 1$.

  By continuity of f' at α, we see that $|f'(\gamma)| < \frac{1}{c_0}$, for some constant c_0 for all γ within 1 of α, where the constant c_0 depends only on α.

  Then
  $$\left|\alpha - \frac{p}{q}\right| = \left|\frac{f(\frac{p}{q})}{f'(\gamma)}\right| > \frac{c_0}{q^n}.$$

  Finally, choose $c = \min(c_0, 1)$ to cover both cases.

Liouville's Transcendental Number

- In order to find a transcendental number, we need to find an α, where the inequality of Liouville's Theorem fails for all n.

  Liouville suggested choosing

  $$\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}} = 0.110001000000000000000001 00\ldots.$$

  Define

  $$\frac{p_r}{q_r} = \sum_{k=1}^{r} \frac{1}{10^{k!}}.$$

  The first three numbers are

  $$\frac{p_1}{q_1} = 0.1, \quad \frac{p_2}{q_2} = 0.11, \quad \frac{p_3}{q_3} = 0.110001.$$

Liouville's Transcendental Number (Cont'd)

- Then $q_r = 10^{r!}$.

  Moreover,

  $$\left|\alpha - \frac{p_r}{q_r}\right| = \sum_{k=r+1}^{\infty} \frac{1}{10^{k!}} < \frac{2}{10^{(r+1)!}} = \frac{2}{(10^{r!})^{r+1}} = \frac{2}{q_r^{r+1}}.$$

  Assume, towards a contradiction, that α is algebraic of some degree n.

  Then, there is a constant c, such that, for all rationals $\frac{p}{q}$,

  $$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^n}.$$

  However, choosing $\frac{p}{q} = \frac{p_r}{q_r}$, for large enough $r > n$, contradicts the previous inequality.

Subsection 2

Minimal Polynomials

Minimal Polynomial

- A **monic polynomial** is one whose leading coefficient is 1.

Lemma

If α is algebraic, then there is a unique monic polynomial $f(X) \in \mathbb{Q}[X]$ of smallest degree with α as a root.

- Suppose α is a root of a polynomial

$$f(X) = c_0X^n + c_1X^{n-1} + \cdots + c_n, \quad c_0 \neq 0.$$

Then it is also a root of

$$X^n + \frac{c_1}{c_0}X^{n-1} + \cdots + \frac{c_n}{c_0},$$

got by dividing through by the leading coefficient.

Among all the monic polynomials with α as a root, let $f(X)$ be one with smallest degree.

Minimal Polynomial (Cont'd)

- Claim: $f(X)$ is unique.

  Suppose that $g(X)$ is another monic polynomial of the same degree as $f(X)$, with α as a root.

  Then α is also a root of $(f-g)(X)$.

  Moreover, the leading terms of $f(X)$ and $g(X)$ cancel.

  So the degree of $f-g$ is smaller than that of f or g.

  If $f-g \neq 0$, then we can divide through by its leading coefficient to find a monic polynomial of smaller degree than f with α as a root.

  But this contradicts the choice of $f(X)$.

Irreducibility of the Minimal Polynomial

Definition

Let α be an algebraic number. The **minimal polynomial of α over $\mathbb{Q}$** is the monic polynomial over $\mathbb{Q}$ of smallest degree with α as a root.

Lemma

If $m(X)$ is the minimal polynomial of the algebraic number α, then it is irreducible.

- Suppose $m(X)$ factorizes as the product $f(X)g(X)$ of two polynomials over $\mathbb{Q}$ of smaller degree.

  Since $m(\alpha) = 0$, we have $f(\alpha)g(\alpha) = 0$.

  Thus, α is a root of either f or g.

  This contradicts the choice of m as the polynomial of smallest degree with α as a root.

Divisibility Property of the Minimal Polynomial

Lemma

Suppose that α is a root of some polynomial $f(X) \in \mathbb{Q}[X]$.
If $m(X)$ is the minimal polynomial of α, then $m(X) \mid f(X)$.

- The ring of rational polynomials $\mathbb{Q}[X]$ has a division algorithm.
  So, we can find polynomials $q(X), r(X) \in \mathbb{Q}[X]$, such that

$$f(X) = q(X)m(X) + r(X),$$

where $r(X)$ is the zero polynomial, or has smaller degree than $m(X)$.
Substitute $X = \alpha$ to get

$$f(\alpha) = q(\alpha)m(\alpha) + r(\alpha).$$

As $f(\alpha) = m(\alpha) = 0$, we must have $r(\alpha) = 0$.

Divisibility Property of the Minimal Polynomial (Cont'd)

- However, $r(X)$ has smaller degree than $m(X)$.

  Moreover, $m(X)$ was the monic polynomial of smallest degree with α as a root.

  So, if $r(X)$ were non-zero, we could scale it to get a monic polynomial of smaller degree than $m(X)$ with α as a root.

  This would contradict the definition of $m(X)$.

  Therefore, $r(X)$ must be the zero polynomial.

  In particular,

  $$f(X) = q(X)m(X).$$

  So $f(X)$ is a multiple of $m(X)$.

Minimal Polynomials over a Field K

- Suppose K is any field.
- Assume α satisfies some equation over K.
- Then we also have a notion of **minimal polynomial over K**.
- This is the monic polynomial with coefficients in K of smallest degree with α as a root.
- Any other polynomial with coefficients in K with α as a root is a multiple of the minimal polynomial.

Subsection 3

The Field of Algebraic Numbers

Fields and Subfields of $\mathbb{C}$

- Recall that a **field** is a set which satisfies:
  - Exactly the same algebraic properties as $\mathbb{Q}$ so that we be able to add, subtract, multiply and divide (by non-zero elements) as in $\mathbb{Q}$;
  - The usual algebraic rules (e.g., addition and multiplication are commutative and associative).
- Since we are dealing with subsets of the complex numbers $\mathbb{C}$, all these rules are inherited from $\mathbb{C}$.
- Thus, to check that the set $\mathscr{A}$ of algebraic numbers is a field, we just have to check that the collection of algebraic numbers is closed under the usual arithmetic operations.
- That is, we want to see that if α and β are algebraic numbers, then so are $\alpha+\beta$, $\alpha-\beta$ and $\alpha\beta$, and if $\beta\neq 0$, so is $\frac{\alpha}{\beta}$.

The Field $\mathbb{Q}(\alpha)$ and the Ring $\mathbb{Q}[\alpha]$

- Recall that for any complex number α, $\mathbb{Q}(\alpha)$ denotes the smallest field one can obtain by applying all the usual arithmetic operations (addition, subtraction, multiplication, division) to the rational numbers and α;
- It actually consists of all quotients $\frac{p(\alpha)}{q(\alpha)}$, where $p(X)$ and $q(X)$ are polynomials with rational coefficients, and where $q(\alpha) \neq 0$.
- On the other hand, $Q[\alpha]$ denotes the ring of all polynomial expressions in α.
- It is the smallest ring one can obtain by applying the arithmetic operations of addition, subtraction and multiplication (but not division) to the rational numbers and α.

  Example: $\frac{3\alpha^3+\alpha-1}{\alpha^2+2}$ is in $\mathbb{Q}(\alpha)$, but not necessarily in $\mathbb{Q}[\alpha]$.
- Clearly, we have $Q[\alpha] \subseteq \mathbb{Q}(\alpha)$.

$\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$ for Algebraic α

Proposition

If α is algebraic, $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$, and so every element of $\mathbb{Q}(\alpha)$ can be written as a polynomial in α.

- We have to explain that every quotient of polynomials $\frac{p(\alpha)}{q(\alpha)}$ with $q(\alpha) \neq 0$ can be written alternatively as a polynomial in α.

  Let $m(X)$ denote the minimal polynomial of α over $\mathbb{Q}$.

  The greatest common factor of $m(X)$ and $q(X)$ must divide $m(X)$.

  As $m(X)$ is irreducible, its only factors are 1 and $m(X)$ itself.

  But $m(X)$ is not a factor of $q(X)$, as $m(\alpha) = 0$, but $q(\alpha) \neq 0$.

$\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$ for Algebraic α (Cont'd)

- Thus, there are polynomials $s(X)$ and $t(X)$ over $\mathbb{Q}$, such that
$$s(X)q(X) + t(X)m(X) = 1.$$
In particular,
$$s(\alpha)q(\alpha) + t(\alpha)m(\alpha) = 1.$$
Therefore, $s(\alpha)q(\alpha) = 1$, because $m(\alpha) = 0$.
We conclude that $\frac{1}{q(\alpha)} = s(\alpha)$.
So
$$\frac{p(\alpha)}{q(\alpha)} = p(\alpha)s(\alpha),$$
a polynomial expression in α.

Characterization of Algebraic Numbers

- We saw that, if α is algebraic, then $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$.
- Suppose, now, that α is transcendental.
- Then there is no way to write $\frac{1}{\alpha}$ as a polynomial in α.
- Otherwise, we could multiply through by α and find a rational polynomial with α as a root.
- Therefore, $\frac{1}{\alpha}$ is in $\mathbb{Q}(\alpha)$, but not in $\mathbb{Q}[\alpha]$.
- Thus, if α is not algebraic, then $\mathbb{Q}(\alpha)$ is strictly bigger than $\mathbb{Q}[\alpha]$.
- It follows that the property

$$\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$$

characterizes algebraic numbers.

The Degree of Field Extensions

- The **degree** of the field extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ is the dimension of the set $\mathbb{Q}(\alpha)$ when regarded as a vector space over $\mathbb{Q}$.
- That is, it equals the number of elements in a basis $\{\omega_1, \dots, \omega_n\}$ so that every element of $\mathbb{Q}(\alpha)$ can be expressed uniquely as a sum

$$a_1\omega_1 + \cdots + a_n\omega_n, \quad a_i \in \mathbb{Q}.$$

- The **degree** of $\mathbb{Q}(\alpha)/\mathbb{Q}$ is denoted $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.

  Example: $\mathbb{Q}(\sqrt{2})$ has degree 2 over $\mathbb{Q}$.

  Each element in $\mathbb{Q}(\sqrt{2})$ can be written as $a + b\sqrt{2}$.

Algebraicity and Degree of Extension

Proposition

Let α be a complex number. Then the following are equivalent:

1. α is algebraic;
2. The field extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ is of finite degree.

(1)⇒(2): Suppose that α is algebraic.

Consider the minimal polynomial for α,

$$m(X) = X^n + c_1 X^{n-1} + \cdots + c_n.$$

Then $\alpha^n + c_1 \alpha^{n-1} + \cdots + c_n = 0$.

Rearranging, $\alpha^n = -(c_1 \alpha^{n-1} + \cdots + c_n)$.

By hypothesis, α is algebraic.

So every element of $\mathbb{Q}(\alpha)$ can be written as a polynomial in α.

Algebraicity and Degree of Extension (Cont'd)

- If the polynomial expression for an element has degree n or above, we can reduce the degree by replacing all occurrences of α^r, for $r \geq n$, using the preceding equation.

  So every element of $\mathbb{Q}(\alpha)$ can be written as an expression

  $$a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + \cdots + a_0, \quad a_i \in \mathbb{Q}.$$

  Claim: This expression of an element of $\mathbb{Q}(\alpha)$ is unique.

  Suppose an element can be written in two different ways

  $$\begin{aligned} & a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + \cdots + a_0 \\ & \quad = b_{n-1}\alpha^{n-1} + b_{n-2}\alpha^{n-2} + \cdots + b_0. \end{aligned}$$

  Subtracting one side from the other gives a polynomial of degree strictly smaller than n with α as a root.

  However, the minimal polynomial is $m(X)$, of degree n.

  So there can be no polynomial of degree less than n with α as a root.

Algebraicity and Degree of Extension (Cont'd)

- We showed that every element of $\mathbb{Q}(\alpha)$ is a unique rational linear combination of the n elements $1, \alpha, \ldots, \alpha^{n-1}$.

  Thus, $\mathbb{Q}(\alpha)$ is n-dimensional as a vector space over $\mathbb{Q}$.

  Therefore, $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is finite.

  (2)⇒(1): Suppose $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is some finite number n.

  Then any $n+1$ elements of the $\mathbb{Q}$-vector space $\mathbb{Q}(\alpha)$ are dependent.

  In particular, the elements $1, \alpha, \ldots, \alpha^n$ are linearly dependent.

  So there exists a linear relationship

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0.$$

  Consequently, α satisfies a polynomial equation over $\mathbb{Q}$.

  Therefore, α is algebraic.

Degree of Extension and of Minimal Polynomial

Corollary

Suppose that α is algebraic. Then the degree of the extension $[\mathbb{Q}(\alpha):\mathbb{Q}]$ is the same as the degree of the minimal polynomial of α over $\mathbb{Q}$.
Every element of $\mathbb{Q}(\alpha)$ can be written as a polynomial in α of degree less than $[\mathbb{Q}(\alpha):\mathbb{Q}]$.

- This just follows from the proof of the proposition.
- More generally, the same argument shows that if K is any field, then an element α is algebraic over K (i.e., satisfies a polynomial equation with coefficients in K) if and only if $[K(\alpha):K]$ is finite.
- Moreover, in that case, the degree $[K(\alpha):K]$ is also the degree of the minimal polynomial of α over K.

Adjoining More Than One Number to a Field

- We can adjoin more than one number to a field.
- Consider, e.g., α and β algebraic.
- Define

$$\mathbb{Q}(\alpha,\beta) := \mathbb{Q}(\alpha)(\beta).$$

- This is the set of all polynomial expressions in β with coefficients in $\mathbb{Q}(\alpha)$.
- We can show that this just gives all the polynomials in the two variables α and β.

Closure Under Algebraic Operations

Corollary

Suppose that α and β are algebraic. Then $\alpha+\beta$, $\alpha-\beta$ and $\alpha\beta$ are algebraic. If also $\beta \neq 0$, then $\frac{\alpha}{\beta}$ is algebraic.

- Suppose that α and β are algebraic.

  By the proposition, $[\mathbb{Q}(\alpha):\mathbb{Q}]$ and $[\mathbb{Q}(\beta):\mathbb{Q}]$ are finite.

  Write

$$\begin{aligned} m &= [\mathbb{Q}(\alpha):\mathbb{Q}], \\ n &= [\mathbb{Q}(\beta):\mathbb{Q}]. \end{aligned}$$

  Claim: $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]$ is finite.

Closure Under Algebraic Operations (Cont'd)

- A typical element of $\mathbb{Q}(\alpha,\beta)$ is a polynomial expression

$$\sum_{i=0}^{k}\sum_{j=0}^{\ell} a_{ij}\alpha^i\beta^j.$$

We know the following:
  - Every α^i, with $i \geq m$, can be written as a polynomial in α of degree at most $m-1$;
  - Every β^j, with $j \geq n$, can be written as a polynomial in β of degree at most $n-1$.

Substituting, we see that any element of $\mathbb{Q}(\alpha,\beta)$ can be written

$$\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} a'_{ij}\alpha^i\beta^j, \quad a'_{ij}.$$

So $\mathbb{Q}(\alpha,\beta)$ is spanned by the set $\{\alpha^i\beta^j : 0 \leq i \leq m-1, 0 \leq j \leq n-1\}$.
Thus, $\mathbb{Q}(\alpha,\beta)$ has a finite spanning set as a $\mathbb{Q}$-vector space.
Therefore $[\mathbb{Q}(\alpha,\beta) : \mathbb{Q}]$ is finite.

Closure Under Algebraic Operations (Conclusion)

- Suppose α and β are algebraic.

  We show that $\alpha+\beta$ is algebraic.

  Note that $\alpha+\beta \in \mathbb{Q}(\alpha,\beta)$.

  So $\mathbb{Q}(\alpha+\beta) \subseteq \mathbb{Q}(\alpha,\beta)$.

  It follows that $[\mathbb{Q}(\alpha+\beta):\mathbb{Q}] \le [\mathbb{Q}(\alpha,\beta):\mathbb{Q}]$.

  Hence, $[\mathbb{Q}(\alpha+\beta):\mathbb{Q}]$ is finite.

  So $\alpha+\beta$ must be algebraic.

  The arguments for $\alpha-\beta$, $\alpha\beta$ and $\frac{\alpha}{\beta}$ are all similar, as each lies in $\mathbb{Q}(\alpha,\beta)$.

Corollary

The algebraic numbers $\mathscr{A}$ form a field.

Subsection 4

Number Fields

Number Fields

- The field $\mathscr{A}$ is countable.
- But it is much larger than the rational numbers $\mathbb{Q}$ (e.g., it has infinite degree over $\mathbb{Q}$).
- So it is too large to be really useful.
- The fields in which we are going to generalize ideas of primes, factorizations, and so on, are the finite extensions of $\mathbb{Q}$.

Definition

A field K is a **number field** if it is a finite extension of $\mathbb{Q}$. The **degree** of K is the degree of the field extension $[K : \mathbb{Q}]$, i.e., the dimension of K as a vector space over $\mathbb{Q}$.

- In particular, every element in K lies inside a finite extension of $\mathbb{Q}$.
- By a previous proposition, every element of K is necessarily algebraic.

Examples

1. $\mathbb{Q}$ itself is a number field.
2. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is a number field.

   Every element is a $\mathbb{Q}$-linear combination of 1 and $\sqrt{2}$.

   So $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, which is finite.
3. Similarly, $\mathbb{Q}(i)$ is a number field, as is $\mathbb{Q}(\sqrt{d})$ for any integer d.

   We may assume that d is not divisible by a square ("squarefree").

   If $d = m^2 d'$, then $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'})$.

   It is easy to see (from the quadratic formula) that every quadratic field $\mathbb{Q}(\alpha)$ is of this form.

   So every quadratic number field is $\mathbb{Q}(\sqrt{d})$, for some squarefree d.

Examples (Cont'd)

4. $\mathbb{Q}(\sqrt[3]{2})$ is a number field, as $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$, which is finite.
   Every element can be written in the form
   $$a+b\sqrt[3]{2}+c(\sqrt[3]{2})^2, \quad a,b,c\in\mathbb{Q}.$$
   So 1, $\sqrt[3]{2}$, $(\sqrt[3]{2})^2$ form a basis for $\mathbb{Q}(\sqrt[3]{2})$ as a vector space over $\mathbb{Q}$.
5. $\mathbb{Q}(\sqrt{2},\sqrt{3})$ is also a number field.
   Every element can be written in the form
   $$a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}, \quad a,b,c\in\mathbb{Q}.$$
   So $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$ forms a basis for $\mathbb{Q}(\sqrt{2},\sqrt{3})$ over $\mathbb{Q}$.
   It follows that $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=4$.
6. $\mathbb{Q}(\pi)$ is not a number field.
   π is transcendental.
   So it does not satisfy any polynomial equation over $\mathbb{Q}$.
   Therefore, $[\mathbb{Q}(\pi):\mathbb{Q}]$ is infinite.

The Characteristic of a Field and Simple Extensions

- Every number field contains the rationals.
- So every number field is infinite and of characteristic 0.
- The **characteristic** of a field is 0 if $1+1+\cdots+1$ is never equal to 0, and is p if p is the smallest number such that $1+1+\cdots+1=0$, where p is the number of 1's in the left-hand sum.
- Fields of characteristic 0 always contain $\mathbb{Q}$.
- Fields of characteristic p exist for any prime number p.
- They always contain the integers modulo p, $\{0,1,\ldots,p-1\}$, which is the smallest field of characteristic p, and is denoted by $\mathbb{F}_p$.
- An extension is **simple** if it is generated by a single element.

Extensions of $\mathbb{Q}$ in $\mathbb{C}$

- Every element of a number field is algebraic.
- So it is a root of a polynomial with rational coefficients.
- All roots of polynomials with rational coefficients are complex numbers.
- So we can view every number field as a subfield of the complex numbers $\mathbb{C}$.
- However, there is not usually a natural way to do this.

  Example: Suppose a number field contains a square root $\sqrt{-1}$ of -1.

  We have a choice whether to view this as i or as $-i$ inside the complex numbers.

Irreducibility in $\mathbb{Q}[X]$ and Roots in $\mathbb{C}$

Lemma

Suppose that $f(X) \in \mathbb{Q}[X]$ is an irreducible polynomial. Then it has distinct roots in $\mathbb{C}$.

- Over $\mathbb{C}$, factorize $f(X)$ as

$$c\prod_{i=1}^{r}(X-\gamma_i)^{d_i}.$$

Suppose, to the contrary, that the lemma fails.
Then $d_i > 1$, for some i.
So $f(X)$ would have a factor $(X-\gamma_i)^2$.
Write

$$f(X) = (X-\gamma_i)^2 g(X).$$

We see that $(X-\gamma_i)$ is also a factor of the derivative $f'(X)$.
So $(X-\gamma_i)$ is a common factor of f and f'.

Irreducibility in $\mathbb{Q}[X]$ and Roots in $\mathbb{C}$ (Cont'd)

- Thus, the greatest common factor h of f and f' has degree ≥ 1.

  But the highest common factor of f and f' is obtained by Euclid's algorithm in $\mathbb{Q}[X]$, and is a polynomial with rational coefficients that divides into both f and f'.

  However, f is irreducible.

  So its only factors are 1 and f.

  Since h has degree at least 1, we conclude that $h = f$.

  But then we obtain $f \mid f'$.

  This contradicts the fact that the degree of f is bigger than the degree of f', which is a nonzero polynomial (as f has degree $d \geq 1$).

Irreducibility and Characteristic of the Field

- More generally, the proof of the lemma shows that any irreducible polynomial over a field of characteristic 0 has distinct roots.
- In characteristic p, things change.
- Here it is possible for an irreducible polynomial to have derivative 0.
- The polynomial may only involve terms in X^p.
- Their derivatives then are divisible by p, and vanish.

  Example: In a field of characteristic p, consider the polynomial

$$f(X) = X^p.$$

  $f(X)$ is not irreducible.

  It is, however, an example where f divides f', as $f' = 0$.

The Primitive Element Theorem

Theorem (Primitive Element)

Suppose $K \subseteq L$ is a finite extension of fields of characteristic 0 (e.g., number fields). Then $L = K(\gamma)$, for some element $\gamma \in L$.

- Suppose L is generated over K by m elements.
  We first treat the case $m = 2$. Suppose $L = K(\alpha, \beta)$.
  Let f and g denote the minimal polynomials of α and β over K.
  Suppose $\alpha_1 = \alpha$, $\alpha_2, \ldots, \alpha_s$ are the roots of f in $\mathbb{C}$.
  Suppose $\beta_1 = \beta, \beta_2, \ldots, \beta_t$ are the roots of g in $\mathbb{C}$.
  Irreducible polynomials always have distinct roots.
  Thus, if $j \neq 1$, $\alpha_i + X\beta_j = \alpha_1 + X\beta_1$ has a unique solution
  $$X = \frac{\alpha_i - \alpha_1}{\beta_1 - \beta_j}.$$
  Choose a $c \in K$ different from each of these X's.
  Then each $\alpha_i + c\beta_j$ is different from $\alpha + c\beta$.

The Primitive Element Theorem (Cont'd)

Claim: $\gamma = \alpha + c\beta$ generates L over K.

Certainly $\gamma \in K(\alpha, \beta) = L$.

It suffices to verify that $\alpha, \beta \in K(\gamma)$.

Consider the polynomials $g(X)$ and $f(\gamma - cX)$.

They both have coefficients in $K(\gamma)$.

Moreover, they both have β as a root.

The other roots of $g(X)$ are $\beta_2, \ldots, \beta_t$.

Moreover, $\gamma - c\beta_j$ is not any α_i, unless $i = j = 1$.

So β is the only common root of $g(X)$ and $f(\gamma - cX)$.

Thus, $(X - \beta)$ is the highest common factor of $g(X)$ and $f(\gamma - cX)$.

But the highest common factor is a polynomial defined over any field containing the coefficients of the original two polynomials.

In particular, it follows that $X - \beta$ has coefficients in $K(\gamma)$.

So $\beta \in K(\gamma)$. Then $\alpha = \gamma - c\beta \in K(\gamma)$.

The Primitive Element Theorem (The Case $m > 2$)

- Consider the case where $m > 2$.

  We can prove this using the result for $m = 2$.

  Suppose $L = K(\alpha_1, \ldots, \alpha_m)$.

  View L as
  $$K(\alpha_1, \ldots, \alpha_{m-2})(\alpha_{m-1}, \alpha_m).$$
  The case $m = 2$ allows us to write this as
  $$K(\alpha_1, \ldots, \alpha_{m-2})(\gamma_{m-1}).$$
  Rewrite this as
  $$K(\alpha_1, \ldots, \alpha_{m-3})(\alpha_{m-2}, \gamma_{m-1}).$$
  Use, again, the case $m = 2$ to reduce the number further.

  Continuing in this way, we eventually get down to just one element.

Consequence for Number Fields

- The preceding proof uses properties of fields of characteristic 0 in two places.
  - When using the fact that irreducible polynomials always have distinct roots, which is true for any field of characteristic 0.
  - When choosing a value of c different from all values in some finite set, which we can do because fields of characteristic 0 are infinite.

Corollary

Let K be a number field. Then $K = \mathbb{Q}(\gamma)$, for some element γ.

Example

- By the corollary, it should be possible to express the number field $\mathbb{Q}(\sqrt{2},\sqrt{3})$ as $\mathbb{Q}(\gamma)$, for some element γ.

  By the proof of the theorem, it seems that we should be able to take $\gamma = \sqrt{2} + c\sqrt{3}$ for almost any choice of c (only finitely many values might be excluded).

  We try $c = 1$, so that $\gamma = \sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2},\sqrt{3})$.

  Then we have
  - $1 = 1$;
  - $\gamma = \sqrt{2} + \sqrt{3}$;
  - $\gamma^2 = (\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}$;
  - $\gamma^3 = (\sqrt{2} + \sqrt{3})(5 + 2\sqrt{6}) = 11\sqrt{2} + 9\sqrt{3}$.

  We see that
  $$\sqrt{2} = \frac{\gamma^3 - 9\gamma}{2} \quad \text{and} \quad \sqrt{3} = \frac{11\gamma - \gamma^3}{2}.$$

Example (Cont'd)

- We got
$$\sqrt{2} = \frac{\gamma^3 - 9\gamma}{2} \quad \text{and} \quad \sqrt{3} = \frac{11\gamma - \gamma^3}{2}.$$
It follows that both $\sqrt{2}$ and $\sqrt{3}$ can be written as polynomials in γ.
So $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\gamma)$.
Therefore,
$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\gamma).$$
On the other hand, $\gamma \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
This gives the other inclusion
$$\mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

Subsection 5

Integrality

Integers in a Number Field

- When we "do number theory", we almost always refer to properties of the integers $\mathbb{Z}$, rather than $\mathbb{Q}$.
- So to work in a number field K, we need to define a subset $\mathbb{Z}_K$ of "integers in K".
- We impose the following requirements.
  - $\mathbb{Z}_K$ should be a ring, so that we can add, subtract and multiply in $\mathbb{Z}_K$;
  - The integers in $\mathbb{Q}$ turn out to be $\mathbb{Z}$;
  - Given two number fields $K \subseteq L$ and an element $\alpha \in K$, α is an integer in K if and only if it is an integer in L.

    That is, if $K \subseteq L$ is an extension of number fields,

$$\mathbb{Z}_L \cap K = \mathbb{Z}_K.$$

A Failed First Attempt

- We looked at the Gaussian integers,
$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}.$$
- They seemed to have the appropriate properties in $\mathbb{Q}(i)$.
- It seems reasonable to hope that our definition of integers should give $\mathbb{Z}[i]$ as the integers for $\mathbb{Q}(i)$.
- We also know that every number field can be written in the form $\mathbb{Q}(\gamma)$.
- So, at first glance, it might seem reasonable to suggest that we define its integers to be $\mathbb{Z}[\gamma]$.

A Failed First Attempt (Cont'd)

- $\mathbb{Z}[\gamma]$ is a ring whose elements are polynomials in γ with integer coefficients.
- Any two of these can be added, subtracted or multiplied.
- In addition, $\mathbb{Z}[\gamma]$ gives the right answer for $\mathbb{Q}(i)$.
- Unfortunately, this is not a good definition.
- A number field may be written in more than one way as $\mathbb{Q}(\gamma)$.
- These expressions may give different answers for the integers.

  Example: Note that $\sqrt{8} = 2\sqrt{2}$.

  Therefore, $\mathbb{Q}(\sqrt{8}) = \mathbb{Q}(\sqrt{2})$.

  But $\mathbb{Z}[\sqrt{8}] \neq \mathbb{Z}[\sqrt{2}]$, since $\sqrt{2} \notin \mathbb{Z}[\sqrt{8}]$.

Algebraic Integers

- Associated to α is its *minimal polynomial over* $\mathbb{Q}$.
- Recall that this is the monic polynomial with rational coefficients of smallest degree which has α as a root.

Definition

Let α be an algebraic number. We say that α is an **algebraic integer** if the minimal polynomial of α over $\mathbb{Q}$ has coefficients in $\mathbb{Z}$.

Examples:

1. Every integer n is an algebraic integer.
   Its minimal polynomial over $\mathbb{Q}$ is $X - n$.
   The coefficients of this polynomial are indeed integral.
2. i is an algebraic integer.
   Its minimal polynomial is $X^2 + 1$, which is in $\mathbb{Z}[X]$.
3. $\sqrt{2}$ is an algebraic integer.
   Its minimal polynomial is $X^2 - 2$, again in $\mathbb{Z}[X]$.

More Examples

Examples (Cont'd):

4. $\omega = \dfrac{-1+\sqrt{-3}}{2}$ is an algebraic integer
   It is a root of the polynomial X^2+X+1.
   This polynomial is irreducible.
   So it must be the minimal polynomial of ω.
5. $\dfrac{-1+\sqrt{3}}{2}$ is not an algebraic integer.
   Its minimal polynomial is $X^2+X-\frac{1}{2}$.
   This involves fractional coefficients.
6. π is not an algebraic integer.
   It is not even an algebraic number.

- It may be surprising that $\frac{-1+\sqrt{-3}}{2}$ is an integer, but $\frac{-1+\sqrt{3}}{2}$ is not.
- Otherwise, the definition looks reasonable.

Sufficient Condition for Integrality

Lemma

Suppose that α satisfies any monic polynomial with coefficients in $\mathbb{Z}$. Then α is an algebraic integer.

- Suppose α is a root of the monic polynomial $f(X) \in \mathbb{Z}[X]$.

  Let $m(X) \in \mathbb{Q}[X]$ denote the minimal polynomial of α over $\mathbb{Q}$.

  We will show that $m(X) \in \mathbb{Z}[X]$.

  We have already seen that $m(X) \mid f(X)$.

  So $f(X) = q(X)m(X)$, for some polynomial $q(X) \in \mathbb{Q}[X]$.

  Since $f(X)$ and $m(X)$ are both monic, clearly $q(X)$ is also.

  So $f(X) = q(X)m(X)$ expresses $f(X) \in \mathbb{Z}[X]$ as a product of two monic polynomials $q(X)$ and $m(X)$ with rational coefficients.

Sufficient Condition for Integrality (Cont'd)

- Claim: $q(X)$ and $m(X)$ are both in $\mathbb{Z}[X]$.

  Choose positive integers a and b such that:
  - $aq(X)$ and $bm(X)$ are polynomials with integer coefficients;
  - The highest common factors of the coefficients of $aq(X)$, $bm(X)$ are 1.

  Indeed, a and b are just the least common multiples of the denominators of the coefficients of q and m, respectively.

  Then we have $(ab)f(X) = aq(X)bm(X)$.

  If $ab \neq 1$, choose a prime number $p \mid ab$.

  There are coefficients of $aq(X)$ and $bm(X)$ not divisible by p.

Sufficient Condition for Integrality (Cont'd)

- So there are also terms in the product whose coefficients are not divisible by p. E.g., consider the term coming from:
  - The first term of $aq(X)$ with coefficient not divisible by p;
  - The first term of $bm(X)$ with coefficient not divisible by p.

  On the other hand, the product is $(ab)f(X)$.

  So all the coefficients must be divisible by the integer ab.

  Therefore, they must be divisible by p.

  This contradiction shows that $ab = 1$.

  Therefore, $a = b = 1$, as a and b are positive integers.

  So both $q(X)$ and $m(X)$ are already in $\mathbb{Z}[X]$.

  In particular, $m(X) \in \mathbb{Z}[X]$.

  So the minimal polynomial of α has integral coefficients.

Gauss's Lemma

- We have essentially proven **Gauss's Lemma**:

  Suppose a polynomial $f(X) \in \mathbb{Z}[X]$ is reducible in $\mathbb{Q}[X]$.
  Then it is reducible in $\mathbb{Z}[X]$.

- Equivalently, if $f(X)$ factorizes into polynomials with rational coefficients then it factorizes into polynomials with integer coefficients.

Algebraic Numbers and Algebraic Integers

Claim: Every algebraic number has an integer multiple which is an algebraic integer. Equivalently, every algebraic number can be expressed as the quotient of an algebraic integer by an element of $\mathbb{Z}$.

Suppose that α is an algebraic number.

Then α is the root of some monic polynomial with coefficients in $\mathbb{Q}$,

$$X^n + a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \cdots + a_0 = 0.$$

Let d be an integer which is a common multiple of all the denominators of $a_{n-1}, \ldots, a_0$. Then $d\alpha$ is a root of

$$X^n + a_{n-1}dX^{n-1} + a_{n-2}d^2X^{n-2} + \cdots + a_0d^n = 0.$$

This is a monic polynomial with integer coefficients.

Therefore, $d\alpha$ is an algebraic integer.

Subsection 6

The Ring of All Algebraic Integers

Finitely Generated Modules

- A **module** M over a ring R is like a vector space over a field.
  - We can add two elements of M to get another element of M;
  - We can multiply an element of M by an element of R.
- The same rules are satisfied as for vector spaces.
- The theory of modules over rings is a little more complicated than vector spaces over fields, but for now, we just need the concept which is analogous to "finite dimensional" for vector spaces.
- The module $\mathbb{Z}[\alpha]$ is **finitely generated** over $\mathbb{Z}$ if there are finitely many elements $\omega_1, \ldots, \omega_n \in \mathbb{Z}[\alpha]$, such that every element of $\mathbb{Z}[\alpha]$ can be written as a sum

$$a_1\omega_1 + \cdots + a_n\omega_n$$

for suitable integers $a_1, \ldots, a_n \in \mathbb{Z}$.

Algebraic Characterization of Algebraic Integers

Proposition

Let $\alpha \in \mathbb{C}$. The following are equivalent:

1. α is an algebraic integer;
2. $\mathbb{Z}[\alpha]$ is a finitely generated module over $\mathbb{Z}$.

(1)⇒(2): Suppose that α is an algebraic integer.

Then α is a root of a monic polynomial $f(X) \in \mathbb{Z}[X]$ of some degree n.

Given any polynomial $g(X) \in \mathbb{Z}[X]$, write

$$g(X) = q(X)f(X) + r(X), \quad q(X), r(X) \in \mathbb{Z}[X],$$

where $r(X) = 0$ or the degree of $r(X)$ is less than n.

Note that, if $f(X)$ were not monic, we could only deduce that $q(X)$ and $r(X)$ would have rational coefficients.

Algebraic Characterization of Algebraic Integers (Cont'd)

- We wrote

$$g(X) = q(X)f(X) + r(X), \quad q(X), r(X) \in \mathbb{Z}[X].$$

Substitute in $X = \alpha$.

Then $g(\alpha) = r(\alpha)$, as α is a root of f.

So $g(\alpha)$ can be expressed as a polynomial of degree less than n.

So $g(\alpha)$ can be written as a linear combination of

$$1, \alpha, \ldots, \alpha^{n-1},$$

with integer coefficients.

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

Algebraic Characterization of Algebraic Integers (Converse)

(2)⇒(1): Suppose that $\mathbb{Z}[\alpha] = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$.
For each i, the product $\alpha\omega_i$ is again in $\mathbb{Z}[\alpha]$.
So it can be written as a linear combination of the spanning set,

$$\alpha\omega_i = \sum_{j=1}^{n} a_{ij}\omega_j, \quad a_{ij} \in \mathbb{Z}.$$

Consider the column vector $\boldsymbol{v} = (\omega_1, \ldots, \omega_n)^t$.
The previous equation implies that $\alpha\boldsymbol{v} = A\boldsymbol{v}$, where $A = (a_{ij})$.
That is, $\boldsymbol{v}$ is an eigenvector of A with eigenvalue α.
Therefore, α it is a root of the characteristic polynomial of A.
Characteristic polynomials are always monic.
Note, also, that the entries of A are integral.
So its characteristic polynomial has coefficients in $\mathbb{Z}$.
Thus, α is a root of a monic polynomial with integer coefficients.
So α is integral.

Algebraic Integers in Rings Containing $\mathbb{Z}$

- The next result is a corollary to the proof of the previous proposition, and a mild generalization.

Corollary

Let R be a ring containing $\mathbb{Z}$. If R is finitely generated as a $\mathbb{Z}$-module, then every element $\alpha \in R$ is the root of a monic polynomial with coefficients in $\mathbb{Z}$.

- The argument is exactly the same as before.

  By hypothesis, R is finitely generated.

  So $R = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$.

  For each i, we have $\alpha\omega_i = \sum_{j=1}^n a_{ij}\omega_j$, for some integers $a_{ij} \in \mathbb{Z}$.

  Then α is a root of the characteristic polynomial for the matrix (a_{ij}).

Two Algebraic Integers

Proposition

Suppose that α and β are algebraic integers. Then $\mathbb{Z}[\alpha, \beta]$ is finitely generated as a $\mathbb{Z}$-module.

- By the proposition, $\mathbb{Z}[\alpha]$, $\mathbb{Z}[\beta]$ are finitely generated as $\mathbb{Z}$-modules. That is:
  - There are elements
  $$\omega_1, \ldots, \omega_m \in \mathbb{Z}[\alpha],$$
  such that every element of $\mathbb{Z}[\alpha]$ can be written as a $\mathbb{Z}$-linear combination of these elements;
  - There are elements
  $$\theta_1, \ldots, \theta_n \in \mathbb{Z}[\beta],$$
  such that every element of $\mathbb{Z}[\beta]$ is a $\mathbb{Z}$-linear combination of these elements.

Two Algebraic Integers

- We show that every element γ of $\mathbb{Z}[\alpha,\beta]$ is a $\mathbb{Z}$-linear combination of the finite set
$$\{\omega_i\theta_j : 1 \le i \le m, 1 \le j \le n\}.$$
Now γ can be written as a polynomial
$$\sum_{k,\ell} a_{k\ell}\alpha^k\beta^\ell, \quad a_{k\ell} \in \mathbb{Z}.$$
Each $\alpha^k \in \mathbb{Z}[\alpha]$.
So it can be written as a $\mathbb{Z}$-linear combination of $\{\omega_i : 1 \le i \le m\}$.
Each $\beta^j \in \mathbb{Z}[\beta]$.
So it can be written as a $\mathbb{Z}$-linear combination of $\{\theta_j : 1 \le j \le n\}$.
Substituting these in, we see that γ can be written as a $\mathbb{Z}$-linear combination of the set $\{\omega_i\theta_j : 1 \le i \le m, 1 \le j \le n\}$, as required.

The Ring of Algebraic Integers

Corollary

The set of all algebraic integers forms a ring.

- Let α and β be algebraic integers.

  We need to check that $\alpha+\beta$, $\alpha-\beta$ and $\alpha\beta$ are algebraic integers.

  By the preceding proposition, $\mathbb{Z}[\alpha,\beta]$ is finitely generated as a $\mathbb{Z}$-module.

  Clearly, $\alpha+\beta\in\mathbb{Z}[\alpha,\beta]$.

  By a previous proposition, $\alpha+\beta$ is an algebraic integer.

  Now $\alpha-\beta$ and $\alpha\beta$ are also in $\mathbb{Z}[\alpha,\beta]$.

  So, by the same argument, they are also integral.

Example

- We illustrate a way to construct polynomials satisfied by the sum (or difference, or product) of two algebraic numbers.
  Example: We show that the sum
  $$\theta = \frac{1+\sqrt{5}}{2} + \frac{-1+\sqrt{-3}}{2} = \frac{\sqrt{5}+\sqrt{-3}}{2}$$
  is an algebraic integer, by computing its minimal polynomial.
  Write
  $$\alpha = \frac{1+\sqrt{5}}{2} \quad \text{and} \quad \beta = \frac{-1+\sqrt{-3}}{2}.$$
  α has minimal polynomial $X^2 - X - 1$.
  β has minimal polynomial $X^2 + X + 1$.
  Form the vector $\boldsymbol{v} = (1\ \alpha\ \beta\ \alpha\beta)^t$.
  We are going to find matrices A and B, with entries in $\mathbb{Z}$, such that
  $$A\boldsymbol{v} = \alpha\boldsymbol{v} \quad \text{and} \quad B\boldsymbol{v} = \beta\boldsymbol{v}.$$

Example (Cont'd)

- For $\boldsymbol{v} = (1 \ \alpha \ \beta \ \alpha\beta)^t$, we seek A and B, with entries in $\mathbb{Z}$, such that

$$A\boldsymbol{v} = \alpha\boldsymbol{v} \quad \text{and} \quad B\boldsymbol{v} = \beta\boldsymbol{v}.$$

  That is, α is an eigenvalue of A, and β is an eigenvalue of B.

  Then $(A+B)\boldsymbol{v} = (\alpha+\beta)\boldsymbol{v}$.

  So $\alpha+\beta$ is an eigenvalue of $A+B$.

  It is therefore a root of the characteristic polynomial of $A+B$, which is defined over $\mathbb{Z}$, since the entries of $A+B$ are integers.

  This gives a polynomial with $\alpha+\beta$ as a root.

Example (Matrix A)

- We first try to construct the matrix A. We must have

$$A\begin{pmatrix}1\\ \alpha\\ \beta\\ \alpha\beta\end{pmatrix}=\alpha\begin{pmatrix}1\\ \alpha\\ \beta\\ \alpha\beta\end{pmatrix}=\begin{pmatrix}\alpha\\ \alpha^2\\ \alpha\beta\\ \alpha^2\beta\end{pmatrix}.$$

But α is a root of $X^2=X+1$. So $\alpha^2=\alpha+1$. Thus, we need to solve

$$A\begin{pmatrix}1\\ \alpha\\ \beta\\ \alpha\beta\end{pmatrix}=\begin{pmatrix}\alpha\\ \alpha+1\\ \alpha\beta\\ (\alpha+1)\beta\end{pmatrix}.$$

We find $A=\begin{pmatrix}0&1&0&0\\ 1&1&0&0\\ 0&0&0&1\\ 0&0&1&1\end{pmatrix}$.

Example (Matrix B)

- Similarly, we can find a matrix B with the property that

$$B\begin{pmatrix} 1 \\ \alpha \\ \beta \\ \alpha\beta \end{pmatrix} = \beta\begin{pmatrix} 1 \\ \alpha \\ \beta \\ \alpha\beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha\beta \\ \beta^2 \\ \alpha\beta^2 \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha\beta \\ -(\beta+1) \\ -\alpha(\beta+1) \end{pmatrix}.$$

We take

$$B = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & -1 & 0 \\ 0 & -1 & 0 & -1 \end{pmatrix}.$$

Example (Matrix $A+B$)

- Then
$$A+B=\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ -1 & 0 & -1 & 1 \\ 0 & -1 & 1 & 0 \end{pmatrix}.$$
Our preceding argument shows that θ should be a root of the characteristic polynomial of $A+B$.

In the same way, note that
$$AB\mathbf{v}=A(B\mathbf{v})=A(\beta\mathbf{v})=\beta(A\mathbf{v})=\alpha\beta\mathbf{v}.$$
So $\alpha\beta$ is an eigenvalue of AB.

So $\alpha\beta$ is a root of the characteristic polynomial of AB.

Generalizing the Method

- Suppose α is a root of an equation of degree m.

  Suppose β is a root of an equation of degree n.

  Form the vector of length mn:

  $$\boldsymbol{v} = (1, \ldots, \alpha^{m-1}, \beta, \ldots, \alpha^{m-1}\beta, \ldots, \beta^{n-1}, \ldots, \alpha^{m-1}\beta^{n-1})^t.$$

  As in the example above, we can find $mn \times mn$-matrices A and B, such that

  $$A\boldsymbol{v} = \alpha\boldsymbol{v} \quad \text{and} \quad B\boldsymbol{v} = \beta\boldsymbol{v}.$$

  Then A and B will be $mn \times mn$-matrices.

  $\alpha + \beta$, $\alpha - \beta$ and $\alpha\beta$ are eigenvalues of $A + B$, $A - B$ and AB, respectively (with $\boldsymbol{v}$ as eigenvector).

  The characteristic polynomials of $A + B$, $A - B$ and AB have degree mn.

Generalizing the Method (Cont'd)

- Suppose α and β are both algebraic integers.

  Then the matrices A and B have entries in $\mathbb{Z}$.

  So the entries of $A+B$, $A-B$ and AB are all also in $\mathbb{Z}$.

  Therefore, the characteristic polynomials of these matrices are all integral.

  Moreover, they are monic, by definition.

  This gives another proof that the eigenvalues $\alpha+\beta$, $\alpha-\beta$ and $\alpha\beta$ are all algebraic integers.

Difference, Products and Quotients of Algebraic Numbers

- The same method also shows that the sum, difference and product of any two algebraic numbers is again algebraic.
- The two matrices A and B will in general no longer be integral, but have rational entries.
- We can extend the method to the case of quotients.

  If $\beta \neq 0$, then B will be invertible.

  Then $\boldsymbol{v}$ is an eigenvector of AB^{-1} with eigenvalue $\frac{\alpha}{\beta}$.

  This quotient is a root of the characteristic polynomial of the rational matrix AB^{-1}.

Subsection 7

Rings of Integers of Number Fields

Integers in a Number Field

Definition

Let K be a number field. Then the integers in K are

$$\mathbb{Z}_K = \{\alpha \in K : \alpha \text{ is an algebraic integer}\}.$$

- We first check that this gives the right answer for $\mathbb{Q}$.

  A rational $a \in \mathbb{Q}$ has minimal polynomial $X - a$.

  The coefficients are in $\mathbb{Z}$ if and only if $a \in \mathbb{Z}$.

  So the integers in $\mathbb{Q}$ according to the definition are indeed $\mathbb{Z}$.
- Assume, next, $K \subseteq L$ is an extension of number fields and $\alpha \in K$.

  Then α is an integer in K if and only if it is an integer in L.

  This follows simply because the condition determining whether or not α is an algebraic integer makes no reference to any field K.

The Ring of Integers of K

Corollary

Let K be a number field. Then $\mathbb{Z}_K$ is a ring.

- Suppose $\alpha, \beta \in \mathbb{Z}_K$.

  We need to check that $\alpha + \beta$, $\alpha - \beta$ and $\alpha\beta$ all lie in $\mathbb{Z}_K$.

  They certainly all lie in K.

  By a previous corollary, they are all algebraic integers.

  So they lie in $\mathbb{Z}_K$.

  Remark: $\mathbb{Z}_K$ is even an integral domain.

  Indeed $\mathbb{Z}_K \subseteq K$. As K is a field, $\mathbb{Z}_K \subseteq K$ has no zero-divisors.
- $\mathbb{Z}_K$ is called the **ring of integers** of K.

Characterization of $\mathbb{Z}_K$

- A generalization of a preceding proposition allows us to characterize the ring of integers $\mathbb{Z}_K$ as the largest subring of K which is a finitely generated $\mathbb{Z}$-module.

Proposition

Suppose R is a subring of a number field K, and that R is finitely generated as a $\mathbb{Z}$-module. Then $R \subseteq \mathbb{Z}_K$.

- Let R is a subring of a number field K.

  Suppose R is finitely generated as a $\mathbb{Z}$-module and $\alpha \in R$.

  By a previous corollary, α is the root of a monic polynomial with coefficients in $\mathbb{Z}$.

  Therefore, $\alpha \in \mathbb{Z}_K$.

Ring of Integers in $\mathbb{Q}(\sqrt{d})$

Proposition

Suppose that d is a squarefree integer (i.e., not divisible by the square of any prime). Then:

1. If $d \equiv 2$ or $3 \pmod 4$, then the ring of integers in $\mathbb{Q}(\sqrt{d})$ is
$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}.$$
2. If $d \equiv 1 \pmod 4$, then the ring of integers in $\mathbb{Q}(\sqrt{d})$ is
$$\mathbb{Z}[\rho_d] = \{a + b\rho_d : a, b \in \mathbb{Z}\},$$
where $\rho_d = \frac{1+\sqrt{d}}{2}$.

Ring of Integers in $\mathbb{Q}(\sqrt{d})$

- Let $\alpha = a + b\sqrt{d}$, with $a, b \in \mathbb{Q}$.

  Then α satisfies the equation $(X - a)^2 = b^2 d$.

  Equivalently,

  $$X^2 - 2aX + (a^2 - b^2 d) = 0.$$

  We seek conditions on a and b to make this have integer coefficients.

  This implies that $2a \in \mathbb{Z}$ and $a^2 - b^2 d \in \mathbb{Z}$.

  The first condition implies $a \in \mathbb{Z}$ or $a = \frac{A}{2}$, where A is an odd integer.

  If $a \in \mathbb{Z}$, the second condition becomes $b^2 d \in \mathbb{Z}$.

  As d is squarefree, this requires $b \in \mathbb{Z}$.

  So the set

  $$\{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$$

  is always contained in the ring of integers.

Ring of Integers in $\mathbb{Q}(\sqrt{d})$ (Cont'd)

- We examine when $a = \frac{A}{2}$, A an odd integer, can arise.
  We need $\frac{A^2}{4} - b^2 d \in \mathbb{Z}$. Equivalently, $A^2 - 4b^2 d \equiv 0 \pmod 4$.
  This certainly requires $4b^2 d \in \mathbb{Z}$.
  As d is squarefree, $2b$ must be an integer, B say.
  Further, b itself cannot be in $\mathbb{Z}$. Otherwise, $\frac{A^2}{4} - b^2 d \notin \mathbb{Z}$.
  Thus B is an odd integer.
  Then $A^2 - B^2 d \equiv 0 \pmod 4$, with A and B odd integers.
  But the squares of odd numbers are all $1 \pmod 4$.
  Thus, $1 - d \equiv 0 \pmod 4$.
  - If $d \equiv 1 \pmod 4$, the second case can arise. The integers are
    $$\{a + b\sqrt{d} : \text{either } a, b \in \mathbb{Z}, \text{ or both } a \text{ and } b \text{ are halves of odd integers}\}.$$
    This set is easily seen to be the same as that of the statement.
  - If $d \not\equiv 1 \pmod 4$, then the only integers are $\{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$.

Remarks on the Ring of Integers of $\mathbb{Q}(\sqrt{d})$

- If $d = -1$, so that $d \equiv 3 \pmod 4$, this result shows that the ring of integers of $\mathbb{Q}(i)$ is $\mathbb{Z}[i]$.
- The ring of integers of $\mathbb{Q}(\sqrt{d})$ is not always just $\mathbb{Z}[\sqrt{d}]$.

  Although every element in $\mathbb{Z}[\sqrt{d}]$ is an algebraic integer, there are sometimes additional integers.

  Examples:
  - If $d = -3$, then $\frac{-1+\sqrt{-3}}{2}$ is an integer.

    It it is a root of $X^2 + X + 1$.
  - If $d = 5$, then $\frac{1+\sqrt{5}}{2}$ is an integer.

    It is a root of $X^2 - X - 1$.