Math 361

February 10, 2023

Review quiz from last time

1. Let $A \subseteq B$ be domains. What does it mean to say the $\alpha \in B$ is *integral* over A?
2. Define the following terms:
   (i) Number field.
   (ii) Algebraic number.
   (iii) Algebraic integer.

Today

1. Review our main theorem for the discriminants proved last time.

Today

1. Review our main theorem for the discriminants proved last time.
2. Show that $\mathfrak{O}_K$ is a free $\mathbb{Z}$-module of rank n.

Today

1. Review our main theorem for the discriminants proved last time.
2. Show that $\mathfrak{O}_K$ is a free $\mathbb{Z}$-module of rank n.
3. Define the discriminant of a number field.

Today

1. Review our main theorem for the discriminants proved last time.
2. Show that $\mathfrak{O}_K$ is a free $\mathbb{Z}$-module of rank n.
3. Define the discriminant of a number field.
4. How to sometimes find a $\mathbb{Z}$-basis for $\mathfrak{O}_K$.

Review of discriminant theorem from last time

Let K be a number field, and let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Q}$-basis for K.

Review of discriminant theorem from last time

Let K be a number field, and let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Q}$-basis for K. Then the discriminant, $\Delta[\alpha_1, \ldots, \alpha_n]$, is a nonzero rational number.

Review of discriminant theorem from last time

Let K be a number field, and let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Q}$-basis for K. Then the discriminant, $\Delta[\alpha_1, \ldots, \alpha_n]$, is a nonzero rational number. If the α_i are algebraic integers, then $\Delta[\alpha_1, \ldots, \alpha_n]$ is a nonzero rational integer.

Review of discriminant theorem from last time

To define the discriminant, we need the embeddings $K \to \mathbb{C}$.

Review of discriminant theorem from last time

To define the discriminant, we need the embeddings $K \to \mathbb{C}$.

- Pick $\theta \in K$ such that $K = \mathbb{Q}(\theta)$.

Review of discriminant theorem from last time

To define the discriminant, we need the embeddings $K \to \mathbb{C}$.

- Pick $\theta \in K$ such that $K = \mathbb{Q}(\theta)$.
- Let p be the minimal polynomial for θ over $\mathbb{Q}$.

Review of discriminant theorem from last time

To define the discriminant, we need the embeddings $K \to \mathbb{C}$.

- Pick $\theta \in K$ such that $K = \mathbb{Q}(\theta)$.
- Let p be the minimal polynomial for θ over $\mathbb{Q}$.
- Factor: $p = \prod_{i=1}^{n}(x - \theta_i)$.

Review of discriminant theorem from last time

To define the discriminant, we need the embeddings $K \to \mathbb{C}$.

- Pick $\theta \in K$ such that $K = \mathbb{Q}(\theta)$.
- Let p be the minimal polynomial for θ over $\mathbb{Q}$.
- Factor: $p = \prod_{i=1}^{n}(x - \theta_i)$.
- $\{1, \theta, \ldots, \theta^{n-1}\}$ is a $\mathbb{Q}$-basis for K. Hence, sending $\theta \to \theta_i$ defines an embedding σ_i.

Review of discriminant theorem from last time

To define the discriminant, we need the embeddings $K \to \mathbb{C}$.

- Pick $\theta \in K$ such that $K = \mathbb{Q}(\theta)$.
- Let p be the minimal polynomial for θ over $\mathbb{Q}$.
- Factor: $p = \prod_{i=1}^{n}(x - \theta_i)$.
- $\{1, \theta, \ldots, \theta^{n-1}\}$ is a $\mathbb{Q}$-basis for K. Hence, sending $\theta \to \theta_i$ defines an embedding σ_i. This procedure gives all of the embeddings.

Review of discriminant theorem from last time

To define the discriminant, we need the embeddings $K \to \mathbb{C}$.

- Pick $\theta \in K$ such that $K = \mathbb{Q}(\theta)$.
- Let p be the minimal polynomial for θ over $\mathbb{Q}$.
- Factor: $p = \prod_{i=1}^{n}(x - \theta_i)$.
- $\{1, \theta, \ldots, \theta^{n-1}\}$ is a $\mathbb{Q}$-basis for K. Hence, sending $\theta \to \theta_i$ defines an embedding σ_i. This procedure gives all of the embeddings.
- The discriminant of the basis $\{\alpha_1, \ldots, \alpha_n\}$ is

$$\Delta[\alpha_1, \ldots, \alpha_n] := \det(\sigma_i(\alpha_j))^2.$$

Symmetric polynomials in the roots of a polynomial

Recall the connection between a polynomial in $f \in \mathbb{Q}[x]$ and the symmetric polynomials in its roots:

$$f = (x - \theta_1)(x - \theta_2)(x - \theta_3)(x - \theta_4).$$

Symmetric polynomials in the roots of a polynomial

Recall the connection between a polynomial in $f \in \mathbb{Q}[x]$ and the symmetric polynomials in its roots:

$$f = (x - \theta_1)(x - \theta_2)(x - \theta_3)(x - \theta_4).$$

Expand:

Symmetric polynomials in the roots of a polynomial

Recall the connection between a polynomial in $f \in \mathbb{Q}[x]$ and the symmetric polynomials in its roots:

$$f = (x - \theta_1)(x - \theta_2)(x - \theta_3)(x - \theta_4).$$

Expand:

$$f = x^4 - (\theta_1 + \cdots + \theta_4)x^3 + (\theta_1\theta_2 + \cdots + \theta_3\theta_4)x^2$$
$$- (\theta_1\theta_2\theta_3 + \cdots + \theta_2\theta_3\theta_4)x + (\theta_1\theta_2\theta_3\theta_4)$$

Symmetric polynomials in the roots of a polynomial

Recall the connection between a polynomial in $f \in \mathbb{Q}[x]$ and the symmetric polynomials in its roots:

$$f = (x - \theta_1)(x - \theta_2)(x - \theta_3)(x - \theta_4).$$

Expand:

$$\begin{aligned} f &= x^4 - (\theta_1 + \cdots + \theta_4)x^3 + (\theta_1\theta_2 + \cdots + \theta_3\theta_4)x^2 \\ &\quad - (\theta_1\theta_2\theta_3 + \cdots + \theta_2\theta_3\theta_4)x + (\theta_1\theta_2\theta_3\theta_4) \\ &= x^4 - s_1(\theta_1, \theta_2, \theta_3, \theta_4)x^3 + s_2(\theta_1, \theta_2, \theta_3, \theta_4)x^2 \\ &\quad - s_3(\theta_1, \theta_2, \theta_3, \theta_4)x + s_4(\theta_1, \theta_2, \theta_3, \theta_4). \end{aligned}$$

Symmetric polynomials in the roots of a polynomial

Recall the connection between a polynomial in $f \in \mathbb{Q}[x]$ and the symmetric polynomials in its roots:

$$f = (x - \theta_1)(x - \theta_2)(x - \theta_3)(x - \theta_4).$$

Expand:

$$\begin{aligned} f &= x^4 - (\theta_1 + \cdots + \theta_4)x^3 + (\theta_1\theta_2 + \cdots + \theta_3\theta_4)x^2 \\ &\quad - (\theta_1\theta_2\theta_3 + \cdots + \theta_2\theta_3\theta_4)x + (\theta_1\theta_2\theta_3\theta_4) \\ &= x^4 - s_1(\theta_1, \theta_2, \theta_3, \theta_4)x^3 + s_2(\theta_1, \theta_2, \theta_3, \theta_4)x^2 \\ &\quad - s_3(\theta_1, \theta_2, \theta_3, \theta_4)x + s_4(\theta_1, \theta_2, \theta_3, \theta_4). \end{aligned}$$

Punch line: The $s_i(\theta_1, \ldots, \theta_n)$ are the coefficients of f, and hence, are rational numbers.

Proof of discriminant theorem

Idea behind proof:

Proof of discriminant theorem

Idea behind proof:

- Compute $\Delta[1, \theta, \ldots, \theta^{n-1}]$ using a Vandermonde determinant.

Proof of discriminant theorem

Idea behind proof:

- Compute $\Delta[1, \theta, \ldots, \theta^{n-1}]$ using a Vandermonde determinant.
- Compare the two $\mathbb{Q}$-bases $1, \theta, \ldots, \theta^{n-1}$ and $\alpha_1, \ldots, \alpha_n$ using the change of basis formula for discriminants.

Proof of discriminant theorem

Idea behind proof:

- Compute $\Delta[1, \theta, \ldots, \theta^{n-1}]$ using a Vandermonde determinant.
- Compare the two $\mathbb{Q}$-bases $1, \theta, \ldots, \theta^{n-1}$ and $\alpha_1, \ldots, \alpha_n$ using the change of basis formula for discriminants.
- Notice that the resulting formula for $\Delta[\alpha_1, \ldots, \alpha_n]$ is a symmetric function in the roots of p, i.e., in $\theta_1, \ldots, \theta_n$,

Proof of discriminant theorem

Idea behind proof:

- Compute $\Delta[1, \theta, \ldots, \theta^{n-1}]$ using a Vandermonde determinant.
- Compare the two $\mathbb{Q}$-bases $1, \theta, \ldots, \theta^{n-1}$ and $\alpha_1, \ldots, \alpha_n$ using the change of basis formula for discriminants.
- Notice that the resulting formula for $\Delta[\alpha_1, \ldots, \alpha_n]$ is a symmetric function in the roots of p, i.e., in $\theta_1, \ldots, \theta_n$, hence rational (since p has rational coefficients).

Proof of the discriminant theorem

Proof.

$\Delta[1, \theta, \ldots, \theta^{n-1}] =$

Proof of the discriminant theorem

Proof.

$$\Delta[1, \theta, \ldots, \theta^{n-1}] = \det \begin{pmatrix} 1 & \theta_1 & \theta_1^2 & \ldots & \theta_1^{n-1} \\ 1 & \theta_2 & \theta_2^2 & \ldots & \theta_2^{n-1} \\ 1 & \theta_3 & \theta_3^2 & \ldots & \theta_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \theta_n & \theta_n^2 & \ldots & \theta_n^{n-1} \end{pmatrix}^2$$

Proof of the discriminant theorem

Proof.

$$\Delta[1,\theta,\ldots,\theta^{n-1}] = \det\begin{pmatrix} 1 & \theta_1 & \theta_1^2 & \ldots & \theta_1^{n-1} \\ 1 & \theta_2 & \theta_2^2 & \ldots & \theta_2^{n-1} \\ 1 & \theta_3 & \theta_3^2 & \ldots & \theta_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \theta_n & \theta_n^2 & \ldots & \theta_n^{n-1} \end{pmatrix}^2 = \prod_{1\le i<j\le n} (\theta_j - \theta_i)^2.$$

Proof of the discriminant theorem

Proof.

$$\Delta[1, \theta, \ldots, \theta^{n-1}] = \det \begin{pmatrix} 1 & \theta_1 & \theta_1^2 & \ldots & \theta_1^{n-1} \\ 1 & \theta_2 & \theta_2^2 & \ldots & \theta_2^{n-1} \\ 1 & \theta_3 & \theta_3^2 & \ldots & \theta_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \theta_n & \theta_n^2 & \ldots & \theta_n^{n-1} \end{pmatrix}^2 = \prod_{1 \le i < j \le n} (\theta_j - \theta_i)^2.$$

Letting C be the change of basis matrix from $1, \theta, \ldots, \theta^{n-1}$ to $\alpha_1, \ldots, \alpha_n$,

Proof of the discriminant theorem

Proof.

$$\Delta[1,\theta,\ldots,\theta^{n-1}] = \det\begin{pmatrix} 1 & \theta_1 & \theta_1^2 & \ldots & \theta_1^{n-1} \\ 1 & \theta_2 & \theta_2^2 & \ldots & \theta_2^{n-1} \\ 1 & \theta_3 & \theta_3^2 & \ldots & \theta_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \theta_n & \theta_n^2 & \ldots & \theta_n^{n-1} \end{pmatrix}^2 = \prod_{1\le i<j\le n}(\theta_j-\theta_i)^2.$$

Letting C be the change of basis matrix from $1,\theta,\ldots,\theta^{n-1}$ to $\alpha_1,\ldots,\alpha_n$, we have

$$\Delta[\alpha_1,\ldots,\alpha_n] = (\det C)^2\Delta[1,\theta,\ldots,\theta^{n-1}] = (\det C)^2\prod_{1\le i<j\le n}(\theta_j-\theta_i)^2.$$

Proof of the discriminant theorem

So far we have

$$\Delta[\alpha_1, \ldots, \alpha_n] = (\det C)^2 \prod_{1 \le i < j \le n} (\theta_i - \theta_j)^2.$$

Proof of the discriminant theorem

So far we have

$$\Delta[\alpha_1, \ldots, \alpha_n] = (\det C)^2 \prod_{1 \le i < j \le n} (\theta_i - \theta_j)^2.$$

Key idea: note that $\Delta[\alpha_1, \ldots, \alpha_n]$ is a symmetric polynomial in the θ_i.

Proof of the discriminant theorem

So far we have

$$\Delta[\alpha_1, \ldots, \alpha_n] = (\det C)^2 \prod_{1 \le i < j \le n} (\theta_i - \theta_j)^2.$$

Key idea: note that $\Delta[\alpha_1, \ldots, \alpha_n]$ is a symmetric polynomial in the θ_i. Let $p = \prod_{i=1}^{n}(x - \theta_i)$ be the minimal polynomial for θ over $\mathbb{Q}$.

Proof of the discriminant theorem

So far we have

$$\Delta[\alpha_1, \ldots, \alpha_n] = (\det C)^2 \prod_{1 \le i < j \le n} (\theta_i - \theta_j)^2.$$

Key idea: note that $\Delta[\alpha_1, \ldots, \alpha_n]$ is a symmetric polynomial in the θ_i. Let $p = \prod_{i=1}^{n}(x - \theta_i)$ be the minimal polynomial for θ over $\mathbb{Q}$. The symmetric polynomials in the θ_i are, up to sign, the coefficients of p,

Proof of the discriminant theorem

So far we have

$$\Delta[\alpha_1, \ldots, \alpha_n] = (\det C)^2 \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j)^2.$$

Key idea: note that $\Delta[\alpha_1, \ldots, \alpha_n]$ is a symmetric polynomial in the θ_i. Let $p = \prod_{i=1}^{n}(x - \theta_i)$ be the minimal polynomial for θ over $\mathbb{Q}$. The symmetric polynomials in the θ_i are, up to sign, the coefficients of p, which are rational.

Proof of the discriminant theorem

So far we have

$$\Delta[\alpha_1, \ldots, \alpha_n] = (\det C)^2 \prod_{1 \le i < j \le n} (\theta_i - \theta_j)^2.$$

Key idea: note that $\Delta[\alpha_1, \ldots, \alpha_n]$ is a symmetric polynomial in the θ_i. Let $p = \prod_{i=1}^{n}(x - \theta_i)$ be the minimal polynomial for θ over $\mathbb{Q}$. The symmetric polynomials in the θ_i are, up to sign, the coefficients of p, which are rational. The entries in C are rational.

Proof of the discriminant theorem

So far we have

$$\Delta[\alpha_1, \ldots, \alpha_n] = (\det C)^2 \prod_{1 \le i < j \le n} (\theta_i - \theta_j)^2.$$

Key idea: note that $\Delta[\alpha_1, \ldots, \alpha_n]$ is a symmetric polynomial in the θ_i. Let $p = \prod_{i=1}^{n}(x - \theta_i)$ be the minimal polynomial for θ over $\mathbb{Q}$. The symmetric polynomials in the θ_i are, up to sign, the coefficients of p, which are rational. The entries in C are rational. Hence, the discriminant is rational.

Proof of the discriminant theorem

So far we have

$$\Delta[\alpha_1, \ldots, \alpha_n] = (\det C)^2 \prod_{1 \le i < j \le n} (\theta_i - \theta_j)^2.$$

Key idea: note that $\Delta[\alpha_1, \ldots, \alpha_n]$ is a symmetric polynomial in the θ_i. Let $p = \prod_{i=1}^{n}(x - \theta_i)$ be the minimal polynomial for θ over $\mathbb{Q}$. The symmetric polynomials in the θ_i are, up to sign, the coefficients of p, which are rational. The entries in C are rational. Hence, the discriminant is rational.

Its positive if the θ_i are real (why?).

Proof of the discriminant theorem

So far we have

$$\Delta[\alpha_1, \ldots, \alpha_n] = (\det C)^2 \prod_{1 \le i < j \le n} (\theta_i - \theta_j)^2.$$

Key idea: note that $\Delta[\alpha_1, \ldots, \alpha_n]$ is a symmetric polynomial in the θ_i. Let $p = \prod_{i=1}^{n}(x - \theta_i)$ be the minimal polynomial for θ over $\mathbb{Q}$. The symmetric polynomials in the θ_i are, up to sign, the coefficients of p, which are rational. The entries in C are rational. Hence, the discriminant is rational.

Its positive if the θ_i are real (why?).

Finally, what can we say if each α_i is an algebraic integer? (See next page.)

Proof of the discriminant theorem

$$\Delta[\alpha_1, \ldots, \alpha_n] = \det(\sigma_i(\alpha_j))^2 = (\det C)^2 \prod_{1 \le i < j \le n} (\theta_i - \theta_j)^2.$$

Proof of the discriminant theorem

$$\Delta[\alpha_1, \ldots, \alpha_n] = \det(\sigma_i(\alpha_j))^2 = (\det C)^2 \prod_{1 \le i < j \le n} (\theta_i - \theta_j)^2.$$

Suppose that each α_i is an algebraic integer.

Proof of the discriminant theorem

$$\Delta[\alpha_1, \ldots, \alpha_n] = \det(\sigma_i(\alpha_j))^2 = (\det C)^2 \prod_{1 \le i < j \le n} (\theta_i - \theta_j)^2.$$

Suppose that each α_i is an algebraic integer. Then the $\sigma_i(\alpha_j)$ are algebraic integers. (Why? Start with the definition of an algebraic integer.)

Proof of the discriminant theorem

$$\Delta[\alpha_1, \ldots, \alpha_n] = \det(\sigma_i(\alpha_j))^2 = (\det C)^2 \prod_{1 \le i < j \le n} (\theta_i - \theta_j)^2.$$

Suppose that each α_i is an algebraic integer. Then the $\sigma_i(\alpha_j)$ are algebraic integers. (Why? Start with the definition of an algebraic integer.)

We have seen that the algebraic integers in K form a ring.

Proof of the discriminant theorem

$$\Delta[\alpha_1, \ldots, \alpha_n] = \det(\sigma_i(\alpha_j))^2 = (\det C)^2 \prod_{1 \le i < j \le n} (\theta_i - \theta_j)^2.$$

Suppose that each α_i is an algebraic integer. Then the $\sigma_i(\alpha_j)$ are algebraic integers. (Why? Start with the definition of an algebraic integer.)

We have seen that the algebraic integers in K form a ring. Hence, the discriminant $\det(\sigma_i(\alpha_j))^2$ is an algebraic integer.

Proof of the discriminant theorem

$$\Delta[\alpha_1, \ldots, \alpha_n] = \det(\sigma_i(\alpha_j))^2 = (\det C)^2 \prod_{1 \le i < j \le n} (\theta_i - \theta_j)^2.$$

Suppose that each α_i is an algebraic integer. Then the $\sigma_i(\alpha_j)$ are algebraic integers. (Why? Start with the definition of an algebraic integer.)

We have seen that the algebraic integers in K form a ring. Hence, the discriminant $\det(\sigma_i(\alpha_j))^2$ is an algebraic integer. However, we have just seen that it is a rational number.

Proof of the discriminant theorem

$$\Delta[\alpha_1, \ldots, \alpha_n] = \det(\sigma_i(\alpha_j))^2 = (\det C)^2 \prod_{1 \le i < j \le n} (\theta_i - \theta_j)^2.$$

Suppose that each α_i is an algebraic integer. Then the $\sigma_i(\alpha_j)$ are algebraic integers. (Why? Start with the definition of an algebraic integer.)

We have seen that the algebraic integers in K form a ring. Hence, the discriminant $\det(\sigma_i(\alpha_j))^2$ is an algebraic integer. However, we have just seen that it is a rational number. We also know that if a rational number is integral over $\mathbb{Q}$, then it must be an ordinary integer. □

The $\mathbb{Z}$-module rank of $\mathfrak{O}_K$

Theorem. Let K be a number field of degree n over $\mathbb{Q}$, i.e., $[K : \mathbb{Q}] = n$. Then its ring of integers $\mathfrak{O}_K$ is a free $\mathbb{Z}$-module of rank n.

The $\mathbb{Z}$-module rank of $\mathfrak{O}_K$

Theorem. Let K be a number field of degree n over $\mathbb{Q}$, i.e., $[K:\mathbb{Q}] = n$. Then its ring of integers $\mathfrak{O}_K$ is a free $\mathbb{Z}$-module of rank n.

Proof. Write $K = \mathbb{Q}(\theta)$ where θ is an algebraic integer.

The $\mathbb{Z}$-module rank of $\mathfrak{O}_K$

Theorem. Let K be a number field of degree n over $\mathbb{Q}$, i.e., $[K : \mathbb{Q}] = n$. Then its ring of integers $\mathfrak{O}_K$ is a free $\mathbb{Z}$-module of rank n.

Proof. Write $K = \mathbb{Q}(\theta)$ where θ is an algebraic integer. Then $\{1, \theta, \ldots, \theta^{n-1}\}$ is a $\mathbb{Q}$-basis of K consisting of algebraic integers.

The $\mathbb{Z}$-module rank of $\mathfrak{O}_K$

Theorem. Let K be a number field of degree n over $\mathbb{Q}$, i.e., $[K : \mathbb{Q}] = n$. Then its ring of integers $\mathfrak{O}_K$ is a free $\mathbb{Z}$-module of rank n.

Proof. Write $K = \mathbb{Q}(\theta)$ where θ is an algebraic integer. Then $\{1, \theta, \ldots, \theta^{n-1}\}$ is a $\mathbb{Q}$-basis of K consisting of algebraic integers. So its discriminant is

The $\mathbb{Z}$-module rank of $\mathfrak{O}_K$

Theorem. Let K be a number field of degree n over $\mathbb{Q}$, i.e., $[K : \mathbb{Q}] = n$. Then its ring of integers $\mathfrak{O}_K$ is a free $\mathbb{Z}$-module of rank n.

Proof. Write $K = \mathbb{Q}(\theta)$ where θ is an algebraic integer. Then $\{1, \theta, \ldots, \theta^{n-1}\}$ is a $\mathbb{Q}$-basis of K consisting of algebraic integers. So its discriminant is an integer.

The $\mathbb{Z}$-module rank of $\mathfrak{O}_K$

Theorem. Let K be a number field of degree n over $\mathbb{Q}$, i.e., $[K : \mathbb{Q}] = n$. Then its ring of integers $\mathfrak{O}_K$ is a free $\mathbb{Z}$-module of rank n.

Proof. Write $K = \mathbb{Q}(\theta)$ where θ is an algebraic integer. Then $\{1, \theta, \ldots, \theta^{n-1}\}$ is a $\mathbb{Q}$-basis of K consisting of algebraic integers. So its discriminant is an integer.

Among all $\mathbb{Q}$-bases for K consisting of algebraic integers, choose one, $\{\alpha_1, \ldots, \alpha_n\}$, such that $|\Delta[\alpha_1, \ldots, \alpha_n]|$ is smallest.

The $\mathbb{Z}$-module rank of $\mathfrak{O}_K$

Theorem. Let K be a number field of degree n over $\mathbb{Q}$, i.e., $[K : \mathbb{Q}] = n$. Then its ring of integers $\mathfrak{O}_K$ is a free $\mathbb{Z}$-module of rank n.

Proof. Write $K = \mathbb{Q}(\theta)$ where θ is an algebraic integer. Then $\{1, \theta, \ldots, \theta^{n-1}\}$ is a $\mathbb{Q}$-basis of K consisting of algebraic integers. So its discriminant is an integer.

Among all $\mathbb{Q}$-bases for K consisting of algebraic integers, choose one, $\{\alpha_1, \ldots, \alpha_n\}$, such that $|\Delta[\alpha_1, \ldots, \alpha_n]|$ is smallest.

For sake of contradiction, suppose that $\{\alpha_1, \ldots, \alpha_n\}$ is not a $\mathbb{Z}$-basis for $\mathfrak{O}_K$.

The $\mathbb{Z}$-module rank of $\mathfrak{O}_K$

Theorem. Let K be a number field of degree n over $\mathbb{Q}$, i.e., $[K : \mathbb{Q}] = n$. Then its ring of integers $\mathfrak{O}_K$ is a free $\mathbb{Z}$-module of rank n.

Proof. Write $K = \mathbb{Q}(\theta)$ where θ is an algebraic integer. Then $\{1, \theta, \ldots, \theta^{n-1}\}$ is a $\mathbb{Q}$-basis of K consisting of algebraic integers. So its discriminant is an integer.

Among all $\mathbb{Q}$-bases for K consisting of algebraic integers, choose one, $\{\alpha_1, \ldots, \alpha_n\}$, such that $|\Delta[\alpha_1, \ldots, \alpha_n]|$ is smallest.

For sake of contradiction, suppose that $\{\alpha_1, \ldots, \alpha_n\}$ is not a $\mathbb{Z}$-basis for $\mathfrak{O}_K$. Then there exists $\alpha \in \mathfrak{O}_K$ such that

$$\alpha = c_1\alpha_1 + \cdots + c_n\alpha_n$$

with $c_i \in \mathbb{Q}$ but with not all $c_i \in \mathbb{Z}$.

The $\mathbb{Z}$-module rank of $\mathfrak{O}_K$

Theorem. Let K be a number field of degree n over $\mathbb{Q}$, i.e., $[K:\mathbb{Q}] = n$. Then its ring of integers $\mathfrak{O}_K$ is a free $\mathbb{Z}$-module of rank n.

Proof. Write $K = \mathbb{Q}(\theta)$ where θ is an algebraic integer. Then $\{1, \theta, \ldots, \theta^{n-1}\}$ is a $\mathbb{Q}$-basis of K consisting of algebraic integers. So its discriminant is an integer.

Among all $\mathbb{Q}$-bases for K consisting of algebraic integers, choose one, $\{\alpha_1, \ldots, \alpha_n\}$, such that $|\Delta[\alpha_1, \ldots, \alpha_n]|$ is smallest.

For sake of contradiction, suppose that $\{\alpha_1, \ldots, \alpha_n\}$ is not a $\mathbb{Z}$-basis for $\mathfrak{O}_K$. Then there exists $\alpha \in \mathfrak{O}_K$ such that

$$\alpha = c_1\alpha_1 + \cdots + c_n\alpha_n$$

with $c_i \in \mathbb{Q}$ but with not all $c_i \in \mathbb{Z}$. Without loss of generality, suppose $c_1 \in \mathbb{Q} \setminus \mathbb{Z}$.

The $\mathbb{Z}$-module rank of $\mathfrak{O}_K$

We have $\alpha \in \mathfrak{O}_K$ such that

$$\alpha = c_1\alpha_1 + \cdots + c_n\alpha_n$$

with $c_1 \in \mathbb{Q} \setminus \mathbb{Z}$.

The $\mathbb{Z}$-module rank of $\mathfrak{O}_K$

We have $\alpha \in \mathfrak{O}_K$ such that

$$\alpha = c_1\alpha_1 + \cdots + c_n\alpha_n$$

with $c_1 \in \mathbb{Q} \setminus \mathbb{Z}$.

Write $c_1 = c + r$ where $c = \lfloor c_1 \rfloor$ and $0 < r < 1$.

The $\mathbb{Z}$-module rank of $\mathfrak{O}_K$

We have $\alpha \in \mathfrak{O}_K$ such that

$$\alpha = c_1\alpha_1 + \cdots + c_n\alpha_n$$

with $c_1 \in \mathbb{Q} \setminus \mathbb{Z}$.

Write $c_1 = c + r$ where $c = \lfloor c_1 \rfloor$ and $0 < r < 1$. Then

$$\alpha = (c + r)\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n.$$

The $\mathbb{Z}$-module rank of $\mathfrak{O}_K$

We have $\alpha \in \mathfrak{O}_K$ such that

$$\alpha = c_1\alpha_1 + \cdots + c_n\alpha_n$$

with $c_1 \in \mathbb{Q} \setminus \mathbb{Z}$.
Write $c_1 = c + r$ where $c = \lfloor c_1 \rfloor$ and $0 < r < 1$. Then

$$\alpha = (c + r)\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n.$$

Define

$$\alpha_1' = \alpha - c\alpha_1 =$$

The $\mathbb{Z}$-module rank of $\mathfrak{O}_K$

We have $\alpha \in \mathfrak{O}_K$ such that

$$\alpha = c_1\alpha_1 + \cdots + c_n\alpha_n$$

with $c_1 \in \mathbb{Q} \setminus \mathbb{Z}$.

Write $c_1 = c + r$ where $c = \lfloor c_1 \rfloor$ and $0 < r < 1$. Then

$$\alpha = (c + r)\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n.$$

Define

$$\alpha_1' = \alpha - c\alpha_1 = r\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n.$$

The $\mathbb{Z}$-module rank of $\mathfrak{O}_K$

We have $\alpha \in \mathfrak{O}_K$ such that

$$\alpha = c_1\alpha_1 + \cdots + c_n\alpha_n$$

with $c_1 \in \mathbb{Q} \setminus \mathbb{Z}$.

Write $c_1 = c + r$ where $c = \lfloor c_1 \rfloor$ and $0 < r < 1$. Then

$$\alpha = (c + r)\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n.$$

Define

$$\alpha_1' = \alpha - c\alpha_1 = r\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n.$$

Then

- α_1' is an algebraic integer. (Why?)

The $\mathbb{Z}$-module rank of $\mathfrak{O}_K$

We have $\alpha \in \mathfrak{O}_K$ such that

$$\alpha = c_1\alpha_1 + \cdots + c_n\alpha_n$$

with $c_1 \in \mathbb{Q} \setminus \mathbb{Z}$.

Write $c_1 = c + r$ where $c = \lfloor c_1 \rfloor$ and $0 < r < 1$. Then

$$\alpha = (c + r)\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n.$$

Define

$$\alpha_1' = \alpha - c\alpha_1 = r\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n.$$

Then

- α_1' is an algebraic integer. (Why?)
- $\{\alpha_1', \alpha_2, \ldots, \alpha_n\}$ is a $\mathbb{Q}$-basis for K consisting of algebraic integers.

The $\mathbb{Z}$-module rank of $\mathfrak{O}_K$

Compare the discriminant of $\{\alpha_1', \alpha_2, \ldots, \alpha_n\}$ to that of $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$.

The $\mathbb{Z}$-module rank of $\mathfrak{O}_K$

Compare the discriminant of $\{\alpha_1', \alpha_2, \ldots, \alpha_n\}$ to that of $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$. Recall

$$\alpha_1' = \alpha - c\alpha_1 =$$

The $\mathbb{Z}$-module rank of $\mathfrak{O}_K$

Compare the discriminant of $\{\alpha_1', \alpha_2, \ldots, \alpha_n\}$ to that of $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$. Recall

$$\alpha_1' = \alpha - c\alpha_1 = r\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n$$

with $0 < r < 1$.

The $\mathbb{Z}$-module rank of $\mathfrak{O}_K$

Compare the discriminant of $\{\alpha_1', \alpha_2, \ldots, \alpha_n\}$ to that of $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$. Recall

$$\alpha_1' = \alpha - c\alpha_1 = r\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n$$

with $0 < r < 1$.

Let C denote the change of basis matrix:

$$\begin{pmatrix} \alpha_1' \\ \alpha_2 \\ \alpha_3 \\ \vdots \\ \alpha_n \end{pmatrix} = \underbrace{\begin{pmatrix} r & c_2 & c_3 & \ldots & c_n \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix}}_{C} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \vdots \\ \alpha_n \end{pmatrix}.$$

The $\mathbb{Z}$-module rank of $\mathfrak{O}_K$

Since

$$\begin{pmatrix} \alpha_1' \\ \alpha_2 \\ \alpha_3 \\ \vdots \\ \alpha_n \end{pmatrix} = \underbrace{\begin{pmatrix} r & c_2 & c_3 & \dots & c_n \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}}_{C} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \vdots \\ \alpha_n \end{pmatrix},$$

The $\mathbb{Z}$-module rank of $\mathfrak{O}_K$

Since

$$\begin{pmatrix} \alpha_1' \\ \alpha_2 \\ \alpha_3 \\ \vdots \\ \alpha_n \end{pmatrix} = \underbrace{\begin{pmatrix} r & c_2 & c_3 & \dots & c_n \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}}_{C} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \vdots \\ \alpha_n \end{pmatrix},$$

we have

$$|\Delta[\alpha_1', \alpha_2 \dots, \alpha_n]| = |(\det C)^2 \Delta[\alpha_1, \dots, \alpha_n]| = r^2 |\Delta[\alpha_1, \dots, \alpha_n]|$$

The $\mathbb{Z}$-module rank of $\mathfrak{O}_K$

Since

$$\begin{pmatrix} \alpha_1' \\ \alpha_2 \\ \alpha_3 \\ \vdots \\ \alpha_n \end{pmatrix} = \underbrace{\begin{pmatrix} r & c_2 & c_3 & \dots & c_n \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}}_{C} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \vdots \\ \alpha_n \end{pmatrix},$$

we have

$$|\Delta[\alpha_1', \alpha_2 \dots, \alpha_n]| = |(\det C)^2 \Delta[\alpha_1, \dots, \alpha_n]| = r^2 |\Delta[\alpha_1, \dots, \alpha_n]|$$

contradicting the minimality of $|\Delta[\alpha_1, \dots, \alpha_n]|$. The result follows.
□

The discriminant of a number field

Proposition. Let K be a number field. Then all integral bases for $\mathfrak{O}_K$ have the same discriminant.

The discriminant of a number field

Proposition. Let K be a number field. Then all integral bases for $\mathfrak{O}_K$ have the same discriminant.

Proof. Suppose that $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ are two.

The discriminant of a number field

Proposition. Let K be a number field. Then all integral bases for $\mathfrak{O}_K$ have the same discriminant.

Proof. Suppose that $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ are two. Then each α_i can be uniquely written as a $\mathbb{Z}$-linear combination of the β_j, and vice versa.

The discriminant of a number field

Proposition. Let K be a number field. Then all integral bases for $\mathfrak{O}_K$ have the same discriminant.

Proof. Suppose that $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ are two. Then each α_i can be uniquely written as a $\mathbb{Z}$-linear combination of the β_j, and vice versa. Let C be the change of basis matrix from the α_i to the β_i, and let D be the change of basis matrix from the β_i to the α_i.

The discriminant of a number field

Proposition. Let K be a number field. Then all integral bases for $\mathfrak{O}_K$ have the same discriminant.

Proof. Suppose that $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ are two. Then each α_i can be uniquely written as a $\mathbb{Z}$-linear combination of the β_j, and vice versa. Let C be the change of basis matrix from the α_i to the β_i, and let D be the change of basis matrix from the β_i to the α_i. Then both C and D have integer entries,

The discriminant of a number field

Proposition. Let K be a number field. Then all integral bases for $\mathfrak{O}_K$ have the same discriminant.

Proof. Suppose that $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ are two. Then each α_i can be uniquely written as a $\mathbb{Z}$-linear combination of the β_j, and vice versa. Let C be the change of basis matrix from the α_i to the β_i, and let D be the change of basis matrix from the β_i to the α_i. Then both C and D have integer entries, and $CD = I_n$.

The discriminant of a number field

Proposition. Let K be a number field. Then all integral bases for $\mathfrak{O}_K$ have the same discriminant.

Proof. Suppose that $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ are two. Then each α_i can be uniquely written as a $\mathbb{Z}$-linear combination of the β_j, and vice versa. Let C be the change of basis matrix from the α_i to the β_i, and let D be the change of basis matrix from the β_i to the α_i. Then both C and D have integer entries, and $CD = I_n$. So $D = C^{-1}$, which shows that the inverse of C also has integer entries.

The discriminant of a number field

Proposition. Let K be a number field. Then all integral bases for $\mathfrak{O}_K$ have the same discriminant.

Proof. Suppose that $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ are two. Then each α_i can be uniquely written as a $\mathbb{Z}$-linear combination of the β_j, and vice versa. Let C be the change of basis matrix from the α_i to the β_i, and let D be the change of basis matrix from the β_i to the α_i. Then both C and D have integer entries, and $CD = I_n$. So $D = C^{-1}$, which shows that the inverse of C also has integer entries. Further, $I_n = CD \Rightarrow 1 = \det(C)\det(D)$,

The discriminant of a number field

Proposition. Let K be a number field. Then all integral bases for $\mathfrak{O}_K$ have the same discriminant.

Proof. Suppose that $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ are two. Then each α_i can be uniquely written as a $\mathbb{Z}$-linear combination of the β_j, and vice versa. Let C be the change of basis matrix from the α_i to the β_i, and let D be the change of basis matrix from the β_i to the α_i. Then both C and D have integer entries, and $CD = I_n$. So $D = C^{-1}$, which shows that the inverse of C also has integer entries. Further, $I_n = CD \Rightarrow 1 = \det(C)\det(D)$, which implies $\det(C) = \pm 1$ (why?).

The discriminant of a number field

Proposition. Let K be a number field. Then all integral bases for $\mathfrak{O}_K$ have the same discriminant.

Proof. Suppose that $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ are two. Then each α_i can be uniquely written as a $\mathbb{Z}$-linear combination of the β_j, and vice versa. Let C be the change of basis matrix from the α_i to the β_i, and let D be the change of basis matrix from the β_i to the α_i. Then both C and D have integer entries, and $CD = I_n$. So $D = C^{-1}$, which shows that the inverse of C also has integer entries. Further, $I_n = CD \Rightarrow 1 = \det(C)\det(D)$, which implies $\det(C) = \pm 1$ (why?). It follows that

$$\Delta[\beta_i, \ldots, \beta_n] = \det(C)^2 \Delta[\alpha_1, \ldots, \alpha_n] = \Delta[\alpha_1, \ldots, \alpha_n].$$

□

The discriminant of a number field

Definition. The *discriminant* of a number field K, denoted $\Delta(K)$ is the discriminant of any integral basis for $\mathfrak{O}_K$.

The discriminant of a number field

Definition. The *discriminant* of a number field K, denoted $\Delta(K)$ is the discriminant of any integral basis for $\mathfrak{O}_K$.

Example. Let $K = \mathbb{Q}(\sqrt{d})$ where $d \in \mathbb{Z}$ and $d \neq 0, 1$.

The discriminant of a number field

Definition. The *discriminant* of a number field K, denoted $\Delta(K)$ is the discriminant of any integral basis for $\mathfrak{O}_K$.

Example. Let $K = \mathbb{Q}(\sqrt{d})$ where $d \in \mathbb{Z}$ and $d \neq 0, 1$. We have seen that $\{1, \sqrt{d}\}$ is an integral basis for $\mathfrak{O}_K$ if $d \not\equiv 1 \bmod 4$,

The discriminant of a number field

Definition. The *discriminant* of a number field K, denoted $\Delta(K)$ is the discriminant of any integral basis for $\mathfrak{O}_K$.

Example. Let $K = \mathbb{Q}(\sqrt{d})$ where $d \in \mathbb{Z}$ and $d \neq 0, 1$. We have seen that $\{1, \sqrt{d}\}$ is an integral basis for $\mathfrak{O}_K$ if $d \neq 1$ mod 4, and $\{1, \frac{1+\sqrt{5}}{2}\}$ is an integral basis if $d = 1$ mod 4.

The discriminant of a number field

Definition. The *discriminant* of a number field K, denoted $\Delta(K)$ is the discriminant of any integral basis for $\mathfrak{O}_K$.

Example. Let $K = \mathbb{Q}(\sqrt{d})$ where $d \in \mathbb{Z}$ and $d \neq 0, 1$. We have seen that $\{1, \sqrt{d}\}$ is an integral basis for $\mathfrak{O}_K$ if $d \neq 1$ mod 4, and $\{1, \frac{1+\sqrt{5}}{2}\}$ is an integral basis if $d = 1$ mod 4. We have

$$\det \begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix} = -2\sqrt{d}$$

The discriminant of a number field

Definition. The *discriminant* of a number field K, denoted $\Delta(K)$ is the discriminant of any integral basis for $\mathfrak{O}_K$.

Example. Let $K = \mathbb{Q}(\sqrt{d})$ where $d \in \mathbb{Z}$ and $d \neq 0, 1$. We have seen that $\{1, \sqrt{d}\}$ is an integral basis for $\mathfrak{O}_K$ if $d \neq 1$ mod 4, and $\{1, \frac{1+\sqrt{5}}{2}\}$ is an integral basis if $d = 1$ mod 4. We have

$$\det \begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix} = -2\sqrt{d} \quad \text{and} \quad \begin{pmatrix} 1 & \frac{1+\sqrt{5}}{2} \\ 1 & \frac{1-\sqrt{5}}{2} \end{pmatrix} = -\sqrt{d}.$$

The discriminant of a number field

Definition. The *discriminant* of a number field K, denoted $\Delta(K)$ is the discriminant of any integral basis for $\mathfrak{O}_K$.

Example. Let $K = \mathbb{Q}(\sqrt{d})$ where $d \in \mathbb{Z}$ and $d \neq 0, 1$. We have seen that $\{1, \sqrt{d}\}$ is an integral basis for $\mathfrak{O}_K$ if $d \neq 1 \bmod 4$, and $\{1, \frac{1+\sqrt{5}}{2}\}$ is an integral basis if $d = 1 \bmod 4$. We have

$$\det \begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix} = -2\sqrt{d} \quad \text{and} \quad \begin{pmatrix} 1 & \frac{1+\sqrt{5}}{2} \\ 1 & \frac{1-\sqrt{5}}{2} \end{pmatrix} = -\sqrt{d}.$$

Therefore,

$$\Delta(K) = \begin{cases} 4d & \text{if } d \neq 1 \bmod 4 \\ d & \text{if } d = 1 \bmod 4. \end{cases}$$

Integral basis criterion

Proposition. Suppose that $\alpha_1, \ldots, \alpha_n$ is a $\mathbb{Q}$-basis for K consisting of algebraic integers.

Integral basis criterion

Proposition. Suppose that $\alpha_1, \ldots, \alpha_n$ is a $\mathbb{Q}$-basis for K consisting of algebraic integers. If $\Delta[\alpha_1, \ldots, \alpha_n]$ is square-free,

Integral basis criterion

Proposition. Suppose that $\alpha_1, \ldots, \alpha_n$ is a $\mathbb{Q}$-basis for K consisting of algebraic integers. If $\Delta[\alpha_1, \ldots, \alpha_n]$ is square-free, then $\alpha_1, \ldots, \alpha_n$ is a $\mathbb{Z}$-basis for $\mathfrak{O}_K$.

Integral basis criterion

Proposition. Suppose that $\alpha_1, \ldots, \alpha_n$ is a $\mathbb{Q}$-basis for K consisting of algebraic integers. If $\Delta[\alpha_1, \ldots, \alpha_n]$ is square-free, then $\alpha_1, \ldots, \alpha_n$ is a $\mathbb{Z}$-basis for $\mathfrak{O}_K$.

Proof. Let $\beta_{1,}, \ldots, \beta_n$ be an integral basis for $\mathfrak{O}_K$.

Integral basis criterion

Proposition. Suppose that $\alpha_1, \ldots, \alpha_n$ is a $\mathbb{Q}$-basis for K consisting of algebraic integers. If $\Delta[\alpha_1, \ldots, \alpha_n]$ is square-free, then $\alpha_1, \ldots, \alpha_n$ is a $\mathbb{Z}$-basis for $\mathfrak{O}_K$.

Proof. Let $\beta_{1,}, \ldots, \beta_n$ be an integral basis for $\mathfrak{O}_K$. Then since the α_i are algebraic integers, there exists an $n \times n$ matrix C with integer entries such that

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = C \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}.$$

Integral basis criterion

Proposition. Suppose that $\alpha_1, \ldots, \alpha_n$ is a $\mathbb{Q}$-basis for K consisting of algebraic integers. If $\Delta[\alpha_1, \ldots, \alpha_n]$ is square-free, then $\alpha_1, \ldots, \alpha_n$ is a $\mathbb{Z}$-basis for $\mathfrak{O}_K$.

Proof. Let $\beta_{1,}, \ldots, \beta_n$ be an integral basis for $\mathfrak{O}_K$. Then since the α_i are algebraic integers, there exists an $n \times n$ matrix C with integer entries such that

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = C \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}.$$

It follows that

$$\Delta[\alpha_1, \ldots, \alpha_n] = \det(C)^2 \Delta[\beta_1, \ldots, \beta_n].$$

Integral basis criterion

Continuing, recall that $\alpha_1, \ldots, \alpha_n$ is a $\mathbb{Q}$-basis for K consisting of algebraic integers, $\beta_1, \ldots, \beta_n$ is a $\mathbb{Z}$-basis for $\mathfrak{O}_K$, and

Integral basis criterion

Continuing, recall that $\alpha_1, \ldots, \alpha_n$ is a $\mathbb{Q}$-basis for K consisting of algebraic integers, $\beta_1, \ldots, \beta_n$ is a $\mathbb{Z}$-basis for $\mathfrak{O}_K$, and

$$\Delta[\alpha_1, \ldots, \alpha_n] = \det(C)^2 \Delta[\beta_1, \ldots, \beta_n].$$

Integral basis criterion

Continuing, recall that $\alpha_1, \ldots, \alpha_n$ is a $\mathbb{Q}$-basis for K consisting of algebraic integers, $\beta_1, \ldots, \beta_n$ is a $\mathbb{Z}$-basis for $\mathfrak{O}_K$, and

$$\Delta[\alpha_1, \ldots, \alpha_n] = \det(C)^2 \Delta[\beta_1, \ldots, \beta_n].$$

Since $\Delta[\alpha_1, \ldots, \alpha_n]$ is square-free,

Integral basis criterion

Continuing, recall that $\alpha_1, \ldots, \alpha_n$ is a $\mathbb{Q}$-basis for K consisting of algebraic integers, $\beta_1, \ldots, \beta_n$ is a $\mathbb{Z}$-basis for $\mathfrak{O}_K$, and

$$\Delta[\alpha_1, \ldots, \alpha_n] = \det(C)^2 \Delta[\beta_1, \ldots, \beta_n].$$

Since $\Delta[\alpha_1, \ldots, \alpha_n]$ is square-free, $\det(C) = \pm 1$.

Integral basis criterion

Continuing, recall that $\alpha_1, \ldots, \alpha_n$ is a $\mathbb{Q}$-basis for K consisting of algebraic integers, $\beta_1, \ldots, \beta_n$ is a $\mathbb{Z}$-basis for $\mathfrak{O}_K$, and

$$\Delta[\alpha_1, \ldots, \alpha_n] = \det(C)^2 \Delta[\beta_1, \ldots, \beta_n].$$

Since $\Delta[\alpha_1, \ldots, \alpha_n]$ is square-free, $\det(C) = \pm 1$. This implies C^{-1} has integer entries (why?).

Integral basis criterion

Continuing, recall that $\alpha_1, \ldots, \alpha_n$ is a $\mathbb{Q}$-basis for K consisting of algebraic integers, $\beta_1, \ldots, \beta_n$ is a $\mathbb{Z}$-basis for $\mathfrak{O}_K$, and

$$\Delta[\alpha_1, \ldots, \alpha_n] = \det(C)^2 \Delta[\beta_1, \ldots, \beta_n].$$

Since $\Delta[\alpha_1, \ldots, \alpha_n]$ is square-free, $\det(C) = \pm 1$. This implies C^{-1} has integer entries (why?). Then

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = C \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} \Longrightarrow C^{-1} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}.$$

Integral basis criterion

Continuing, recall that $\alpha_1, \ldots, \alpha_n$ is a $\mathbb{Q}$-basis for K consisting of algebraic integers, $\beta_1, \ldots, \beta_n$ is a $\mathbb{Z}$-basis for $\mathfrak{O}_K$, and

$$\Delta[\alpha_1, \ldots, \alpha_n] = \det(C)^2 \Delta[\beta_1, \ldots, \beta_n].$$

Since $\Delta[\alpha_1, \ldots, \alpha_n]$ is square-free, $\det(C) = \pm 1$. This implies C^{-1} has integer entries (why?). Then

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = C \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} \Longrightarrow C^{-1} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}.$$

Hence, the β_i are integer linear combinations of that α_i.

Integral basis criterion

Continuing, recall that $\alpha_1, \ldots, \alpha_n$ is a $\mathbb{Q}$-basis for K consisting of algebraic integers, $\beta_1, \ldots, \beta_n$ is a $\mathbb{Z}$-basis for $\mathfrak{O}_K$, and

$$\Delta[\alpha_1, \ldots, \alpha_n] = \det(C)^2 \Delta[\beta_1, \ldots, \beta_n].$$

Since $\Delta[\alpha_1, \ldots, \alpha_n]$ is square-free, $\det(C) = \pm 1$. This implies C^{-1} has integer entries (why?). Then

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = C \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} \Longrightarrow C^{-1} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}.$$

Hence, the β_i are integer linear combinations of that α_i. It follows that the α_i form a $\mathbb{Z}$-basis for $\mathfrak{O}_K$. $\square$

True/False question

Let K be a number field.

True/False question

Let K be a number field.

1. By the primitive element theorem, there exists an algebraic number $\theta \in K$ such that $K = \mathbb{Q}(\theta)$. Is it always possible to take θ to be an algebraic integer?

True/False question

Let K be a number field.

1. By the primitive element theorem, there exists an algebraic number $\theta \in K$ such that $K = \mathbb{Q}(\theta)$. Is it always possible to take θ to be an algebraic integer?

2. In the case where $K = \mathbb{Q}(\theta)$ and θ is an algebraic integer, is $\{1, \theta, \ldots, \theta^{n-1}\}$ a $\mathbb{Z}$-module bases for $\mathfrak{O}_K$?