Introduction to Algebraic Number Theory

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 500

Subsection 1

Embeddings

Introducing Conjugates of Algebraic Numbers

- Suppose that K is a number field and that $[K:\mathbb{Q}] = n$.
- By a previous corollary, there exists $\gamma \in K$, such that $K = \mathbb{Q}(\gamma)$.
- Let f denote the minimal polynomial of γ over $\mathbb{Q}$.
- By a previous corollary, f has degree n.
- Now $\mathbb{C}$ is algebraically closed.
- So we can factor $f(X)$ completely over $\mathbb{C}$.
- That is, if $\gamma_1, \ldots, \gamma_n \in \mathbb{C}$ are the (complex) roots of f,

$$f(X) = \prod_{i=1}^{n} (X - \gamma_i).$$

One of these is γ itself, so we will assume $\gamma_1 = \gamma$.

Conjugates of Algebraic Numbers

Definition

If $\gamma \in K$ has $f(X) \in \mathbb{Q}[X]$ as its minimal polynomial as above, then the roots $\gamma_1, \ldots, \gamma_n$ are the **conjugates** of γ.

- Conjugate elements have the same minimal polynomial.
- Indeed, $\gamma_1, \ldots, \gamma_n$ are all roots of the monic irreducible polynomial f.
- So f is the minimal polynomial for each of them.
- By a previous lemma, the conjugates of an algebraic number are all distinct.

Algebraic Conjugates and Complex Conjugates

Example: Suppose that $\alpha = i$.

Then its minimal polynomial is $X^2 + 1$.

The two complex roots of this are $\pm i$.

Thus, the two conjugates of i are i and $-i$.

Claim: Suppose that $\alpha = a + bi \in \mathbb{Q}(i)$.

Then its conjugates (in the sense above) are just α and $\overline{\alpha}$.

- Thus, the conjugates of a complex number (in this sense) are the same as the conjugates (in the familiar sense).

A Mild Generalization

- The concept of conjugacy generalizes somewhat.
- Let $L \subseteq K$ be an extension of fields.
- Suppose $\alpha \in K$ has minimal polynomial $f(X) \in L[X]$ over L.
- Then the **conjugates of α over L** are the roots of f.

Homomorphisms Induced by Conjugates

- Suppose $K = \mathbb{Q}(\gamma)$.
- Then, given any element of K, we can write it as a polynomial expression in γ with coefficients in $\mathbb{Q}$.
- For each $k = 1, \ldots, n$, consider the map

$$\sigma_k : \gamma \mapsto \gamma_k.$$

- This map induces a field homomorphism

$$\sigma_k : \mathbb{Q}(\gamma) \to \mathbb{Q}(\gamma_k) \subseteq \mathbb{C};$$
$$\sum_{i=0}^{n-1} x_i \gamma^i \mapsto \sum_{i=0}^{n-1} x_i \gamma_k^i.$$

Homomorphisms Are Well-Defined

- The map σ_k is well-defined.

  That is, if the same element of $\mathbb{Q}(\gamma)$ can be written in two different ways as a polynomial expression of γ, then applying σ_k to either expression gives the same answer.

  Suppose $g_1(\gamma) = g_2(\gamma)$.

  Then γ is a root of $g_1 - g_2$.

  So the minimal polynomial of γ divides $g_1 - g_2$.

  But this minimal polynomial is just f.

  Now γ_k is also a root of f.

  Thus, $f(\gamma_k) = 0$.

  So $g_1(\gamma_k) = g_2(\gamma_k)$.

Injectivity of Conjugate Homomorphisms

Claim: All maps σ_i are injective.

Suppose $g_1(\gamma)$ and $g_2(\gamma)$ are two elements of $K = \mathbb{Q}(\gamma)$, such that

$$\sigma_k(g_1(\gamma)) = \sigma_k(g_2(\gamma)).$$

By definition of σ_k, $g_1(\gamma_k) = g_2(\gamma_k)$.

So γ_k must be a root of $g_1 - g_2$.

Therefore, the minimal polynomial of γ_k divides $g_1 - g_2$.

But this minimal polynomial is exactly f.

So $f \mid g_1 - g_2$. Hence, $g_1(\gamma) = g_2(\gamma)$.

Definition

An **embedding** means an injective field homomorphism.

- Thus, $\sigma_1, \ldots, \sigma_n$ are all embeddings.

Embeddings of a Number Field into $\mathbb{C}$

Proposition

If K is a number field of degree n, then the maps $\sigma_1,\ldots,\sigma_n$ are all of the n distinct field embeddings $K \to \mathbb{C}$.

- The arguments just given show that they are all well-defined injective field homomorphisms.

  Conversely, suppose $\sigma : K \to \mathbb{C}$ is a field homomorphism and $K = \mathbb{Q}(\gamma)$.

  Then σ must be determined by its effect on γ, as

$$\sigma\left(\sum_{i=0}^{n-1} x_i \gamma^i\right) = \sum_{i=0}^{n-1} x_i \sigma(\gamma)^i.$$

Embeddings of a Number Field into $\mathbb{C}$ (Cont'd)

- Now apply σ to the equality $f(\gamma) = 0$ to get

$$f(\sigma(\gamma)) = \sigma(f(\gamma)) = \sigma(0) = 0.$$

So $\sigma(\gamma)$ is a root of f.

This shows that $\sigma(\gamma) = \gamma_k$, for some k.

It is then clear that $\sigma = \sigma_k$.

Example

- Consider the field $K = \mathbb{Q}(i)$.
- We have already seen that the conjugates of i are i and $-i$.
- So we get two embeddings from K into $\mathbb{C}$, given by

$$\begin{aligned} \sigma_1(a+bi) &= a+bi; \\ \sigma_2(a+bi) &= a-bi. \end{aligned}$$

- This gives us two ways to think of $\mathbb{Q}(i)$ as a subfield of $\mathbb{C}$.

Remark

- It is sometimes important when writing $\mathbb{Q}(\sqrt{2})$, say, to keep in mind that:
  - The element "$\sqrt{2}$" should be regarded as just an abstract square root of 2;
  - This element is not necessarily to be identified with the positive real number $1.4142\ldots$.
- We are writing $\mathbb{Q}(\sqrt{2})$ as a shorthand for

$$\text{"}\mathbb{Q}(\alpha) \text{ where } \alpha \text{ is some number with } \alpha^2 = 2\text{".}$$

- Choosing an embedding from $\mathbb{Q}(\sqrt{2})$ into $\mathbb{C}$ is tantamount to identifying the abstract element $\sqrt{2}$ with the particular number $1.4142\ldots$ or $-1.4142\ldots$.

Extending Embeddings into $\mathbb{C}$ to Field Extensions

Proposition

Suppose that $K \subseteq L$ is a finite extension of fields, and that we have a fixed embedding $\iota : K \to \mathbb{C}$. Then there are $[L : K]$ ways to extend the embedding ι to an embedding $L \to \mathbb{C}$ (that is, to define embeddings $L \to \mathbb{C}$ which agree with ι on the elements of L that belong to K).

- By the Theorem of the Primitive Element, we can write $L = K(\gamma)$, where γ has minimal polynomial over K of degree $n = [L : K]$.

  Let $\gamma_1, \ldots, \gamma_n$ denote the roots of the minimal polynomial.

  Define extensions $\sigma_k : L \to \mathbb{C}$ by insisting that

$$\sigma_k\left(\sum_{i=0}^{n-1} x_i \gamma^i\right) = \sum_{i=0}^{n-1} \iota(x_i)\gamma_k^i.$$

  The verification that these are all the embeddings is then identical to the previous arguments.

Example

- Suppose that K is a number field, and that $\alpha \in K$.
- We look at the images of α under each of the embeddings.

Example: Suppose that $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, and that $\alpha = \sqrt{6}$.

The embeddings from K into $\mathbb{C}$ are given by:

$$\begin{array}{rcl} \sigma_1(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) & = & a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}; \\ \sigma_2(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) & = & a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6}; \\ \sigma_3(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) & = & a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}; \\ \sigma_4(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) & = & a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6}. \end{array}$$

Then

$$\sigma_1(\sqrt{6}) = \sigma_4(\sqrt{6}) = \sqrt{6},$$
$$\sigma_2(\sqrt{6}) = \sigma_3(\sqrt{6}) = -\sqrt{6}.$$

These images are just the conjugates of $\sqrt{6}$, but each occurs twice.

Degree of a Tower of Extensions

Theorem

Suppose that $K \subseteq L \subseteq M$ is a "tower" of fields. Assume M is a finite extension of L, and L is a finite extension of K. Then we have

$$[M:K] = [M:L][L:K].$$

- Suppose that $[M:L] = m$ and $[L:K] = n$.
  Then the following hold.
  - There are elements $\omega_1, \ldots, \omega_n$, such that every element of L is a linear combination of $\omega_1, \ldots, \omega_n$, with coefficients in K;
  - There are elements $\theta_1, \ldots, \theta_m$, such that every element of M is a linear combination of $\theta_1, \ldots, \theta_m$, with coefficients in L.

Degree of a Tower of Extensions (Cont'd)

Claim: $\{\theta_i\omega_j\}$ is a basis for M as a K-vector space.

Let $\mu \in M$.

Express it first as a linear combination of

$$\theta_1, \ldots, \theta_m,$$

with coefficients in L.

Then express each of these coefficients as linear combinations of

$$\omega_1, \ldots, \omega_n,$$

with coefficients in K.

This shows that μ can be written as a linear combination of $\{\theta_i\omega_j\}$, with coefficients in K.

Degree of a Tower of Extensions (Cont'd)

Claim: These $\{\theta_i\omega_j\}$ form a linearly independent set.
To see this, we take a linear combination which is 0,

$$\alpha_{11}\theta_1\omega_1+\alpha_{12}\theta_1\omega_2+\cdots+\alpha_{1n}\theta_1\omega_n+\alpha_{21}\theta_2\omega_1+\cdots+\alpha_{mn}\theta_m\omega_n=0.$$

Rearrange this as

$$(\alpha_{11}\omega_1+\cdots+\alpha_{1n}\omega_n)\theta_1+\cdots+(\alpha_{m1}\omega_1+\cdots+\alpha_{mn}\omega_n)\theta_m=0.$$

Now this is a linear combination of $\theta_1,\ldots,\theta_m$ with coefficients in L.
Since they form a basis, each of the coefficients must vanish,

$$\alpha_{i1}\omega_1+\cdots+\alpha_{in}\omega_n=0, \text{ for all } i.$$

Now $\omega_1,\ldots,\omega_n$ forms a basis for L as a vector space over K.
So we again conclude that each $\alpha_{ij}=0$.
Thus, $\{\theta_i\omega_j\}$ form a basis for M over K.
It follows that $[M:K]=mn$.

The Degree d_α and r_α

- Consider a number field K of degree n over $\mathbb{Q}$.
- Suppose $\alpha \in K$ with minimal polynomial $g(X) \in \mathbb{Q}[X]$.
- Then α generates a field $\mathbb{Q}(\alpha)$ contained in K.
- If g has degree d_α, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d_\alpha$.
- Suppose that the conjugates of α are written

$$\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_{d_\alpha}.$$

- Form the tower of fields $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq K$.
- We know that

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

- So we see that $d_\alpha \mid n$.
- Write $r = r_\alpha$ for $\frac{n}{d_\alpha}$.

Images of α under the σ_i's

Proposition

The images $\sigma_i(\alpha)$ are the conjugates $\{\alpha_1,\ldots,\alpha_{d_\alpha}\}$, each occurring with multiplicity r_α.

- We have extension fields $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq K$.

  By a previous proposition, we know that there are d_α embeddings

  $$\iota_k : \mathbb{Q}(\alpha) \to \mathbb{C}.$$

  The embedding ι_k is determined by the property that $\iota_k(\alpha) = \alpha_k$.

  Choose any of these embeddings $\iota_k : \mathbb{Q}(\alpha) \to \mathbb{C}$.

  The extension $\mathbb{Q}(\alpha) \subseteq K$ has degree r_α.

  By a previous proposition, the embedding ι_k extends to an embedding $K \to \mathbb{C}$ in r_α ways.

Images of α under the σ_i's (Cont'd)

- By definition of an extension, each extension of ι_k maps α to α_k.

  We can perform this extension for each of the d_α embeddings ι_k.

  In this way each embedding is extended in r_α ways.

  We thus obtain $d_\alpha r_\alpha = n$ embeddings from K to $\mathbb{C}$.

  But there are exactly n embeddings from K into $\mathbb{C}$.

  Thus, all of the embeddings $\sigma_i : K \to \mathbb{C}$ have been obtained.

  Moreover, as we have seen, α is taken to each of its conjugates $\{\alpha_1, \ldots, \alpha_{d_\alpha}\}$ with multiplicity r_α.

The Product with Factors $X - \sigma_k(\alpha)$

Corollary

Suppose α in K has minimal polynomial g of degree d_α, and that $r_\alpha = \frac{n}{d_\alpha}$. Then

$$\prod_{i=1}^{n}(X - \sigma_k(\alpha)) = g(X)^{r_\alpha}.$$

- Both sides are monic polynomials with the same roots.

Subsection 2

Norms and Traces

Multiplication by α

- Let K be a number field, with $[K:\mathbb{Q}] = n$.
- Suppose that $\alpha \in K$.
- Multiplication by α gives a map

$$m_\alpha : K \to K; \qquad x \mapsto \alpha x.$$

Claim: This map is $\mathbb{Q}$-linear.

It is easy to see that, for $x, x' \in K$ and $t \in \mathbb{Q}$,

$$\begin{aligned} m_\alpha(x+x') &= \alpha(x+x') = \alpha x + \alpha x' = m_\alpha(x) + m_\alpha(x'); \\ m_\alpha(tx) &= \alpha(tx) = t(\alpha x) = t m_\alpha(x). \end{aligned}$$

- The map is even K-linear, since $m_\alpha(tx) = t m_\alpha(x)$, for $t \in K$.

Trace and Norm of an Element in a Number Field

- Choose a basis for K over $\mathbb{Q}$.
- Then the map m_α is represented by an $n \times n$-matrix.
- We define:
  - The **trace** of α, written $T_{K/\mathbb{Q}}(\alpha)$, to be the trace of this matrix;
  - The **norm** of α, written $N_{K/\mathbb{Q}}(\alpha)$, to be the determinant of the matrix.
- Choosing a different basis would give a conjugate $n \times n$-matrix representing the map.
- By a result in Linear Algebra, the trace and determinant of an endomorphism do not depend on the choice of basis.
- When the field K is clearly understood, we may simply write $N(\alpha)$ and $T(\alpha)$ for the norm and trace.
- If L/K is an extension of number fields, there is an analogous notion of $T_{L/K}$ and $N_{L/K}$.

Example

- Suppose that $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and take $\alpha = \sqrt{2} + \sqrt{3}$.
  Choose a basis $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ for K.
  Multiplying by α has the following effect,

$$\alpha(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = (2b + 3c) + (a + 3d)\sqrt{2} + (a + 2d)\sqrt{3} + (b + c)\sqrt{6}.$$

Interpreted as a map on coefficients $\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \mapsto \begin{pmatrix} 2b + 3c \\ a + 3d \\ a + 2d \\ b + c \end{pmatrix}$.

This is the map given by multiplication by $\begin{pmatrix} 0 & 2 & 3 & 0 \\ 1 & 0 & 0 & 3 \\ 1 & 0 & 0 & 2 \\ 0 & 1 & 1 & 0 \end{pmatrix}$.

The trace is the sum of the diagonal entries, which is 0.

The norm of α is the determinant of the matrix, which is 1.

Min Polynomial of α and Characteristic Polynomial of m_α

Proposition

Suppose that α is an algebraic number with minimal polynomial $g(X) \in \mathbb{Q}[X]$. Form the map m_α as above. Then the characteristic polynomial of the matrix of m_α is $g(X)$.

- Suppose the min polynomial for α is given by $x^n + c_1 x^{n-1} + \cdots + c_n = 0$.

  We can compute the characteristic polynomial after choosing a basis.

  A basis for $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ is $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$, where α has degree n.

  Note that:

$$\begin{array}{rcl} \alpha \cdot \alpha^k & = & \alpha^{k+1}, \quad k = 0, \ldots, n-2, \\ \alpha \cdot \alpha^{n-1} & = & \alpha^n \\ & = & -c_1 \alpha^{n-1} - \cdots - c_n. \end{array}$$

Min Polynomial of α and Characteristic of m_α (Cont'd)

- So the map m_α is given by

$$\begin{aligned} m_\alpha(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}) & \\ &= \alpha(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}) \\ &= a_0\alpha + \cdots + a_{n-2}\alpha^{n-1} + a_{n-1}\alpha^n \\ &= a_0\alpha + \cdots + a_{n-2}\alpha^{n-1} + a_{n-1}(-c_1\alpha^{n-1} - \cdots - c_n) \\ &= -a_{n-1}c_n + (a_0 - a_{n-1}c_{n-1})\alpha + \cdots + (a_{n-2} - a_{n-1}c_1)\alpha^{n-1}. \end{aligned}$$

Min Polynomial of α and Characteristic of m_α (Cont'd)

- So the map of m_α using this basis is given by
$$\begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} \mapsto \begin{pmatrix} -a_{n-1}c_n \\ a_0 - a_{n-1}c_{n-2} \\ \vdots \\ a_{n-2} - a_{n-1}c_1 \end{pmatrix}.$$
This is the same as multiplication by the matrix
$$\begin{pmatrix} & & & & -c_n \\ 1 & & & & -c_{n-1} \\ & 1 & & & -c_{n-2} \\ & & \ddots & & \vdots \\ & & & 1 & -c_1 \end{pmatrix}.$$
It is easy to check that this matrix has characteristic polynomial given by $x^n + c_1 x^{n-1} + \cdots + c_n = 0$.

The Norm and the Trace are Rational

Lemma

Suppose $\alpha \in K$. Then $N_{K/\mathbb{Q}}(\alpha)$ and $T_{K/\mathbb{Q}}(\alpha)$ are both in $\mathbb{Q}$.

- This simply follows because they are the trace and determinant of a matrix with entries in $\mathbb{Q}$.

Norm, Trace and Embeddings

Proposition

Write $\sigma_1,\ldots,\sigma_n$ for the embeddings of K into $\mathbb{C}$. If $\alpha\in K$, then

$$N_{K/\mathbb{Q}}(\alpha)=\prod_{k=1}^n\sigma_k(\alpha)\quad\text{and}\quad T_{K/\mathbb{Q}}(\alpha)=\sum_{k=1}^n\sigma_k(\alpha).$$

- Let g denote the minimal polynomial of α over $\mathbb{Q}$.

  $\mathbb{Q}(\alpha)$ may be smaller than K (e.g., we might even have $\alpha\in\mathbb{Q}$).

  So the degree of g may be strictly smaller than n.

  As g is irreducible, $[\mathbb{Q}(\alpha):\mathbb{Q}]=\deg g$, written d_α.

  We have field extensions $\mathbb{Q}\subseteq\mathbb{Q}(\alpha)\subseteq K$.

  Let $\{\beta_1,\ldots,\beta_{r_\alpha}\}$ be a basis for K over $\mathbb{Q}(\alpha)$, $[K:\mathbb{Q}(\alpha)]=r_\alpha=\frac{n}{d_\alpha}$.

  Clearly $\{1,\alpha,\ldots,\alpha^{d_\alpha-1}\}$ is a basis for $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$.

Properties of Norm and Trace (Cont'd)

- Now the set $\{\beta_i\alpha^j : 1 \leq i \leq r_\alpha, 0 \leq j < d_\alpha\}$ forms a basis for K over $\mathbb{Q}$.

  Choose this basis, and fix one of the β_i.

  Consider the map m_α on the block spanned by $\{\beta_i, \beta_i\alpha, \ldots, \beta_i\alpha^{d_\alpha - 1}\}$.

  The matrix of this map on this block is the same for all choices of β_i.

  It is the same as the matrix of the map m_α on $\mathbb{Q}(\alpha)$, where we use the basis $\{1, \alpha, \ldots, \alpha^{d_\alpha - 1}\}$.

  We have seen that this matrix has characteristic polynomial g.

  So the characteristic polynomial of m_α on K is given by $g(X)^{r_\alpha}$.

  But the roots of g, by definition, are exactly the conjugates of α.

  So the roots of $g(X)^{r_\alpha}$ are the conjugates of α, with multiplicities r_α.

  By the proposition, these are exactly the images of α under all the embeddings $\sigma_i : K \to \mathbb{C}$.

  The result now follows.

Norms and Traces of Algebraic Integers

Corollary

Suppose $\alpha \in \mathbb{Z}_K$. Then $N_{K/\mathbb{Q}}(\alpha)$ and $T_{K/\mathbb{Q}}(\alpha)$ are both in $\mathbb{Z}$.

- By hypothesis, $\alpha \in \mathbb{Z}_K$.

  So its minimal polynomial $g(X) \in \mathbb{Z}[X]$.

  Therefore, $g(X)^{r_\alpha} \in \mathbb{Z}[X]$.

  This implies that the product

$$\prod_{i=1}^{n}(X - \sigma_i(\alpha)) \in \mathbb{Z}[X].$$

  The constant coefficient of this polynomial is $(-1)^n N_{K/\mathbb{Q}}(\alpha)$.

  In addition, the coefficient of X^{n-1} is $-T_{K/\mathbb{Q}}(\alpha)$.

Subsection 3

The Discriminant

The Discriminant

- Suppose that K is a number field of degree n over $\mathbb{Q}$.
- We saw this means that:
    1. K is generated over $\mathbb{Q}$ by n elements (the definition of the degree);
    2. There are n embeddings $\sigma_1,\ldots,\sigma_n$ from K into $\mathbb{C}$.
- Suppose that $\{\omega_1,\ldots,\omega_n\}$ lie in K.
- For the moment, we will not assume that these form a basis.
- Consider the matrix:

$$M = \begin{pmatrix} \sigma_1(\omega_1) & \sigma_1(\omega_2) & \cdots & \sigma_1(\omega_n) \\ \sigma_2(\omega_1) & \sigma_2(\omega_2) & \cdots & \sigma_2(\omega_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\omega_1) & \sigma_n(\omega_2) & \cdots & \sigma_n(\omega_n) \end{pmatrix}.$$

The Discriminant (Cont'd)

- We will use the determinant of M as a measure of how "widely spaced" the set $\{\omega_1, \ldots, \omega_n\}$ is.
- The determinant of M is defined only up to sign.
- So we use its square.

Definition

Define the **discriminant** of $\{\omega_1, \ldots, \omega_n\}$ to be

$$\Delta\{\omega_1, \ldots, \omega_n\} = (\det M)^2.$$

A Discriminant Formula

Lemma

With the notation as above, form the matrix T, where

$$T_{ij} = T_{K/\mathbb{Q}}(\omega_i \omega_j).$$

Then $\Delta\{\omega_1, \ldots, \omega_n\} = \det T$.

- Simply notice that $\det M = \det M^t$. So

$$\Delta\{\omega_1, \ldots, \omega_n\} = (\det M)^2 = \det(M^t M).$$

But

$$\begin{aligned} (M^t M)_{ij} &= \sum_{k=1}^{n} M_{ik}^t M_{kj} = \sum_{k=1}^{n} M_{ki} M_{kj} \\ &= \sum_{k=1}^{n} \sigma_k(\omega_i)\sigma_k(\omega_j) = \sum_{k=1}^{n} \sigma_k(\omega_i \omega_j). \end{aligned}$$

By a previous proposition, this is equal to $T_{K/\mathbb{Q}}(\omega_i \omega_j)$.

Discriminant of Algebraic Integers

Corollary

Suppose that $\{\omega,\ldots,\omega_n\}$ consists of elements of $\mathbb{Z}_K$. Then

$$\Delta\{\omega_1,\ldots,\omega_n\} \in \mathbb{Z}.$$

- Suppose each $\omega_i \in \mathbb{Z}_K$.

  $\mathbb{Z}_K$ is closed under multiplication.

  So $\omega_i\omega_j \in \mathbb{Z}_K$.

  By a previous corollary, $T_{K/\mathbb{Q}}(\omega_i\omega_j) \in \mathbb{Z}$.

  So, by the lemma, $\Delta\{\omega_1,\ldots,\omega_n\}$ is the determinant of a matrix with entries in $\mathbb{Z}$.

  Thus, $\Delta\{\omega_1,\ldots,\omega_n\}$ is itself in $\mathbb{Z}$.

Example

- Let $K = \mathbb{Q}(\gamma)$, for some γ.
  One natural basis for K over $\mathbb{Q}$ is $\{1, \gamma, \gamma^2, \ldots, \gamma^{n-1}\}$.
  As usual, write $\gamma_1, \ldots, \gamma_n$ for the conjugates of γ.
  Then the discriminant $\Delta\{1, \gamma, \gamma^2, \ldots, \gamma^{n-1}\}$ is given by

$$\begin{vmatrix} 1 & \gamma_1 & \cdots & \gamma_1^{n-1} \\ 1 & \gamma_2 & \cdots & \gamma_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \gamma_n & \cdots & \gamma_n^{n-1} \end{vmatrix}^2.$$

  This is a Vandermonde determinant, which is equal to

$$\prod_{i<j} (\gamma_i - \gamma_j)^2.$$

  We saw that the conjugates of γ are distinct.
  So the discriminant $\Delta\{1, \gamma, \gamma^2, \ldots, \gamma^{n-1}\}$ is nonzero.

Discriminant of the Minimal Polynomial

- Let $K = \mathbb{Q}(\gamma)$, for some γ.
- Suppose $f(X)$ is the minimal polynomial of γ.
- Then its roots are the conjugates $\gamma_1, \ldots, \gamma_n$ of γ.
- Define the **discriminant of** $f(X)$ to be exactly

$$\prod_{i<j} (\gamma_i - \gamma_j)^2.$$

- By the example, the discriminant of $f(X)$ coincides with the discriminant $\Delta\{1, \gamma, \ldots, \gamma^{n-1}\}$.

Relations Between Discriminants

Proposition

Suppose that the elements of two sets $\{\omega_1,\ldots,\omega_n\}$ and $\{\omega'_1,\ldots,\omega'_n\}$ are related by

$$\omega'_i = c_{1i}\omega_1 + \cdots + c_{ni}\omega_n$$

for rational numbers $c_{ij} \in \mathbb{Q}$. Write C for the matrix (c_{ij}). Then

$$\Delta\{\omega'_1,\ldots,\omega'_n\} = (\det C)^2 \Delta\{\omega_1,\ldots,\omega_n\}.$$

Relations Between Discriminants (Cont'd)

- Set
$$M' = \begin{pmatrix} \sigma_1(\omega'_1) & \sigma_1(\omega'_2) & \cdots & \sigma_1(\omega'_n) \\ \sigma_2(\omega'_1) & \sigma_2(\omega'_2) & \cdots & \sigma_2(\omega'_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\omega'_1) & \sigma_n(\omega'_2) & \cdots & \sigma_n(\omega'_n) \end{pmatrix}.$$
Then
$$\Delta\{\omega'_1,\ldots,\omega'_n\} = (\det M')^2.$$
σ_k is a homomorphism, which is the identity on rational numbers.
It follows that
$$\sigma_k(\omega'_i) = c_{1i}\sigma_k(\omega_1) + \cdots + c_{ni}\sigma_k(\omega_n).$$
It is easy to see that this implies that $M' = CM$, where $C = (c_{ij})$.
The result now follows from the multiplicativity of the determinant.

Bases have Nonzero Discriminants

Proposition

Suppose that $\{\omega_1, \ldots, \omega_n\}$ is a basis for K over $\mathbb{Q}$. Then

$$\Delta\{\omega_1, \ldots, \omega_n\} \neq 0.$$

- As usual, write $K = \mathbb{Q}(\gamma)$, for some element $\gamma \in K$.

  Then $\{1, \gamma, \ldots, \gamma^{n-1}\}$ is a basis for K over $\mathbb{Q}$.

  We can write the basis $\{\omega_1, \ldots, \omega_n\}$ in terms of $\{1, \gamma, \ldots, \gamma^{n-1}\}$ as

$$\omega_i = c_{1i}1 + c_{2i}\gamma + \cdots + c_{ni}\gamma^{n-1}.$$

Bases have Nonzero Discriminants (Cont'd)

Claim: Since $\{\omega_1,\ldots,\omega_n\}$ is also a basis, we have $\det(c_{ij}) \neq 0$.

Suppose $\{\omega_1,\ldots,\omega_n\}$ is a basis.

We can write

$$\gamma^{i-1} = c'_{1i}\omega_1 + c'_{2i}\omega_2 + \cdots + c'_{ni}\omega_n.$$

for some c'_{ij}.

Write $C = (c_{ij})$ and $C' = (c'_{ij})$.

We can see that this implies that $C'C = I$.

Hence C and C' are invertible.

The previous proposition shows that

$$\Delta\{\omega_1,\ldots,\omega_n\} = (\det(c_{ij}))^2 \Delta\{1,\gamma,\ldots,\gamma^{n-1}\}.$$

The result follows.

Characterization of Bases

Proposition

The set $\{\omega_1,\ldots,\omega_n\}$ is a basis for K over $\mathbb{Q}$ if and only if $\Delta\{\omega_1,\ldots,\omega_n\} \neq 0$.

- We have already seen that the discriminant of a basis is nonzero.

  Conversely, suppose $\{\omega_1,\ldots,\omega_n\}$ are linearly dependent over $\mathbb{Q}$.

  Then $x_1\omega_1 + \cdots + x_n\omega_n = 0$, for some $x_1,\ldots,x_n \in \mathbb{Q}$, not all zero.

  Apply the embedding σ_k to this equality.

  Since σ is a field homomorphism fixing each element of $\mathbb{Q}$,

  $$x_1\sigma_k(\omega_1) + \cdots + x_n\sigma_k(\omega_n) = 0.$$

  We get a linear dependency between the columns of the matrix M, with $M_{ij} = \sigma_i(\omega_j)$. So $\det M = 0$.

  Thus, $\Delta\{\omega_1,\ldots,\omega_n\} = 0$, as required.

Real and Complex Embeddings

- Some of the n embeddings may map K into the real numbers $\mathbb{R} \subset \mathbb{C}$.
- We call these **real embeddings**.
- The other embeddings occur in complex conjugate pairs.
- I.e., if $\sigma : K \to \mathbb{C}$ is an embedding, then so is $\overline{\sigma}$, where

$$\overline{\sigma}(\omega) = \overline{\sigma(\omega)}.$$

- So **complex embeddings** occur as complex conjugate pairs.
- Denote by:
  - r_1 the number of real embeddings of K into $\mathbb{C}$;
  - r_2 the number of complex conjugate pairs of embeddings.

Measuring the Spacing of $\{\omega_1,\ldots,\omega_n\}$

- Since there are n embeddings in total, we have
$$r_1+2r_2=n.$$
- Every pair $(\sigma,\overline{\sigma})$ of complex embeddings together map K into $\mathbb{C}^2$.
- The image is actually contained in a real 2-dimensional subspace.

  Indeed, suppose
$$\sigma(\omega)=a+bi.$$
  Then
$$\overline{\sigma}(\omega)=a-bi.$$
  So the real and imaginary parts of $\overline{\sigma}(\omega)$ are already determined by the real and imaginary parts of $\sigma(\omega)$.
- So we get that:
  - Each real embedding maps K into $\mathbb{R}\subset\mathbb{C}$;
  - Each pair of complex embeddings map K into a 2-dimensional real subspace of $\mathbb{C}^2$.

Measuring the Spacing of $\{\omega_1,\ldots,\omega_n\}$ (Cont'd)

- We conclude that the collection of all embeddings
$$\iota=(\sigma_1,\ldots,\sigma_n)$$
maps K into a real subspace V of $\mathbb{C}^n$ of real dimension n.
- Given our set $\{\omega_1,\ldots,\omega_n\}$, the image of
$$\mathbb{Z}\iota(\omega_1)+\cdots+\mathbb{Z}\iota(\omega_n)$$
is contained in this subspace V.
  - When the set is not a basis, the image will lie in a subspace of V of strictly smaller dimension.
    In this case the discriminant will vanish.
  - If the set is a basis, the discriminant will measure the volume of a fundamental region for the image.
    Thus, it will measure how sparsely these points are spaced.

Subsection 4

Integral Bases

Integral Bases of $\mathbb{Z}_K$

- We say that the set $\{\omega_1,\ldots,\omega_n\}$ is an **integral basis** for the ring of integers $\mathbb{Z}_K$ if every element of $\mathbb{Z}_K$ is uniquely expressible as a $\mathbb{Z}$-linear combination of elements of the set.

  Example: We have looked at integral bases for quadratic fields.

  Suppose $K=\mathbb{Q}(\sqrt{d})$, with d a squarefree integer.

  Assume, first, that $d \equiv 1 \pmod 4$.

  Then
  $$\mathbb{Z}_K=\mathbb{Z}+\mathbb{Z}\frac{1+\sqrt{d}}{2}.$$

  So an integral basis is $\{1,\frac{1+\sqrt{d}}{2}\}$.

  Assume, next, that $d \equiv 2 \pmod 4$ or $d \equiv 3 \pmod 4$.

  Then
  $$\mathbb{Z}_K=\mathbb{Z}+\mathbb{Z}\sqrt{d}.$$

  So an integral basis is $\{1,\sqrt{d}\}$.

Free Abelian Groups of Rank n and Bases

- It is not obvious that integral bases exist.
- We will show that they do for all number fields K.
- Equivalently, we will prove that the ring of integers of K is a free abelian group of rank $n = [K : \mathbb{Q}]$.
- Recall that a **free abelian group A of rank n** is one which is the direct sum of n subgroups, each infinite cyclic (so isomorphic to $\mathbb{Z}$).
- Then
$$A \cong \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n.$$
- So every element of A can be expressed uniquely as
$$x_1\omega_1 + \cdots + x_n\omega_n, \quad x_i \in \mathbb{Z}.$$
- This is exactly the property required of an integral basis.

Existence of Integral Bases

- Suppose that $[K:\mathbb{Q}]=n$.
- Then we can choose a basis $\{\omega_1,\ldots,\omega_n\}$ for K over $\mathbb{Q}$.
- Thus, every element of K can be written $x_1\omega_1+\cdots+x_n\omega_n$, for $x_i\in\mathbb{Q}$.

Theorem

Let K be a number field. Then the ring of integers $\mathbb{Z}_K$ has an integral basis.

- Given any basis, we can replace each element in our basis with a nonzero multiple so that every basis element is in $\mathbb{Z}_K$.

  We also know that the discriminant of every basis consisting of elements of $\mathbb{Z}_K$ is an integer.

Existence of Integral Bases (Cont'd)

- Choose a basis
$$\{\omega_1, \ldots, \omega_n\},$$
consisting of elements of $\mathbb{Z}_K$, with $|\Delta\{\omega_1, \ldots, \omega_n\}|$ as small as possible.
This can be done since $\Delta\{\omega_1, \ldots, \omega_n\}$ is a positive integer.
Claim: This set is indeed an integral basis for K.
Suppose, to the contrary, that this does not hold.
Then there would be $\omega \in \mathbb{Z}_K$ whose expression in terms of this basis
$$\omega = x_1\omega_1 + \cdots + x_n\omega_n$$
has coefficients which are in $\mathbb{Q}$, but not all in $\mathbb{Z}$.
Reorder the basis elements, if necessary, so that $x_1 \notin \mathbb{Z}$.
Then we can choose $a_1 \in \mathbb{Z}$, with
$$|x_1 - a_1| \le \frac{1}{2}.$$

Existence of Integral Bases (Cont'd)

- Define
$$\omega_1' = \omega - a_1\omega_1 = (x_1 - a_1)\omega_1 + x_2\omega_2 + \cdots + x_n\omega_n.$$
As $\omega \in \mathbb{Z}_K$, $\omega_1 \in \mathbb{Z}_K$, and $a_1 \in \mathbb{Z}$, we have $\omega_1' \in \mathbb{Z}_K$.
Define also
$$\omega_2' = \omega_2, \ldots, \omega_n' = \omega_n.$$
Then $\{\omega_1', \ldots, \omega_n'\}$ is another basis.
It is easy to see that each of the elements of both sets can be expressed as a linear combination of the other (recall that $x_1 - a_1 \neq 0$).
Apply a previous proposition to change bases.

Existence of Integral Bases (Cont'd)

- The change of basis matrix from $\{\omega_1,\ldots,\omega_n\}$ to $\{\omega'_1,\ldots,\omega'_n\}$, is given by

$$C=\begin{pmatrix} x_1-a_1 & x_2 & x_3 & \cdots & x_n \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}.$$

A previous proposition gives

$$\Delta\{\omega'_1,\ldots,\omega'_n\}=(x_1-a_1)^2\Delta\{\omega_1,\ldots,\omega_n\}.$$

But $|x_1-a_1|\le\frac{1}{2}$.
So this means that

$$\Delta\{\omega'_1,\ldots,\omega'_n\}<\Delta\{\omega_1,\ldots,\omega_n\}.$$

This contradicts the minimality of the discriminant of $\{\omega_1,\ldots,\omega_n\}$.

Discriminants of Two Integral Bases

- We saw that integral bases exist.
- In addition, the ring of integers of a number field of degree n is a free abelian group of rank n.

Proposition

If $\{\omega_1, \ldots, \omega_n\}$ and $\{\omega'_1, \ldots, \omega'_n\}$ are two integral bases for a number field K, then

$$\Delta\{\omega'_1, \ldots, \omega'_n\} = \Delta\{\omega_1, \ldots, \omega_n\}.$$

- Suppose $\{\omega_1, \ldots, \omega_n\}$ and $\{\omega'_1, \ldots, \omega'_n\}$ are two integral bases.

  Then each element of the second can be written as an integral linear combination of those in the first,

$$\omega'_i = c_{1i}\omega_1 + \cdots + c_{ni}\omega_n, \quad \text{with } c_{ij} \in \mathbb{Z}.$$

Discriminants of Two Integral Bases (Cont'd)

- Now we have

$$\Delta\{\omega_1',\ldots,\omega_n'\} = (\det C)^2 \Delta\{\omega_1,\ldots,\omega_n\}$$

So the integer $\Delta\{\omega_1,\ldots,\omega_n\}$ divides the integer $\Delta\{\omega_1',\ldots,\omega_n'\}$.
But the same argument applies also in the other direction.
So the integer $\Delta\{\omega_1',\ldots,\omega_n'\}$ divides the integer $\Delta\{\omega_1,\ldots,\omega_n\}$.
From this we see that

$$\Delta\{\omega_1',\ldots,\omega_n'\} = \pm\Delta\{\omega_1,\ldots,\omega_n\}.$$

Also each $c_{ij} \in \mathbb{Z}$. So $\det C \in \mathbb{Z}$.
Therefore, $(\det C)^2 > 0$.
Thus,

$$\Delta\{\omega_1',\ldots,\omega_n'\} = \Delta\{\omega_1,\ldots,\omega_n\}.$$

The Discriminant of a Number Field

- Let K be a number field.
- We have seen that K has an integral basis.
- Moreover, by the proposition, any two integral bases have equal discriminants.

Definition

Suppose that K is a number field. The **discriminant** D_K of K is defined to be the discriminant of any integral basis for K.

Example

- Consider the case $K = \mathbb{Q}(\sqrt{d})$, with d squarefree and $d \equiv 1 \pmod 4$.
  An integral basis is $\{1, \frac{1+\sqrt{d}}{2}\}$.
  There are two embeddings into $\mathbb{C}$, given by

$$\begin{array}{rcl} \sigma_1(a+b\sqrt{d}) & = & a+b\sqrt{d}; \\ \sigma_1(a+b\sqrt{d}) & = & a-b\sqrt{d}. \end{array}$$

  The discriminant is

$$\left| \begin{array}{cc} \sigma_1(1) & \sigma_1(\frac{1+\sqrt{d}}{2}) \\ \sigma_2(1) & \sigma_2(\frac{1+\sqrt{d}}{2}) \end{array} \right|^2 = \left| \begin{array}{cc} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{array} \right|^2 = (-\sqrt{d})^2 = d.$$

  Thus, if $K = \mathbb{Q}(\sqrt{d})$ as above, $D_K = d$.

Example (Cont'd)

- An integral basis for $K = \mathbb{Q}(\sqrt{d})$ with d squarefree and $d \equiv 2 \pmod 4$ or $d \equiv 3 \pmod 4$ is $\{1, \sqrt{d}\}$.

  In this case,

$$D_K = \begin{vmatrix} \sigma_1(1) & \sigma_1(\sqrt{d}) \\ \sigma_2(1) & \sigma_2(\sqrt{d}) \end{vmatrix}^2 = \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 = (-2\sqrt{d})^2 = 4d.$$

Subsection 5

Further Theory of the Discriminant

Minimal Polynomial of γ and Norm of $f'(\gamma)$

Proposition

Suppose that $K = \mathbb{Q}(\gamma)$, and that the minimal polynomial of γ over $\mathbb{Q}$ is $f(X) \in \mathbb{Q}[X]$ of degree n. Then

$$\Delta\{1,\gamma,\ldots,\gamma^{n-1}\} = (-1)^{n(n-1)/2} N_{K/\mathbb{Q}}(f'(\gamma)).$$

- We saw that the discriminant

$$\Delta\{1,\gamma,\ldots,\gamma^{n-1}\} = \prod_{i<j}(\gamma_i - \gamma_j)^2,$$

  where the conjugates of γ are $\gamma_1,\ldots,\gamma_n$.
  Recall that:
  - The conjugates are the roots in $\mathbb{C}$ of the minimal polynomial $f(X)$;
  - Minimal polynomials are monic.

  So $f(X) = \prod_{i=1}^n (X - \gamma_i)$.

Minimal Polynomial of γ and Norm of $f'(\gamma)$ (Cont'd)

- Using the product rule,

$$f'(X) = \sum_{k=1}^{n} \prod_{i \neq k} (X - \gamma_i).$$

Only the term with $k = j$ does not have a factor $(X - \gamma_j)$.
So

$$f'(\gamma_j) = \prod_{i \neq j} (\gamma_j - \gamma_i).$$

Then

$$N_{K/\mathbb{Q}}(f'(\gamma)) = \prod_{j=1}^{n} f'(\gamma_j) = \prod_{j=1}^{n} \prod_{i \neq j} (\gamma_j - \gamma_i).$$

If $i < j$, this product has a bracket $(\gamma_i - \gamma_j)$ and a bracket $(\gamma_j - \gamma_i)$.
It follows that

$$N_{K/\mathbb{Q}}(f'(\gamma)) = \prod_{i<j} [-(\gamma_i - \gamma_j)^2] = (-1)^{n(n-1)/2} \Delta\{1, \gamma, \ldots, \gamma^{n-1}\}.$$

Discriminant of an Integral Basis of K

Lemma

Suppose that $\omega_1,\ldots,\omega_n$ is a basis for K over $\mathbb{Q}$ consisting of elements of $\mathbb{Z}_K$. Then

$$\Delta\{\omega_1,\ldots,\omega_n\}\mathbb{Z}_K \subseteq \mathbb{Z}\omega_1+\cdots+\mathbb{Z}\omega_n.$$

- Let $\alpha\in\mathbb{Z}_K$. By hypothesis, $\{\omega_1,\ldots,\omega_n\}$ is a basis.
  So we can write

  $$\alpha = x_1\omega_1+\cdots+x_n\omega_n, \quad x_1,\ldots,x_n\in\mathbb{Q}.$$

  Multiply through by ω_j to get $\alpha\omega_j=\sum_{i=1}^n x_i\omega_i\omega_j$.
  Take the trace:

  $$T_{K/\mathbb{Q}}(\alpha\omega_j)=\sum_{i=1}^n x_i T_{K/\mathbb{Q}}(\omega_i\omega_j).$$

  Now α and ω_j are in $\mathbb{Z}_K$. So $T_{K/\mathbb{Q}}(\alpha\omega_j)\in\mathbb{Z}$, by a previous corollary.

Discriminant of an Integral Basis of K (Cont'd)

- Similarly, the traces $T_{K/\mathbb{Q}}(\omega_i\omega_j)$ are also in $\mathbb{Z}$, for all i,j.

  So the preceding equations can be regarded as a set of linear equations whose solution is given by $x_1,\ldots,x_n$.

  Cramer's rule implies that the solutions are quotients of integers (given by suitable determinants of integers) by

  $$\det(T_{K/\mathbb{Q}}(\omega_i\omega_j)) = \Delta\{\omega_1,\ldots,\omega_n\}.$$

  So $\Delta\{\omega_1,\ldots,\omega_n\}x_i \in \mathbb{Z}$, for all i.

  Multiplying α by $\Delta\{\omega_1,\ldots,\omega_n\}$, we see that

  $$\Delta\{\omega_1,\ldots,\omega_n\}\alpha \in \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n.$$

Finding Integral Bases of Number Fields

- Strategy for finding integral bases for a number field K:

Step 1 Find any basis for K over $\mathbb{Q}$.
Scale the basis elements so that they are in $\mathbb{Z}_K$.
Let $\{\omega_1, \ldots, \omega_n\}$ be the result.

Step 2 Compute $\Delta = \Delta\{\omega_1, \ldots, \omega_n\}$.
By the lemma, $\mathbb{Z}_K \subseteq \frac{1}{\Delta}(\mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n)$. So every integer must be of the form

$$x_1\omega_1 + \cdots + x_n\omega_n,$$

for $x_i \in \mathbb{Q}$ but where the denominators divide Δ.

Step 3 For a prime $p^2 \mid \Delta$, check whether any element

$$\omega = x_1\omega_1 + \cdots + x_n\omega_n$$

is integral, where x_i is a rational number with denominator dividing p.

Finding Integral Bases of Number Fields (Cont'd)

If such an integral ω exists, where some x_i is not in $\mathbb{Z}$, so has denominator p, replace ω_i with ω to get a set with discriminant $\frac{\Delta}{p^2}$ (by a previous proposition).

Since the discriminant of an integral basis must be in $\mathbb{Z}$, we need only do this for primes p, with $p^2 \mid \Delta$.

Now return to Step 2.

If no such element is integral, for any prime p with $p^2 \mid \Delta$, then we have an integral basis.

Corollary

Suppose that K is a number field and $\omega_1, \ldots, \omega_n$ are elements of $\mathbb{Z}_K$, such that $\Delta\{\omega_1, \ldots, \omega_n\}$ is squarefree. Then $\{\omega_1, \ldots, \omega_n\}$ is an integral basis.

Integral Basis of a Double Extension

Proposition

Suppose that $K_1 = \mathbb{Q}(\gamma_1)$ and $K_2 = \mathbb{Q}(\gamma_2)$ are two number fields of degree n_1 and n_2 respectively, such that $K = \mathbb{Q}(\gamma_1, \gamma_2)$ has degree $n_1 n_2$ over $\mathbb{Q}$. Suppose that $\{\omega_1, \ldots, \omega_{n_1}\}$ and $\{\omega'_1, \ldots, \omega'_{n_2}\}$ are integral bases for K_1 and K_2, respectively, with discriminants D_1 and D_2. If D_1 and D_2 are coprime, then $\{\omega_i \omega'_j\}$ forms an integral basis for K, of discriminant $D_1^{n_2} D_2^{n_1}$.

- We first claim that $\{\omega_i \omega'_j\}$ form a basis for K over $\mathbb{Q}$.

  Every element of K is a polynomial expression in γ_1 and γ_2.

  Every power of γ_1 lies in K_1.

  So it is a linear combination of $\{\omega_1, \ldots, \omega_{n_1}\}$.

  Similarly, every power of γ_2 lies in K_2.

  So it is a linear combination of $\{\omega'_1, \ldots, \omega'_{n_2}\}$.

Integral Basis of a Double Extension (Cont'd)

- Thus, every product $\gamma_1^a \gamma_2^b$ is a linear combination of $\{\omega_i \omega'_j\}$.
  Each element of K is a linear combination of these monomials.
  So it is also a linear combination of this set.
  We have $n_1 n_2$ such elements and, by hypothesis, $[K:\mathbb{Q}] = n_1 n_2$.
  So they must be linearly independent, and, thus, form a basis.
  Claim: $\{\omega_i \omega'_j\}$ form an integral basis.
  If $\alpha \in \mathbb{Z}_K$, we can write $\alpha = \sum_{i=1}^{n_1} \sum_{j=1}^{n_2} x_{ij} \omega_i \omega'_j$. We show $x_{ij} \in \mathbb{Z}$.
  Then
  $$\alpha = \sum_{i=1}^{n_1} \sum_{j=1}^{n_2} x_{ij} \omega_i \omega'_j = \sum_{i=1}^{n_1} (\sum_{j=1}^{n_2} x_{ij} x_{ij} \omega'_j) \omega_i = \sum_{i=1}^{n_1} y_i \omega_i,$$
  where $y_i = \sum_{j=1}^{n_2} x_{ij} \omega'_j \in K_2$.
  We have $[K:\mathbb{Q}] = n_1 n_2$ and $[K_1:\mathbb{Q}] = n_1$.
  So, by the tower law, $[K:K_1] = n_2$.

Integral Basis of a Double Extension (Claim)

- Since $K = K_1(\gamma_2)$, we see that there are n_2 embeddings of K into $\mathbb{C}$ which are the identity on K_1 (regarded as a subfield of $\mathbb{C}$).
  Let $\{\sigma'_1, \ldots, \sigma'_{n_2}\}$ denote these embeddings of K into $\mathbb{C}$.
  Regard these as maps on the elements of $K_2 \subseteq K$.
  They are determined by sending γ_2 to one of its conjugates.
  In this sense, they restrict to the n_2 different embeddings of K_2 into $\mathbb{C}$.
  Let
  $$\boldsymbol{x} = \begin{pmatrix} \sigma'_1(\alpha) \\ \vdots \\ \sigma'_{n_2}(\alpha) \end{pmatrix} \quad \text{and} \quad \boldsymbol{y} = \begin{pmatrix} y_1 \\ \vdots \\ y_{n_2} \end{pmatrix}.$$
  Then $\boldsymbol{x} = M\boldsymbol{y}$, where $M_{k\ell} = \sigma'_k(\omega'_\ell)$. By definition, $D_2 = (\det M)^2$.
  As in a previous lemma, $D_2 y_i = \sum_{j=1}^{n_2} D_2 x_{ij} \omega'_j$ has coefficients in $\mathbb{Z}$.
  So $D_2 x_{ij} \in \mathbb{Z}$.
  In the same way (exchanging the roles of K_1 and K_2), $D_1 x_{ij} \in \mathbb{Z}$.
  As D_1 and D_2 are coprime, we conclude that each $x_{ij} \in \mathbb{Z}$.

Integral Basis of a Double Extension (Cont'd)

- So $\{\omega_i\omega'_j\}$ forms an integral basis for $\mathbb{Z}_K$.

  Let $\{\sigma_1,\ldots,\sigma_{n_1}\}$ be the embeddings of K into $\mathbb{C}$, which are the identity on K_2.

  Then all the embeddings of K into $\mathbb{C}$ are given by $\{\sigma_i\sigma'_j\}$.

  This can easily be seen by observing that an embedding is uniquely determined by its effect on γ_1 and γ_2.

  These, in turn, uniquely determine σ_i and σ'_j.

  The discriminant of the basis $\{\omega_i\omega'_j\}$ is given by $(\det A)^2$, where A is an $n_1n_2 \times n_1n_2$-matrix with

$$A_{ki,\ell j} = (\sigma_k\sigma'_\ell)(\omega_i\omega'_j) = \sigma_k(\omega_i)\sigma'_\ell(\omega'_j).$$

Integral Basis of a Double Extension (Cont'd)

- We can decompose A as $A = BC$, where:
  - B is the $n_2 \times n_2$ matrix of $n_1 \times n_1$-blocks given by

$$B = \begin{pmatrix} Q & 0 & \cdots & 0 \\ 0 & Q & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & Q \end{pmatrix},$$

    where Q is the $n_1 \times n_1$-matrix with $Q_{ki} = \sigma_k(\omega_i)$;
  - C is the block matrix

$$C = \begin{pmatrix} \sigma_1'(\omega_1')I & \sigma_2'(\omega_1')I & \cdots & \sigma_{n_2}'(\omega_1')I \\ \sigma_1'(\omega_2')I & \sigma_2'(\omega_2')I & \cdots & \sigma_{n_2}'(\omega_2')I \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1'(\omega_{n_2}')I & \sigma_2'(\omega_{n_2}')I & \cdots & \sigma_{n_2}'(\omega_{n_2}')I \end{pmatrix},$$

    where I is the $n_1 \times n_1$-identity matrix.

Integral Basis of a Double Extension (Conclusion)

- Clearly
$$\det(B) = \det(Q)^{n_2}.$$
So
$$\det(B)^2 = ((\det Q)^2)^{n_2} = D_1^{n_2}.$$
Also,
$$\det(C) = \det(\sigma'_\ell(\omega'_j))^{n_1}.$$
So
$$\det(C)^2 = D_2^{n_1}.$$
Therefore,
$$\Delta = \det(A)^2 = \det(B)^2 \det(C)^2 = D_1^{n_2} D_2^{n_1}.$$

Subsection 6

Rings of Integers in Some Cubic and Quadratic Fields

Monogenicity and Power Bases

- We consider some examples on the construction of integral bases.
- In two of these examples, we show the ring of integers cannot be expressed in the form $\mathbb{Z}[\gamma]$ for any element γ.
- Fields K where $\mathbb{Z}_K = \mathbb{Z}[\gamma]$ are called **monogenic**.
- In such cases, the basis $\{1, \gamma, \ldots, \gamma^{n-1}\}$ is called a **power basis**.

$K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$

- The ring of integers of $\mathbb{Q}(\sqrt{2})$ is $\mathbb{Z}[\sqrt{2}]$.
- The ring of integers of $\mathbb{Q}(\sqrt{3})$ is $\mathbb{Z}[\sqrt{3}]$.
- One might hope that the ring of integers of $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ should be $\mathbb{Z}[\sqrt{2}, \sqrt{3}]$.
- We have already seen that this is false.
- Moreover, this does not contradict the preceding proposition, since the discriminants of $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are not coprime.

$K=\mathbb{Q}(\sqrt{2},\sqrt{3})$ (Cont'd)

- Let $\alpha\in\mathbb{Z}_K$.
  Then, for some $a,b,c,d\in\mathbb{Q}$, we can write
  $$\alpha=a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}.$$
  Since $\alpha\in\mathbb{Z}_K$, all of its conjugates
  $$\begin{aligned}\alpha_2 &= a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6},\\ \alpha_3 &= a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6},\\ \alpha_4 &= a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6}\end{aligned}$$
  are also algebraic integers.
  The set of algebraic integers is closed under addition.
  It follows that the following are also algebraic integers:
  $$\alpha+\alpha_2=2a+2c\sqrt{3},\quad \alpha+\alpha_3=2a+2b\sqrt{2},\quad \alpha+\alpha_4=2a+2d\sqrt{6}.$$
  By a preceding proposition, these are integral if $2a,2b,2c,2d\in\mathbb{Z}$.

$K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ (Cont'd)

- Thus, there exist $A, B, C, D \in \mathbb{Z}$, with $A = 2a$, $B = 2b$, $C = 2c$ and $D = 2d$, such that
$$\alpha = \frac{A + B\sqrt{2} + C\sqrt{3} + D\sqrt{6}}{2}.$$
In addition, the following is also integral
$$\begin{aligned} \alpha\alpha_2 &= (a + c\sqrt{3})^2 - (b\sqrt{2} + d\sqrt{6})^2 \\ &= a^2 + 2ac\sqrt{3} + 3c^2 - 2b^2 - 4bd\sqrt{3} - 6d^2 \\ &= \tfrac{A^2 + 3C^2 - 2B^2 - 6D^2}{4} + \tfrac{AC - 2BD}{2}\sqrt{3}. \end{aligned}$$
Thus, $4 \mid A^2 + 3C^2 - 2B^2 - 6D^2$ and $2 \mid AC - 2BD$.
The second implies that $2 \mid AC$. So at least one of A and C is even.
If only one were even, then $A^2 + 3C^2 - 2B^2 - 6D^2$ would be odd, and the first requirement would fail. So both A and C are even.

$K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ (Cont'd)

- We saw that both A and C are even.
  Now $2 \mid AC - 2BD$ becomes automatic.
  Moreover, $4 \mid A^2 + 3C^2 - 2B^2 - 6D^2$ reduces to $4 \mid 2B^2 + 6D^2$.
  Equivalently, $2 \mid B^2 + D^2$.
  So B and D are both even or both odd.
  It follows that all integers are of the form
  $$\alpha = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6},$$
  with $a, c \in \mathbb{Z}$ and b and d both integral or both halves of odd integers.
  It remains to check that elements of this form are all integers.
  They are integer linear combinations of $1, \sqrt{2}, \sqrt{3}$ and $\frac{\sqrt{2}+\sqrt{6}}{2} = \frac{1+\sqrt{3}}{2}$.
  The first three are obviously integers.
  The last is integral because it is a root of the monic polynomial $f(X) = X^4 - 4X^2 + 1$, with coefficients in $\mathbb{Z}$.

$K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ (Conclusion)

Claim: $\mathbb{Z}_K = \mathbb{Z}[\gamma]$, where $\gamma = \frac{\sqrt{2}+\sqrt{6}}{2}$.

We have

$$\begin{aligned} \gamma^2 &= 2+\sqrt{3}; \\ \gamma^3 &= \frac{5\sqrt{2}+3\sqrt{6}}{2}. \end{aligned}$$

So

$$\begin{aligned} \sqrt{2} &= \gamma^3 - 3\gamma; \\ \sqrt{3} &= \gamma^2 - 2. \end{aligned}$$

So each element in $\{1, \sqrt{2}, \sqrt{3}, \gamma\}$ is in $\mathbb{Z}[\gamma]$.

Therefore, $\mathbb{Z}_K \subseteq \mathbb{Z}[\gamma]$.

Conversely, $\gamma \in \mathbb{Z}_K$.

So, since $\mathbb{Z}_K$ is a ring, $\mathbb{Z}[\gamma] \subseteq \mathbb{Z}_K$.

$K = \mathbb{Q}(\sqrt{-2}, \sqrt{-5})$

- The determination of the ring of integers in this case is very similar to that of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

  However, we can check that if $\gamma = \frac{\sqrt{-2}+\sqrt{10}}{2}$, the argument above that $\mathbb{Z}_K = \mathbb{Z}[\gamma]$ does not work in this case.

  Claim: There is no element γ such that $\mathbb{Z}_K = \mathbb{Z}[\gamma]$.

  We consider the following elements

$$\begin{array}{rcl} \alpha_1 & = & (1+\sqrt{-2})(1+\sqrt{-5}), \\ \alpha_2 & = & (1+\sqrt{-2})(1-\sqrt{-5}), \\ \alpha_3 & = & (1-\sqrt{-2})(1+\sqrt{-5}), \\ \alpha_4 & = & (1-\sqrt{-2})(1-\sqrt{-5}). \end{array}$$

  Clearly, they all lie in $\mathbb{Z}_K$.

  Moreover, $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 4$.

$K = \mathbb{Q}(\sqrt{-2}, \sqrt{-5})$ (Cont'd)

- Notice that

$$\begin{aligned} \alpha_1\alpha_2 &= (1+\sqrt{-2})^2(1+\sqrt{-5})(1-\sqrt{-5}) \\ &= 6(1+\sqrt{-2})^2. \end{aligned}$$

Similarly, $3 \mid \alpha_i\alpha_j$, for any pair $i \neq j$.
This implies that

$$(\alpha_1+\alpha_2+\alpha_3+\alpha_4)^n \equiv \alpha_1^n+\alpha_2^n+\alpha_3^n+\alpha_4^n \pmod{3},$$

where the congruence actually takes place in $\mathbb{Z}_K$, meaning that the two sides differ by an element of $3\mathbb{Z}_K$. Then

$$\begin{aligned} T_{K/\mathbb{Q}}(\alpha_1^n) &= \alpha_1^n+\alpha_2^n+\alpha_3^n+\alpha_4^n \\ &\equiv (\alpha_1+\alpha_2+\alpha_3+\alpha_4)^n \\ &\equiv 4^n \\ &\equiv 1 \pmod{3}. \end{aligned}$$

$K = \mathbb{Q}(\sqrt{-2}, \sqrt{-5})$ (Cont'd)

- Suppose $3 | \alpha_1^n$.
  Then 3 would also divide any of its conjugates.
  So $3 \mid \alpha_i^n$, for all i.
  So $3 \mid T_{K/\mathbb{Q}}(\alpha_1^n)$.
  Thus, $3 \nmid \alpha_1^n$, for any n.
  Similarly, $3 \nmid \alpha_i^n$ for any i and any n.
  Finally, suppose that $\mathbb{Z}_K = \mathbb{Z}[\gamma]$, for some γ.
  Let $f(X) \in \mathbb{Z}[X]$ be the minimal polynomial of γ.
  As $\alpha_i \in \mathbb{Z}_K$, we can write $\alpha_i = f_i(\gamma)$, for some $f_i \in \mathbb{Z}[X]$.
  Now $3 \mid \alpha_i \alpha_j$, for all $i \neq j$, but $3 \nmid \alpha_i^n$ for any i and n.
  Let $\overline{f}$ denote the polynomial f with its coefficients reduced modulo 3.
  So $\overline{f}(X) \in \mathbb{F}_3[X]$, where $\mathbb{F}_3 = \{0, 1, 2\}$ are the integers modulo 3.

$K = \mathbb{Q}(\sqrt{-2}, \sqrt{-5})$ (Claim)

Claim: If $g(X) \in \mathbb{Z}[X]$, that $3 \mid g(\gamma)$ in $\mathbb{Z}[\gamma]$ if and only if $\overline{g}$ is divisible by $\overline{f}$ in $\mathbb{F}_3[X]$.

Suppose $3 \mid g(\gamma)$ in $\mathbb{Z}[\gamma]$.

Then, $g(\gamma) = 3k(\gamma)$, for some $k(\gamma)$ in $\mathbb{Z}[\gamma]$.

Hence, $(g - 3k)(\gamma) = 0$.

By minimality of f, $f \mid g - 3k$.

This shows that $f \mid g$ in $\mathbb{F}_3[X]$.

Suppose, conversely, that $\overline{f} \mid \overline{g}$ in $\mathbb{F}_3[X]$.

Then there exists $k(x)$, such that $\overline{g}(X) = \overline{f}(X)\overline{k}(X)$ in $\mathbb{F}_3[X]$.

Since $f(\gamma) = 0$, we get $\overline{g}(\gamma) = 0$ in $\mathbb{F}_3[X]$.

So $3 \mid g(\gamma)$ in $\mathbb{Z}[\gamma]$.

$K = \mathbb{Q}(\sqrt{-2}, \sqrt{-5})$ (Cont'd)

- We apply the Claim to $f_i(X)f_j(X)$.

  We know that $3 \mid \alpha_i\alpha_j = f_i(\gamma)f_j(\gamma)$.

  We conclude that $\overline{f} \mid \overline{f}_i\overline{f}_j$, for all $i \neq j$.

  Since $3 \nmid \alpha_i^n$, $\overline{f} \nmid \overline{f}_i^n$ for any i and n.

  So, for all $i \neq j$, $\overline{f}$ has a factor dividing $\overline{f}_i$ but not $\overline{f}_j$.

  Hence, $\overline{f}$ must have at least four different irreducible factors.

  But f is a quartic, so the different factors of $\overline{f}$ must all be linear.

  However, there are only three different linear factors in $\mathbb{F}_3[X]$, namely, $X, X-1$ and $X-2$.

  This gives a contradiction.

$K = \mathbb{Q}(\sqrt[3]{2})$

- As an example of a cubic field, we consider $K = \mathbb{Q}(\sqrt[3]{2})$.

  Write $\alpha = \sqrt[3]{2}$ and $\omega = e^{2\pi i/3}$.

  Note that $1 + \omega + \omega^2 = 0$.

  Suppose that

  $$\theta_1 = a + b\alpha + c\alpha^2, \quad a, b, c \in \mathbb{Q},$$

  lies in $\mathbb{Z}_K$.

  The conjugates of α are also algebraic integers,

  $$\begin{aligned} \theta_2 &= a + b\alpha\omega + c\alpha^2\omega^2; \\ \theta_3 &= a + b\alpha\omega^2 + c\alpha^2\omega. \end{aligned}$$

  But they are not in K.

$K = \mathbb{Q}(\sqrt[3]{2})$ (Cont'd)

- Then the following are also algebraic integers,

$$\begin{array}{rcl} \theta_1+\theta_2+\theta_3 & = & 3a, \\ \theta_1\theta_2+\theta_2\theta_3+\theta_3\theta_1 & = & 3a^2-6bc, \\ \theta_1\theta_2\theta_3 & = & a^3+2b^3+4c^3-6abc. \end{array}$$

As they are also rational, they are all in $\mathbb{Z}$.
Write $A=3a$, $B=3b$ and $C=3c$.
The first equation gives $A\in\mathbb{Z}$.
Multiplying the second by 3 gives $A^2-2BC\equiv 0 \pmod 3$.
Multiplying the third by 27 gives $A^3+2B^3+4C^3-6ABC\equiv 0 \pmod{27}$.
The second and third give $B,C\in\mathbb{Z}$ as follows.
Suppose $A^2-2BC\in\mathbb{Z}$. Then $2BC\in\mathbb{Z}$. So $6ABC\in\mathbb{Z}$. By the last equation, $2B^3+4C^3\in\mathbb{Z}$. But the only way that rationals can satisfy $2BC\in\mathbb{Z}$ and $2B^3+4C^3\in\mathbb{Z}$ is if $B,C\in\mathbb{Z}$ (if a prime p occurs in the denominator of B, say, then as $2BC\in\mathbb{Z}$, it cannot also occur in the denominator of C; so p is in the denominator of $2B^3+4C^3$).

$K = \mathbb{Q}(\sqrt[3]{2})$ (Conclusion)

- Suppose, first, that $3 \mid A$.
  Then, since $A^2 - 2BC \in \mathbb{Z}$, $2BC \equiv 0 \pmod 3$.
  So either B or C is divisible by 3.
  Then $3 \mid A^3 + 2B^3 + 4C^3 - 6ABC$ implies that both must be.
- Suppose, next, that $3 \nmid A$.
  The only solutions to

  $$A^2 - 2BC \equiv 0 \pmod 3 \quad \text{and} \quad A^3 + 2B^3 + 4C^3 - 6ABC \equiv 0 \pmod 3$$

  are $A \equiv 1$, $B \equiv 2$, $C \equiv 1 \pmod 3$ or $A \equiv 2$, $B \equiv 1$, $C \equiv 2 \pmod 3$.
  Set $A = 1 + 3\ell$, $B = 2 + 3m$, $C = 1 + 3n$.
  Then $A^3 + 2B^3 + 4C^3 - 6ABC \equiv 9 \pmod{27}$, for any ℓ, m and n.
  Similarly, set $A = 2 + 3\ell$, $B = 1 + 3m$, $C = 2 + 3n$.
  Then $A^3 + 2B^3 + 4C^3 - 6ABC \equiv 18 \pmod{27}$, for any ℓ, m and n.
  This means that there are no solutions with $3 \nmid A$.

Thus, $3 \mid A$, $3 \mid B$ and $3 \mid C$. This implies that $a, b, c \in \mathbb{Z}$.

So the ring of integers is $\mathbb{Z}[\sqrt[3]{2}]$.

$K = \mathbb{Q}(\sqrt[3]{175})$

- Set $m = 175 = 5^2 \times 7$.

  We will compute $\mathbb{Z}_K$.

  Note that if $\alpha = \sqrt[3]{175}$, then

  $$\alpha^2 = \sqrt[3]{5^4 7^2} = 5\sqrt[3]{5 \cdot 7^2} = 5\sqrt[3]{245}.$$

  So $\alpha' = \sqrt[3]{245}$ is another element in K.

  Moreover,

  $$\alpha'^2 = \sqrt[3]{5^2 7^4} = 7\sqrt[3]{5^2 \cdot 7} = 5\sqrt[3]{175} = 5\alpha.$$

  Furthermore, both α and α' are integral.

  - The first is a root of the monic integral polynomial $X^3 - 175$;
  - The second is a root of the monic integral polynomial $X^3 - 245$.

$K = \mathbb{Q}(\sqrt[3]{175})$ (Claim)

Claim: $\mathbb{Z}_K$ has integral basis $\{1, \alpha, \alpha'\}$.

First compute $\Delta\{1, \alpha, \alpha'\}$.

The embeddings into $\mathbb{C}$ are given by

$$\begin{array}{rcl} \sigma_1(a + b\alpha + c\alpha') & = & a + b\alpha + c\alpha'; \\ \sigma_2(a + b\alpha + c\alpha') & = & a + b\alpha\omega + c\alpha'\omega; \\ \sigma_3(a + b\alpha + c\alpha') & = & a + b\alpha\omega^2 + c\alpha'\omega. \end{array}$$

For the discriminant, we now have

$$\Delta\{1, \alpha, \alpha'\} = \begin{vmatrix} 1 & \alpha & \alpha' \\ 1 & \alpha\omega & \alpha'\omega^2 \\ 1 & \alpha\omega^2 & \alpha'\omega \end{vmatrix} = -3\sqrt{3}i\alpha\alpha'.$$

Note that $\alpha\alpha' = 5 \cdot 7 = 35$. So we have

$$\Delta\{1, \alpha, \alpha'\} = (-3\sqrt{3}i\alpha\alpha')^2 = -3^3 5^2 7^2.$$

$K = \mathbb{Q}(\sqrt[3]{175})$ (Claim Cont'd)

- We conclude that all integers must be of the form

$$\frac{a+b\alpha+c\alpha'}{d}, \quad a,b,c,d \in \mathbb{Z}, \ d \mid 3\times 5\times 7.$$

Suppose $\theta_1 = \frac{a+b\alpha+c\alpha'}{5}$ is an integer.
Then so are its conjugates

$$\theta_2 = \frac{a+b\alpha\omega+c\alpha'\omega^2}{5}, \quad \theta_3 = \frac{a+b\alpha\omega^2+c\alpha'\omega}{5}.$$

Then $\theta_1+\theta_2+\theta_3 = \frac{3a}{5}$ is an integer. So $5 \mid a$.
Now $\theta_1 = A + \frac{b\alpha+c\alpha'}{5}$, where $A \in \mathbb{Z}$. So $\frac{b\alpha+c\alpha'}{5} \in \mathbb{Z}_K$.
Its norm is the product of the conjugates:

$$\frac{b^3\alpha^3+c^3\alpha'^3}{5^3} = \frac{175b^3+245c^3}{125} = \frac{35b^3+49c^3}{25}.$$

We need this to be an integer.

$K = \mathbb{Q}(\sqrt[3]{175})$ (Claim Cont'd)

- Suppose $35b^3 + 49c^3 \equiv 0 \pmod{25}$.

  Then $35b^3 + 49c^3 \equiv 0 \pmod{5}$.

  So $5 \mid c^3$. Hence, $5 \mid c$.

  As $35b^3 + 49c^3 \equiv 0 \pmod{25}$, we also have $5 \mid b$.

  Thus 5 cannot occur in the denominator of an element of $\mathbb{Z}_K$.

  Exactly the same argument works for 7.

  For $p = 3$, we need to consider $\theta_1 = \frac{a+b\alpha+c\alpha'}{3}$ and determine when it is an integer.

  We may use the method of the previous example.

  We find that, if $\theta_1 = \frac{a+b\alpha+c\alpha'}{3}$ is in $\mathbb{Z}_K$, then $3 \mid a$, $3 \mid b$ and $3 \mid c$.

  It follows that $\mathbb{Z}_K$ has $\{1, \alpha, \alpha'\}$ as an integral basis.

$K = \mathbb{Q}(\sqrt[3]{175})$ (Non-Monogenicity)

- Suppose $\{1, \gamma, \gamma^2\}$ is an integral basis, for some γ.

  Let $\gamma = a + b\alpha + c\alpha'$. Then $\gamma - a = b\alpha + c\alpha'$.

  If $\{1, \gamma, \gamma^2\}$ is an integral basis, then we can see that

  $$\{1, \gamma - a, (\gamma - a)^2\}$$

  is also an integral basis.

  So we may assume that γ is simply of the form $b\alpha + c\alpha'$.

  Then, recalling that $\alpha^2 = 5\alpha'$, $\alpha'^2 = 7\alpha$ and $\alpha\alpha' = 35$, we get

  $$\gamma^2 = (b\alpha + c\alpha')^2 = b^2\alpha^2 + 2bc\alpha\alpha' + c^2\alpha'^2 = 5b^2\alpha' + 70bc + 7c^2\alpha.$$

  So we have expressed the elements $\{1, \gamma, \gamma^2\}$ in terms of the basis $\{1, \alpha, \alpha'\}$.

$K = \mathbb{Q}(\sqrt[3]{175})$ (Non-Monogenicity Cont'd)

- The condition that $\{1,\gamma,\gamma^2\}$ is a basis is equivalent to requiring that the change of basis matrix should have determinant ± 1.

  This is

  $$\begin{vmatrix} 1 & 0 & 0 \\ 0 & b & c \\ 70bc & 7c^2 & 5b^2 \end{vmatrix} = 5b^3 - 7c^3.$$

  By working modulo 7, $5b^3 - 7c^3 \neq \pm 1$, for any integers b and c.

  The cubes modulo 7 are 0 and ± 1.

  So we cannot have $5b^3 \equiv \pm 1 \pmod{7}$.

  This contradiction shows that $\mathbb{Z}_K$ has no integral basis of the form $\{1,\gamma,\gamma^2\}$.