Algebraic Number Theory

Dr. Anuj Jakhar

Lectures 5-8

Indian Institute of Technology Bhilai

anujjakhar@iitbhilai.ac.in

August 11, 2021

Integral Basis and Discriminant

- Discriminant whose notion is due to Dedekind, is a basic invariant associated with an algebraic number field.
- Its computation is one of the most important problems in algebraic number theory.
- For an algebraic number field $K = \mathbb{Q}(\theta)$ with θ in the ring $\mathcal{O}_K$ of algebraic integers of K having $f(X)$ as its minimal polynomial over the field $\mathbb{Q}$ of rational numbers, the discriminant d_K of K and the discriminant[1] of the polynomial $f(X)$ are related by the formula

$$discr(f) = [\mathcal{O}_K : \mathbb{Z}[\theta]]^2 d_K.$$

So computation of d_K is closely connected with that of the index of the group $\mathbb{Z}[\theta]$ in $\mathcal{O}_K$.

[1] The discriminant of a monic polynomial of degree n having roots $\theta_1, \ldots, \theta_n$ is defined to be the product $\prod_{1 \le i < j \le n} \left(\theta_i - \theta_j\right)^2$.

- It will be shown that $\mathcal{O}_K$ is a free abelian group of rank equal to the degree of the extension $K/\mathbb{Q}$.
- A $\mathbb{Z}$-basis of the group $\mathcal{O}_K$ is called an integral basis of K.
- In this course, we shall describe explicit integral basis for quadratic, pure cubic[2] and cyclotomic extensions of $\mathbb{Q}$.

[2] By a pure cubic extension of $\mathbb{Q}$, we mean an algebraic number field $\mathbb{Q}(\theta)$ where θ is a root of an irreducible polynomial $X^3 - a$ over $\mathbb{Z}$.

Definition. For an algebraic number field K, the degree of the extension $K/\mathbb{Q}$ is called the degree of K and will be denoted by $[K : \mathbb{Q}]$.

- An algebraic number field of degree 2 is called a quadratic field and one of degree 3 is called a cubic field.
- Algebraic number fields of degrees 4, 5 and 6 are respectively referred to as quartic, quintic and sextic fields.
- A quadratic field K is called real or imaginary according as $K \subseteq \mathbb{R}$ or not.
- A subfield $\mathbb{Q}(\zeta)$ of $\mathbb{C}$, where ζ is a primitive nth root of unity is called the n-th cyclotomic field.

Notation. Let K be an algebraic number field of degree n and $\sigma_1, \sigma_2, \ldots, \sigma_n$ be all the distinct $\mathbb{Q}$-isomorphisms (to be called isomorphisms) of K into $\mathbb{C}$. For an element α belonging to K, we shall denote $\sigma_i(\alpha)$ by $\alpha^{(i)}$. Note that if $K = \mathbb{Q}(\alpha)$, then $\alpha^{(1)}, \ldots, \alpha^{(n)}$ are distinct.

Definition. Let K be an algebraic number field of degree n and let $\{w_1, \ldots, w_n\}$ be a basis of $K/\mathbb{Q}$ as a vector space. The square of the determinant of $n \times n$ matrix $\left(w_i^{(j)}\right)_{i,j}$ is called discriminant of the basis $\{w_1, \ldots, w_n\}$ and will be denoted by $D_{K/\mathbb{Q}}(w_1, \ldots, w_n)$.

The following lemma gives another expression for the discriminant of a basis.

Lemma 1. If $\{w_1, \ldots, w_n\}$ is a basis of an algebraic number field K as a vector space over $\mathbb{Q}$, then

$$D_{K/\mathbb{Q}}(w_1, \ldots, w_n) = \det\left(Tr_{K/\mathbb{Q}}(w_i w_j)\right)_{i,j}.$$

Proof.

- Let P denote the $n \times n$ matrix $\left(w_i^{(j)}\right)_{i,j}$ and P^t denote its transpose.
- By Theorem 16, we know that, $Tr_{K/\mathbb{Q}}(\alpha) = \alpha^{(1)} + \cdots + \alpha^{(n)}$ for α belonging to K.
- Keeping this in mind, one can check that $PP^t = \left(Tr_{K/\mathbb{Q}}(w_i w_j)\right)_{i,j}$. On taking determinant, the lemma is proved.

Remark. If $\{w_1, \ldots, w_n\}$ is as in the above lemma and if all w_i's belong to $\mathcal{O}_K$, then $D_{K/\mathbb{Q}}(w_1, \ldots, w_n)$ is in $\mathbb{Z}$, because $Tr_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ for α belonging to $\mathcal{O}_K$ in view of Corollary 18.

The next lemma relates the discriminant of two bases.

Lemma 2. Let K be an algebraic number field of degree n. If $\{w_1, w_2, \ldots, w_n\}$ and $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ are two bases of $K/\mathbb{Q}$ and C is the transition matrix from $\{w_1, w_2, \ldots, w_n\}$ to $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, then

$$D_{K/\mathbb{Q}}(\alpha_1, \alpha_2, \ldots, \alpha_n) = (\det C)^2 D_{K/\mathbb{Q}}(w_1, w_2, \ldots, w_n).$$

Proof. Write $C = (c_{ij})_{n\times n}$, then $\alpha_i = \sum_{j=1}^{n} c_{ij} w_j$; consequently

$$\alpha_i^{(r)} = \sum_{j=1}^{n} c_{ij} w_j^{(r)}, \quad 1 \leq i \leq n,\ 1 \leq r \leq n. \tag{1}$$

Denote the $n \times n$ matrices $\left(w_i^{(j)}\right)_{i,j}$ and $\left(\alpha_i^{(j)}\right)_{i,j}$ by P and Q respectively. We can rewrite the n^2 equations given by (1) in the matrix form as $Q = CP$. Taking determinant on both sides and then squaring, we obtain the desired equality.

We now see two important lemmas.

Lemma 3. Let $f(X) \in \mathbb{Q}[X]$ be a monic irreducible polynomial of degree n having a root θ in $\mathbb{C}$. If $K = \mathbb{Q}(\theta)$, then $D_{K/\mathbb{Q}}(1, \theta, \ldots, \theta^{n-1}) = \mathit{discr}(f)$.

Lemma 4. For an algebraic number field K, $D_{K/\mathbb{Q}}(w_1, w_2, \ldots, w_n)$ is non-zero for any basis $\{w_1, w_2, \ldots, w_n\}$ of $K/\mathbb{Q}$.

Note that if $\beta_1, \beta_2, \ldots, \beta_n$ are elements of an algebraic number field K of degree n which are linearly dependent over $\mathbb{Q}$, then the determinant of the matrix $\left(\beta_i^{(j)}\right)_{i,j}$ is zero, because if β_k is a $\mathbb{Q}$-linear combination of $\beta_1, \ldots, \beta_{k-1}$, then the kth row of the matrix $\left(\beta_i^{(j)}\right)_{i,j}$ is a linear combination of its first $k-1$ rows.

Proof of Lemma 3. Let $\sigma_1, \ldots, \sigma_n$ be all the distinct isomorphisms of K into $\mathbb{C}$. Then $\theta^{(i)} := \sigma_i(\theta)$ is a root of $f(X)$ for $1 \leq i \leq n$.

- Since these roots are distinct, $f(X) = \prod_{i=1}^{n} (X - \theta^{(i)})$.
- By definition of discriminant of a basis,

$$D_{K/\mathbb{Q}}(1, \theta, \ldots, \theta^{n-1}) = \begin{vmatrix} 1 & 1 & \ldots & 1 \\ \theta^{(1)} & \theta^{(2)} & \ldots & \theta^{(n)} \\ \vdots & \vdots & \ddots & \vdots \\ (\theta^{(1)})^{n-1} & (\theta^{(2)})^{n-1} & \ldots & (\theta^{(n)})^{n-1} \end{vmatrix}^2 .$$

- Keeping in mind the determinant of the Vandermonde matrix, we see that the right hand side of the above equation equals $\prod_{1 \leq i < j \leq n} (\theta^{(i)} - \theta^{(j)})^2$, which is the discriminant of $f(X)$.

Proof of Lemma 4. Write $K = \mathbb{Q}(\theta)$. Then $\theta^{(1)}, \ldots, \theta^{(n)}$ are distinct.

- Let C denote the transition matrix from a basis $\{w_1, w_2, \ldots, w_n\}$ of $K/\mathbb{Q}$ to $\{1, \theta, \ldots, \theta^{n-1}\}$.
- By Lemma 2, we have

$$D_{K/\mathbb{Q}}(1, \theta, \ldots, \theta^{n-1}) = (\det C)^2 D_{K/\mathbb{Q}}(w_1, w_2, \ldots, w_n).$$

- The desired result follows from above equation and Lemma 3, because

$$D_{K/\mathbb{Q}}(1, \theta, \ldots, \theta^{n-1}) = \prod_{1 \le i < j \le n} \left(\theta^{(i)} - \theta^{(j)}\right)^2,$$

which is different from zero.

The following lemma is very useful for computing $D_{K/\mathbb{Q}}(1, \theta, \ldots, \theta^{n-1})$.

Lemma 5. Let $K = \mathbb{Q}(\theta)$ be an algebraic number field of degree n and $f(X)$ be the minimal polynomial of θ over $\mathbb{Q}$. Then $D_{K/\mathbb{Q}}(1, \theta, \ldots, \theta^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(f'(\theta))$.

Proof of Lemma 5. Let $\sigma_1, \ldots, \sigma_n$ be all the distinct isomorphisms of K into $\mathbb{C}$. Then $\theta^{(i)} := \sigma_i(\theta)$ is a root of $f(X)$ for $1 \leq i \leq n$.

- Since these roots are distinct, $f(X) = \prod_{i=1}^{n} (X - \theta^{(i)})$. By Corollary 16,

$$N_{K/\mathbb{Q}}(f'(\theta)) = \prod_{i=1}^{n} \sigma_i(f'(\theta)) = \prod_{i=1}^{n} f'(\theta^{(i)}). \tag{2}$$

- In the equation $f'(X) = \sum_{j=1}^{n} \frac{f(X)}{(X - \theta^{(j)})}$, substituting $X = \theta^{(i)}$, we see that

$$f'(\theta^{(i)}) = \prod_{k=1, k \neq i}^{n} (\theta^{(i)} - \theta^{(k)}).$$

- Therefore it follows from (2) that

$$N_{K/\mathbb{Q}}(f'(\theta)) = \prod_{i=1}^{n} \prod_{k=1, k\neq i}^{n} (\theta^{(i)} - \theta^{(k)}). \tag{3}$$

- By Lemma 3, we have

$$D_{K/\mathbb{Q}}(1, \theta, \ldots, \theta^{n-1}) = \prod_{1\leq i<j\leq n} (\theta^{(i)} - \theta^{(j)})^2.$$

- On comparing the above equation with (3), we obtain the desired result.

Integral basis

Let K be an algebraic number field. A set $\{w_1, w_2, \ldots, w_n\}$ of algebraic integers in K is said to be an integral basis of K if every algebraic integer in K can be uniquely written as $a_1 w_1 + a_2 w_2 + \cdots + a_n w_n$ with a_i's in $\mathbb{Z}$.

The following theorem proves the existence of an integral basis.

Theorem 6. Let K be an algebraic number field of degree n. Then the following hold:

(i) K has an integral basis.

(ii) Any integral basis of K has n elements.

Definition. A square matrix with entries from $\mathbb{Z}$ is called unimodular if its determinant is ± 1. Equivalently a square matrix with entries in $\mathbb{Z}$ is called unimodular if its inverse has entries in $\mathbb{Z}$.

Proof of Theorem 6. Consider the set

$$S = \{|D_{K/\mathbb{Q}}(\beta_1, \beta_2, \ldots, \beta_n)| \mid \{\beta_1, \beta_2, \ldots, \beta_n\} \subseteq \mathcal{O}_K \text{ runs over bases of } K/\mathbb{Q}$$

- Observe that S is non-empty. By virtue of Lemma 4 and Remark after Lemma 1, S is a subset of the set of natural numbers.
- Therefore S has a smallest element, say l. So there exists a basis $\{w_1, w_2, \ldots, w_n\}$ of $K/\mathbb{Q}$ consisting of algebraic integers such that $|D_{K/\mathbb{Q}}(w_1, w_2, \ldots, w_n)| = l$, i.e.,

$$D_{K/\mathbb{Q}}(w_1, w_2, \ldots, w_n) = \pm l.$$

- Claim is that $\{w_1, w_2, \ldots, w_n\}$ is an integral basis of K.
- To prove the claim, it is enough to show that each α belonging to $\mathcal{O}_K$ can be written as $a_1 w_1 + a_2 w_2 + \cdots + a_n w_n$, with a_i's in $\mathbb{Z}$, because uniqueness is already there. Suppose to the contrary, there exists $\alpha \in \mathcal{O}_K$ such that $\alpha = \sum_{i=1}^{n} b_i w_i$, where b_i's belong to $\mathbb{Q}$ and at least one $b_i \notin \mathbb{Z}$.

- Assume without loss of generality that $b_1 \notin \mathbb{Z}$.
- We can write $b_1 = \lfloor b_1 \rfloor + q$, where $\lfloor b_1 \rfloor$ is the largest integer not exceeding b_1 and $0 < q < 1$, $q \in \mathbb{Q}$.
- Consider the element β_1 of $\mathcal{O}_K$ given by

$$\beta_1 = \alpha - \lfloor b_1 \rfloor w_1 = q w_1 + b_2 w_2 + \cdots + b_n w_n.$$

- Note that $\{\beta_1, w_2, \ldots, w_n\}$ is a basis of $K/\mathbb{Q}$ and consists of elements of $\mathcal{O}_K$.
- If C denotes the transition matrix from $\{w_1, w_2, \ldots, w_n\}$ to $\{\beta_1, w_2, \ldots, w_n\}$, then by virtue of Lemma 2, we have

$$D_{K/\mathbb{Q}}(\beta_1, w_2, \ldots, w_n) = (\det C)^2 D_{K/\mathbb{Q}}(w_1, w_2, \ldots, w_n) = \pm q^2 I$$

and hence $\left|D_{K/\mathbb{Q}}(\beta_1, w_2, \ldots, w_n)\right| = q^2 I < I$. This contradicts the definition of I and hence the claim is proved.

- Assertion (ii) will be proved once we show that whenever $\mathcal{B}$ is an integral basis of K, then $\mathcal{B}$ is also a basis of the vector space $K/\mathbb{Q}$.
- It is enough to show that $\mathcal{B}$ generates K as a vector space over $\mathbb{Q}$.
- Let β be any element of K. Then by Theorem 5, there exists a non-zero integer r such that $r\beta \in \mathcal{O}_K$.
- So $r\beta$ can be written as a finite linear combination of elements of $\mathcal{B}$ with coefficients in $\mathbb{Z}$ and hence the result follows.

Definition. A square matrix with entries from $\mathbb{Z}$ is called unimodular if its determinant is ± 1. Equivalently a square matrix with entries in $\mathbb{Z}$ is called unimodular if its inverse has entries in $\mathbb{Z}$.

Definition (discriminant of K).

- Let K be an algebraic number field of degree n.
- Let $\{w_1, \ldots, w_n\}$ and $\{\alpha_1, \ldots, \alpha_n\}$ be two integral bases of K.
- Then there exist $n \times n$ matrices A and B with entries from $\mathbb{Z}$ such that

$$\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = A \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix} = B \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix},$$

  which implies that $AB = I$ and hence $\det A = \pm 1$.
- So by virtue of Lemma 2, $D_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)$
  $= (\det A)^2 D_{K/\mathbb{Q}}(w_1, \ldots, w_n) = D_{K/\mathbb{Q}}(w_1, \ldots, w_n)$.
- Therefore any two integral bases of K have the same discriminant.
- This common value of the discriminant is called the discriminant of the field K.
- We shall denote it by d_K.

The following basic lemma gives a criterion for a basis of $K/\mathbb{Q}$ to be an integral basis of K.

Lemma 7. Let K be an algebraic number field of degree n and $\beta_1, \beta_2, \ldots, \beta_n$ be algebraic integers in K which are linearly independent over $\mathbb{Q}$. Then the quotient $D_{K/\mathbb{Q}}(\beta_1, \beta_2, \ldots, \beta_n)/d_K$ is the square of an integer. In particular, if $D_{K/\mathbb{Q}}(\beta_1, \beta_2, \ldots, \beta_n) = d_K$, then $\beta_1, \beta_2, \ldots, \beta_n$ form an integral basis of K.

Proof of Lemma 7. Let $\{w_1, w_2, \ldots, w_n\}$ be an integral basis of K and C be the transition matrix from $\{w_1, w_2, \ldots, w_n\}$ to $\{\beta_1, \beta_2, \ldots, \beta_n\}$. Then C has entries in $\mathbb{Z}$.

- In view of Lemma 2, $D_{K/\mathbb{Q}}(\beta_1, \beta_2, \ldots, \beta_n) = (\det C)^2 d_K$.
- So $D_{K/\mathbb{Q}}(\beta_1, \beta_2, \ldots, \beta_n)/d_K$ is the square of an integer.
- If $D_{K/\mathbb{Q}}(\beta_1, \beta_2, \ldots, \beta_n) = d_K$, then C is a unimodular matrix and hence $\beta_1, \beta_2, \ldots, \beta_n$ form an integral basis of K.

First we determine explicitly the discriminant and an integral basis of a quadratic field. It can be easily seen that every quadratic field can be uniquely written as $\mathbb{Q}(\sqrt{d})$, where d is a squarefree integer.

Theorem 8. For a quadratic field $K = \mathbb{Q}(\sqrt{d})$ with d a squarefree integer, the following hold:

(i) If $d \equiv 2$ or $3 \mod 4$, then $\{1, \sqrt{d}\}$ is an integral basis of K and $d_K = 4d$.

(ii) If $d \equiv 1 \mod 4$, then $\{1, (1+\sqrt{d})/2\}$ is an integral basis of K and $d_K = d$.

Properties of Discriminant

Recall that if $A = (a_{ij})_{i,j}$ is an $n \times n$ matrix, then

$$\det A = \sum_{(j_1, j_2, \ldots, j_n)} a_{1j_1} a_{2j_2} \cdots a_{nj_n} - \sum_{(k_1, k_2, \ldots, k_n)} a_{1k_1} a_{2k_2} \cdots a_{nk_n} \ ,$$

where $(j_1, j_2, \ldots, j_n)$ runs over all even permutations of $\{1, 2, \ldots, n\}$ and $(k_1, k_2, \ldots, k_n)$ runs over all odd permutations of $\{1, 2, \ldots, n\}$.

The next theorem by Ludwig Stickelberger was first announced in the International Congress of Mathematicians held in Zurich in 1897. The present proof of this theorem was given by Schur in 1929.

Stickelberger's Theorem. For any algebraic number field K, its discriminant d_K is congruent to 0 or 1 modulo 4.

Definition. An isomorphism σ of an algebraic number field K into $\mathbb{C}$ will be called real if $\sigma(K) \subseteq \mathbb{R}$, otherwise it will be called non-real. Note that non-real isomorphisms of K occur in conjugate pairs.

The following theorem which determines the sign of the discriminant of an algebraic number field was first proved by Alexander von Brill in the year 1877.

Brill's Theorem. Let K be an algebraic number field of degree $n = r_1 + 2r_2$, where r_1 is the number of real isomorphisms of K and $2r_2$ is the number of non-real isomorphisms of K, then $(-1)^{r_2} d_K > 0$.

The next two lemmas besides being of independent interest will be used for finding the discriminant of algebraic number fields.

Lemma 9. Let M be a free abelian group with basis $\{w_1, \ldots, w_m\}$ having rank $m \geq 1$. Let N be a non-zero subgroup of M. Prove that after a suitable reordering of $w_1, \ldots, w_m$, there exists a basis $\{\eta_1, \ldots, \eta_k\}$ of N of the form

$$\begin{array}{lllllllll}
\eta_1 & = & c_{11}w_1 & + & c_{12}w_2 & + & \cdots & + & c_{1m}w_m \\
\eta_2 & = & & & c_{22}w_2 & + & \cdots & + & c_{2m}w_m \\
\vdots & & & & & \ddots & & & \vdots \\
\eta_k & = & & & & & c_{kk}w_k & + \cdots + & c_{km}w_m
\end{array}$$

with $c_{ij} \in \mathbb{Z}$, $c_{ii} > 0$ for $1 \leq i \leq k \leq m$.

Remark. If M and N are as in the above lemma and have the same rank, then without reordering $w_1, w_2, \ldots, w_m$, one can construct a basis of N of the type $\eta_1, \eta_2, \ldots, \eta_m$.

Lemma 10. If M is a free abelian group of finite rank and N is a subgroup of M such that $\text{rank}(N) = \text{rank}(M)$, then the index $[M : N]$ is finite and equals the absolute value of the determinant of the transition matrix from any basis of M to any basis of N.

For an algebraic number field K, the following theorem gives the index of a subgroup of $\mathcal{O}_K$ generated by a basis $\mathcal{B}$ of $K/\mathbb{Q}$ consisting of algebraic integers in terms of discriminant of $\mathcal{B}$ and d_K. This result is a refined version of Lemma 7.

Theorem 11. Let $\{\beta_1, \beta_2, \ldots, \beta_n\}$ be a basis of an algebraic number field K as a vector space over $\mathbb{Q}$ consisting of algebraic integers. Let N denote the free abelian group generated by $\beta_1, \beta_2, \ldots, \beta_n$. Then

$$[\mathcal{O}_K : N]^2 = D_{K/\mathbb{Q}}(\beta_1, \beta_2, \ldots, \beta_n)/d_K.$$

The following corollary is an immediate consequence of the last theorem.

Corollary 12. Let $K = \mathbb{Q}(\theta)$ be an algebraic number field of degree n with θ an algebraic integer. Then the index of the subgroup $\mathbb{Z}[\theta]$ in $\mathcal{O}_K$ is given by

$$[\mathcal{O}_K : \mathbb{Z}[\theta]]^2 = D_{K/\mathbb{Q}}(1, \theta, \ldots, \theta^{n-1})/d_K.$$

In the setup of the above corollary and by Lemma 3, $D_{K/\mathbb{Q}}(1, \theta, \ldots, \theta^{n-1}) = \mathit{discr}(f)$, where $f(X)$ is the minimal polynomial of θ over $\mathbb{Q}$. So the above equation may be rewritten as

$$\mathit{discr}(f) = [\mathcal{O}_K : \mathbb{Z}[\theta]]^2 d_K.$$

Notation. Let $K = \mathbb{Q}(\theta)$ be as in the above corollary. The index of the subgroup $\mathbb{Z}[\theta]$ in $\mathcal{O}_K$ is called the index of θ and will be denoted by $\operatorname{ind}\theta$.

Definition. An algebraic number field K of degree n is said to be monogenic if there exists an element $\theta \in \mathcal{O}_K$ such that $\{1, \theta, \ldots, \theta^{n-1}\}$ is an integral basis of K; an integral basis of the type $\{1, \theta, \ldots, \theta^{n-1}\}$ is called a power basis of K.

In view of Theorem 8, every quadratic field is monogenic. It will be shown that a cubic field of the type $\mathbb{Q}(\sqrt[3]{m})$ is also monogenic when m is a squarefree integer which is not congruent to ± 1 modulo 9. Also we will prove that every cyclotomic field is monogenic. In 1878, Dedekind showed that not every algebraic number field is monogenic by proving that the cubic field $K = \mathbb{Q}(\theta)$ with $\theta^3 - \theta^2 - 2\theta - 8 = 0$, is not monogenic.

The next result is sometimes useful for computing the discriminant and integral basis.

Theorem 13. Let $K = \mathbb{Q}(\theta)$ be an algebraic number field with θ an algebraic integer. If the minimal polynomial of θ over $\mathbb{Q}$ is an Eisenstein polynomial[3] with respect to a prime p, then p does not divide $\operatorname{ind}\theta$.

---

[3] A polynomial $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ with coefficients from $\mathbb{Z}$ is said to be an Eisenstein polynomial with respect to a prime p if $p \nmid a_n$, $p | a_i$ for $0 \leq i \leq n-1$ and $p^2 \nmid a_0$. Such a polynomial is irreducible over $\mathbb{Q}$.

Examples

1. Compute the discriminant and an integral basis of the field $K = \mathbb{Q}(\theta)$ where θ is a root of the polynomial $f(X) = X^3 - X + 1$.

- Observe that $f(X)$ is irreducible over $\mathbb{Q}$, because if $f(X)$ is reducible over $\mathbb{Q}$, then $f(X)$ has a rational root, say α_1. Since each root of $f(X)$ is an algebraic integer, $\alpha_1 \in \mathbb{Z}$. If α_2, α_3 are other roots of $f(X)$, then $\alpha_2\alpha_3 = \frac{-1}{\alpha_1} \in \mathbb{Q}$ and hence $\alpha_2\alpha_3 \in \mathbb{Z}$. Therefore $\alpha_1 = \pm 1$. But by direct verification, neither 1 nor -1 is a root of $f(X)$. This contradiction proves that $f(X)$ is irreducible over $\mathbb{Q}$.
- Applying Lemma 5, it can be easily seen that $D_{K/\mathbb{Q}}(1, \theta, \theta^2) = (-1)^{\frac{3(3-1)}{2}} N_{K/\mathbb{Q}}(f'(\theta)) = -N_{K/\mathbb{Q}}(3\theta^2 - 1) = -23$.
- Therefore by Lemma 7, $\{1, \theta, \theta^2\}$ is an integral basis of K and $d_K = -23$.

Note: the field K in the above example is the cubic field whose discriminant has smallest absolute value among all cubic fields.

2. Compute the discriminant and an integral basis of the field $K = \mathbb{Q}(\theta)$ where θ is a root of the polynomial $f(X) = X^3 - 2X^2 + 2$.

- Let $K = \mathbb{Q}(\theta)$ where θ is a root of the polynomial $f(X) = X^3 - 2X^2 + 2$ which is an Eisenstein polynomial with respect to the prime 2 and hence is irreducible over $\mathbb{Q}$.
- By Corollary 12 and Lemma 5, we have

$$d_K(\operatorname{ind}\theta)^2 = D_{K/\mathbb{Q}}(1, \theta, \theta^2) = -N_{K/\mathbb{Q}}(3\theta^2 - 4\theta) = -44,$$

  which shows that $\operatorname{ind}\theta$ divides 2.
- In view of Theorem 13, $\operatorname{ind}\theta$ is coprime to 2. We conclude that $\operatorname{ind}\theta$ equals 1, $d_K = -44$ and $\{1, \theta, \theta^2\}$ is an integral basis of K.

3. Compute the discriminant and an integral basis of the field $K = \mathbb{Q}(\theta)$ where θ is a root of the polynomial $f(X) = X^3 - 9X - 6$.

- Note that $f(X)$ is an Eisenstein polynomial w.r.t. the prime 3 and hence is irreducible over $\mathbb{Q}$.
- By Corollary 12 and Lemma 5, we see that

$$d_K(\operatorname{ind}\theta)^2 = D_{K/\mathbb{Q}}(1, \theta, \theta^2) = -N_{K/\mathbb{Q}}(3\theta^2 - 9) = 2^3 \cdot 3^5.$$

- It follows from the above equation and from Theorem 13 that $\operatorname{ind}\theta$ is 1 or 2.
- If $\operatorname{ind}\theta$ is 2, then $d_K = 2 \cdot 3^5$ which is impossible because $d_K \equiv 0$ or $1 \pmod 4$ by Stickelberger's theorem.
- So $\operatorname{ind}\theta$ is 1 and $d_K = 2^3 \cdot 3^5$.

Integral Basis and Discriminant of $\mathbb{Q}(\sqrt[3]{m})$

Theorem 14. Let $K = \mathbb{Q}(\theta)$ be a cubic field with $\theta^3 = m = ab^2$, where a, b are relatively prime squarefree integers. The following hold:

(i) If $m \not\equiv 1$ or $8 \pmod 9$, then $\{1, \theta, \theta^2/b\}$ is an integral basis of K and $d_K = -27a^2b^2$.

(ii) If $m \equiv 1 \pmod 9$, then $\{\theta, \theta^2/b, (1+\theta+\theta^2)/3\}$ is an integral basis of K and $d_K = -3a^2b^2$.

(iii) If $m \equiv 8 \pmod 9$, then $\{\theta, \theta^2/b, (1-\theta+\theta^2)/3\}$ is an integral basis of K and $d_K = -3a^2b^2$.

The following lemma is crucial step in the proof of the above theorem.

Lemma 15. Let $K = \mathbb{Q}(\theta)$ be a cubic field with $\theta^3 = m = ab^2$, where a, b are relatively prime squarefree integers. Then $d_K = -27a^2b^2$ if 3 divides ab and $d_K = -3^r a^2b^2$ with $r = 1$ or 3 when $3 \nmid ab$.

Integral Basis and Discriminant of Cyclotomic Fields

We first find the discriminant and an integral basis of cyclotomic fields generated by pth root of unity for a prime p. Recall that if ζ is a primitive nth root of unity, then the degree of the nth cyclotomic field $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$ is $\phi(n)$

Theorem 16. Let ζ be a primitive pth root of unity, p an odd prime. Then $\{1, \zeta, \ldots, \zeta^{p-2}\}$ is an integral basis of $K = \mathbb{Q}(\zeta)$ and $d_K = (-1)^{\frac{p-1}{2}} p^{p-2}$.

The argument used in the proof of the above theorem has been extended to prove the following more general theorem.

Theorem 17. Let ζ be a primitive (p^r)th root of unity, p any prime (odd or even), $p^r \geq 3$. Then $\{1, \zeta, \ldots, \zeta^{\phi(p^r)-1}\}$ is an integral basis of $K = \mathbb{Q}(\zeta)$ and $d_K = (-1)^{\frac{\phi(p^r)}{2}} p^{r\phi(p^r)-p^{r-1}}$.

The following two propositions, which are of indepedent interest, will be used to compute the discriminant of a general cyclotomic field.

Notation. If S and T are subrings of a ring R, then ST will stands for the composite ring, i.e., the smallest subring of R containing $S \cup T$. Similar notation will be used for the composite of two subfields of a field.

Proposition 18. Let K and L be algebraic number fields of degree m and n respectively. Let $d = (d_K, d_L)$. If $[KL : \mathbb{Q}] = mn$, then $\mathcal{O}_{KL} \subseteq \frac{1}{d}(\mathcal{O}_K \mathcal{O}_L)$. In particular when $d = 1$, then $\mathcal{O}_K \mathcal{O}_L = \mathcal{O}_{KL}$.

Proposition 19. Let K and L be algebraic number fields of degree m and n respectively such that $[KL : \mathbb{Q}] = mn$. If $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ and $\{\beta_1, \beta_2, \ldots, \beta_n\}$ are bases of $K/\mathbb{Q}$ and $L/\mathbb{Q}$ respectively, then the discriminant of the basis $\{\alpha_i \beta_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ of $KL/\mathbb{Q}$ is given by

$$D_{KL/\mathbb{Q}}(\alpha_1\beta_1, \ldots, \alpha_m\beta_n) = \Big(D_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_m)\Big)^n \Big(D_{L/\mathbb{Q}}(\beta_1, \ldots, \beta_n)\Big)^m.$$

We quickly deduce the following corollary from the above two propositions.

Corollary 20. Let $\mathbb{Q}(\sqrt{u}), \mathbb{Q}(\sqrt{v})$ be two distinct quadratic fields having discriminants u, v respectively which are coprime. Then the discriminant of the composite field $\mathbb{Q}(\sqrt{u}, \sqrt{v})$ is u^2v^2.

We now state the discriminant and an integral basis of $\mathbb{Q}(\zeta_m)$ for general m, where ζ_m stands for a primitive mth root of unity.

Theorem 21. Let m be any integer ≥ 3 such that $m \not\equiv 2 \pmod 4$. Let ζ a primitive mth root of unity. Then $\{1, \zeta, \ldots, \zeta^{\phi(m)-1}\}$ is an integral basis of $K = \mathbb{Q}(\zeta)$ and

$$d_K = \frac{(-1)^{\frac{\phi(m)}{2}} m^{\phi(m)}}{\prod\limits_{p|m} p^{\phi(m)/(p-1)}},$$

where p runs over all primes dividing m.

Corollary 22. Let ζ be a primitive mth root of unity, $m \geq 3$. Then the ring of algebraic integers of $\mathbb{Q}(\zeta + \zeta^{-1})$ is $\mathbb{Z}[\zeta + \zeta^{-1}]$.

Exercises

- Find the discriminant and an integral basis of the field $K = \mathbb{Q}(\theta)$, where $\theta^3 + \theta + 1 = 0$.
- Find the discriminant and an integral basis of the field $K = \mathbb{Q}(\theta)$, where $\theta^3 - \theta + 1 = 0$.
- If the minimal polynomial of a complex number α over $\mathbb{Q}$ is $X^n + aX + b$, show that for $K = \mathbb{Q}(\alpha)$,
  $D_{K/\mathbb{Q}}(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}}(n^n b^{n-1} + a^n(1-n)^{n-1})$.
- Find the discriminant and integral basis of $\mathbb{Q}(\sqrt[3]{5}), \mathbb{Q}(\sqrt[3]{6})$.
- Find an integral basis of each of the three cubic fields.
  (a) $K_1 = \mathbb{Q}(\theta)$, $\theta^3 - 18\theta - 6 = 0$.
  (b) $K_2 = \mathbb{Q}(\theta)$, $\theta^3 - 36\theta - 78 = 0$.
  (c) $K_3 = \mathbb{Q}(\theta)$, $\theta^3 - 54\theta - 150 = 0$.
  Verify all the three fields have the same discriminant.

Exercises Contd..

- Find an integral basis and the discriminant of $\mathbb{Q}(\theta)$, where $\theta^5 - 25\theta - 5 = 0$.
- Find the discriminant and integral basis of $\mathbb{Q}(\sqrt[3]{75}), \mathbb{Q}(\sqrt[3]{99})$ and $\mathbb{Q}(\sqrt[3]{100})$.
- Find the discriminant and integral basis of $\mathbb{Q}(\sqrt[3]{10}), \mathbb{Q}(\sqrt[3]{28})$.