Explicit Methods in Algebraic Number Theory

Amalia Pizarro Madariaga
Instituto de Matemáticas
Universidad de Valparaíso, Chile
amalia.pizarro@uv.cl

1 Lecture 1

1.1 Number fields and ring of integers

Algebraic number theory studies the arithmetic aspects of the number fields. Such fields are involved in the solution of many rational problems, as the following diophantine problems.

Pell Equation: Find integer numbers x, y such that $x^2 - dy^2 - 1 = 0$, with $d > 1$ squarefree.
Note that $x^2 - dy^2 = (x - \sqrt{d}y)(x + \sqrt{d}y)$, if we consider the ring $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$. So, to solve this diophantine equation is equivalent to look into $\mathbb{Z}[\sqrt{d}]^*$.

Pythagorean triples: Find integers numbers without common factors x, y, z such that $x^2 + y^2 = z^2$.
$x^2 + y^2 = (x + yi)(x - iy)$ in $\mathbb{Z}[i]$. We have $\mathbb{Z}[i]$ in a unique factorization domain (exercise), so each element in $\mathbb{Z}[i]$ can be written in a unique way (unless order an multiplication by units) as the product of irreducible elements. By using this fact, it is possible to prove that $x + iy = u\alpha^2$, with $\alpha, u \in \mathbb{Z}[i]$ and u a unit (i.e $u \in \{\pm 1\}$. (exercise).
If $\alpha = m + ni$, with $m, n \in \mathbb{Z}$, then $x + iy = \pm(m + ni)^2 = \pm(m^2 + 2mni - n^2)$, i.e., $x = \pm(m^2 - n^2), y = \pm 2mn$. Therefore, $z^2 = (m^2 + n^2)^2$ and $z = \pm(m^2 + n^2)$. m and n must be relatively primes and not both odd.

Is it possible to apply this idea to solve the general case $x^n + y^n = z^n, n > 2$?
Fermat [1] conjectured that there is no integer solution non zero for $n > 2$. In order to study this problem, it is enough to consider the case $n = p$, with p an odd prime.
Suppose that for some odd prime p there is a solution $x, y, z \in \mathbb{Z} - \{0\}$ with no common factors. Let us consider the following cases:

(a) p does not divide any x, y, z.

[1] Now it is known as the Last Fermat Theorem and was proved by Andrew Wiles in 94

(b) p divides exactly one of them.

We will only see the case (a).

- $p = 3$.
  If x, y, z are not multiples of 3, then $x^3, y^3, z^3 \equiv \pm 1 \pmod 9$ and $x^3 + y^3 \not\equiv z^3 \pmod 9$, so it cannot have non trivial solution.
- $p > 3$.

$$x^p + y^p = (x + y)(x + \zeta_p y)(x + \zeta_p^2 y) \cdots (x + \zeta_p^{p-1} y) = z^p,$$

  where $\zeta_p = e^{2\pi i/p}$ in $\mathbb{Z}[\zeta_p] = \{a_{p-2}\zeta_p^{p-2} + \ldots a_1\zeta_p + a_0\}$ (exercise).

Kummer asserted that this ring was a unique factorization domain and from here he obtained a proof of the Fermat Theorem. However, only is valid if $p < 23$. Idea: If we assume that $\mathbb{Z}[\zeta_p]$ is a UFD, it is possible to prove that $x + \zeta_p y = u\alpha^p$, for some $\alpha \in \mathbb{Z}[\zeta_p]$ and $u \in \mathbb{Z}[\zeta_p]^*$ and also that if x, y are not divisible by p, then $x \equiv y \pmod p$. Putting $x^p + (-z)^p = (-y)^p$, we obtain that $x \equiv -z \pmod p$. This implies

$$2x^p x \equiv x^p + y^p = z^p x \equiv (-x)^p \pmod p,$$

so $p \mid 3x^p$, but $p \neq 3$ and p does not divide x, which is a contradiction and then there is no solutions of the case (a).

More general case: Dedekind discovered that although the elements of $\mathbb{Z}[\zeta_p]$ may not factor in a unique way in irreducibles, the ideals of this ring always factors in product of prime ideals. From here, it is possible to prove that the principal ideal generated by $x + \zeta_p y$ may be written as $(x + \zeta_p y) = I^p$, for some I ideal.
There are certain primes p (regular primes) for which I may be a principal ideal $I = (\alpha)$, then

$$(x + \zeta_p y) = I^p = (\alpha)^p = (\alpha^p),$$

and again $(x + \zeta_p y) = u\alpha^p$, for u a unit. Then $x \equiv y \pmod p$, which is a contradiction.

1.2 Number Fields

Definition 1. *A field K is an **algebraic number field** if is a finite extension of $\mathbb{Q}$. Their elements will be called **algebraic numbers**, that is, they are roots of nonzero polynomials with rational coefficients. The monic polynomial $P_\alpha(x)$ of lowest degree of which $\alpha \in K$ is a root is called de **minimal polynomial** of α.*

If α is root of $g(x) \in \mathbb{Q}[x]$, then $P_\alpha(x) | g(x)$.

Example 1. ***Quadratic fields.***
Quadratic fields are extension K of $\mathbb{Q}$ of degree 2 $\mathbb{Q}(\sqrt{d})$, where d is squarefree. If $d < 0$ we say that $\mathbb{Q}(\sqrt{d})$ is an imaginary quadratic field and of $d > 0$ a real quadratic field.

Example 2. ***Cyclotomic fields.***

Let $n \geq 1$ and let ζ_n be a primitive n-th root of unity in $\mathbb{C}$. The n-th cyclotomic field is the field $\mathbb{Q}(\zeta_n)$. The degree of this field over $\mathbb{Q}$ is $\phi(n)$, where ϕ is the Euler's phi function.
The minimal polynomial of ζ_n over $\mathbb{Q}$ is called the cyclotomic polynomial $\Phi_n(x)$ and it verifies the following:

(i) Let U_n be the group of n-th roots of unity in $\mathbb{C}$ and let $U_n' = \{\zeta_n^a : 0 \leq a < n,\ gcd(a,n) = 1\}$. Then

$$\Phi_n(x) = \prod_{\zeta \in U'} (x - \zeta).$$

(ii) $\Phi_n(x)$ is a monic polynomial with integer coefficients and irreducible over $\mathbb{Q}$. Its degree is $\phi(n)$.

(ii) $\prod_{d|n} \Phi_d(x) = x^n - 1$.

1.3 Algebraic Integers

Definition 2. *An element α in a number field will be called **algebraic integer** if there exists a monic polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$.*

Example 3. *$\sqrt[3]{2}, \sqrt{2}+2$ are algebraic integers. $\frac{\sqrt{2}}{3}$ is algebraic, but it is no an algebraic integer.*

Theorem 1.1. *Let α be an algebraic integer. Then, the minimal polynomial of α has integer coefficients.*

Proof. Let $P_\alpha(x) \in \mathbb{Q}[x]$ the minimal polynomial of α and $g(x) \in \mathbb{Z}[x]$ with $g(\alpha) = 0$. Then $g = P_\alpha h$, for some $h(x) \in \mathbb{Q}[x]$. If $P_\alpha(x) \notin \mathbb{Z}[x]$, then there is a prime p dividing the denominator of some coefficient of P_α. Let p^i the biggest power of p with this property and p^j the biggest power dividing the coefficients of h. Then:

$$p^{i+j} g = (p^i P_\alpha)(p^j h) \equiv 0 \pmod{p}.$$

As $\mathbb{Z}_p[x]$ is an integral domain, $p^i P_\alpha$ or $p^j h$ are zero mod p, which is a contradiction. □

From now, we will denote by $\mathcal{O}_K$ the set of algebraic integers in the number field K.

Corollary 1. $\mathcal{O}_\mathbb{Q} = \mathbb{Z}$.

1.4 Characterization of Algebraic Integers

Theorem 1.2. *The following assertions are equivalents:*

(i) α *is algebraic integer.*

(ii) $\mathbb{Z}[\alpha] = \{f(\alpha) : f(x) \in \mathbb{Z}[x]\}$ *is a finitely generated* $\mathbb{Z}$*-module.*

(iii) There exists a finitely generated $\mathbb{Z}$*-module* M *such that* $\alpha M \subseteq M$ *and* $\gamma M \neq \{0\}$ *for all* $\gamma \in \mathbb{Z}[\alpha] - \{0\}$.

Proof. $i) \Rightarrow ii)$ Let $f(x) = x^n + a_1 x + \ldots a_0 \in \mathbb{Z}[x]$ and $f(\alpha) = 0$. Let us consider the following $\mathbb{Z}$-module: $M = \mathbb{Z} + \mathbb{Z}\alpha + \ldots \mathbb{Z}\alpha^{n-1}$. It is clear that $M \subseteq \mathbb{Z}[\alpha]$. By induction: suppose that $\alpha^k \in M$, then:

$$\begin{aligned} \alpha^{n+k} &= \alpha^k \alpha^n \\ &= \alpha^k[-(a_{n-1}\alpha^{n-1} + \ldots + a_0] \\ &= (-\alpha^k a_{n-1})\alpha^{n-1} + \ldots + (-\alpha^k a_0). \end{aligned}$$

Because $-\alpha^k a_i \in \mathbb{Z}[\alpha]$ for $i = 0, 1, \ldots, n-1$, we have that $\alpha^{n+k} \in M$, therefore $M = \mathbb{Z}[\alpha]$.
$ii) \Rightarrow iii)$. We take $M = \mathbb{Z}[\alpha]$. As $\alpha \in M$, then $\alpha M \subseteq M$ and $\gamma = \gamma \cdot 1 \in \gamma M$.
$iii) \Rightarrow i)$. Let $\{x_1, x_2 \ldots x_r\}$ be a generators of M. By hypothesis $\alpha x_i \in M$, then there exists a set of integers numbers c_{ij} such that $\alpha x_i = \sum_{j=1}^{r} c_{ij} x_j$, for all $i = 1, \ldots, r$. Let $C = (c_{ij})_{ij}$, then

$$C \cdot \begin{pmatrix} x_1 \\ . \\ . \\ . \\ x_r \end{pmatrix} = \alpha \cdot \begin{pmatrix} x_1 \\ . \\ . \\ . \\ x_r \end{pmatrix} \Leftrightarrow (C - \alpha I_d) \begin{pmatrix} x_1 \\ . \\ . \\ . \\ x_r \end{pmatrix} = 0.$$

There is at least one x_i non zero, so $det(C - \alpha I_d) = 0$ and then $det(C - xI_d) \in \mathbb{Z}[x]$. □

Theorem 1.3. *Let* K *be a number field. Then* $\mathcal{O}_K$ *is a ring.*

Proof. If α, β are algebraic integers, then $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are a finitely generated as $\mathbb{Z}$-modules. From here, we have that $M = \mathbb{Z}[\alpha, \beta]$ also is a finitely generated $\mathbb{Z}$-module. Moreover, $(\alpha \pm \beta)M \subseteq M$ and $(\alpha\beta)M \subseteq M$, and then $\alpha \pm \beta$ and $\alpha\beta$ belong to the set of algebraic integers. □

1.5 Discriminant of Number Fields

Let K be a number field with $[K : \mathbb{Q}] = n$ and let $\sigma_1, \ldots, \sigma_n$ be the complex embeddings of K. For $\alpha_1, \ldots, \alpha_n \in K$ we define the **discriminant of** $\alpha_1, \ldots, \alpha_n$ by

$$D_K(\alpha_1, \ldots, \alpha_n) = \det(\sigma_i(\alpha_j))^2. \tag{1.1}$$

Theorem 1.4.

$$D_K(\alpha_1, \ldots, \alpha_n) = \det(T_K(\alpha_i \alpha_j).$$

Lemma 1. *If* $\gamma_i = \sum_{j=1}^n c_{ij}\alpha_j$, *with* $c_{ij} \in \mathbb{Q}$, *then*

$$D_K(\gamma_1, \ldots, \gamma_n) = \det(c_{ij})^2 D_K(\alpha_1, \ldots, \alpha_n).$$

Proof. $\gamma_k\gamma_m = \sum_{i,j=1}^n c_{ki}c_{mj}\alpha_i\alpha_j$. □

Theorem 1.5. $D_K(\alpha_1, \ldots, \alpha_n) \neq 0$ *if and only if the set* $\{\alpha_1, \ldots, \alpha_n\}$ *is linearly independent over* $\mathbb{Q}$.

Proof. If $\{\alpha_1, \ldots, \alpha_n\}$ is linearly dependent over $\mathbb{Q}$ then the columns if the matrix $(\sigma_i(\alpha_j))$ are linearly dependent, so $D_K(\alpha_1, \ldots, \alpha_n) = 0$. Reciprocally, if $D_K(\alpha_1, \ldots, \alpha_n) = 0$ then the columns of $(T_K(\alpha_i\alpha_j))_{ij}$ are l.d. Let us suppose that $\alpha_1, \ldots, \alpha_n$ is l.i.. We fix rational numbers (not all zero) such that $a_1R_1 + \ldots + a_nR_n = \overrightarrow{0}$, where R_l are the columns of $(T_K(\alpha_i\alpha_j))_{ij}$ and let $\alpha = a_1\alpha_1 + \ldots + a_n\alpha_n \neq 0$. Looking the j-th coordinate of each row, we see that $T_k(\alpha\alpha_j) = 0$ for all j. Note that $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is in fact, a basis for K over $\mathbb{Q}$ and then $\{\alpha\alpha_1, \alpha\alpha_2, \ldots, \alpha\alpha_n\}$ is a also a basis, then $T_K(\beta) = 0$ for all $\beta \in K$, which is a contradiction.

□

Theorem 1.6. *Let* $K = \mathbb{Q}(\alpha)$, *and* $\alpha_1, \alpha_2, \ldots, \alpha_n$ *the conjugated of* α *over* $\mathbb{Q}$. *Then*

$$D_K(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) = \prod_{1 \leq r < s \leq n} (\alpha_r - \alpha_s)^2 = \pm N_K(f'(\alpha)),$$

where f *is the irreducible monic polynomial of* α *over* $\mathbb{Q}$ *and the signe is* $+$ *if and only if* $n \equiv 0$ *or* 1 *(mod 4).*

Proof. It is not difficult to prove that

$$D_K(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) = \det \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{pmatrix}^2 = \prod_{1 \leq r < s \leq n} (\alpha_r - \alpha_s)^2.$$

By using that $N_K(f'(\alpha)) = \prod_{i=1}^n \sigma_i(f'(\alpha))$, we prove the second equality. □

1.6 Integral basis

By using discriminant, we can prove that the ring of integers $\mathcal{O}_K$ of a number field K with $[K : \mathbb{Q}] = n$ is a free abelian group of rank n, that is, is the direct product of n subgroups, each of which is isomorphic to $\mathbb{Z}$. It is known that if A and B are free abelian groups of rank n, and $A \subseteq B \subseteq C$, then so is C. If $\alpha \in K$, then there exists an integer $m \in \mathbb{Z}$ such that $m\alpha$ is an algebraic integer. Following this, we can find a basis of K over $\mathbb{Q}$, say $\{\alpha_1, \ldots, \alpha_n\}$, contained in $\mathcal{O}_K$. So, the free abelian group of rank n $A = \mathbb{Z}\alpha_1 + \ldots + \mathbb{Z}\alpha_n$ is contained in $\mathcal{O}_K$.

Theorem 1.7. *Let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis for K over $\mathbb{Q}$ consisting entirely of algebraic integers, and set $D = D_K(\alpha_1, \ldots, \alpha_n)$. Then, every $\alpha \in \mathcal{O}_K$ can be expressed in the form*

$$\frac{1}{D}(m_1\alpha_1 + \ldots + m_n\alpha_n)$$

with $m_j \in \mathbb{Z}$ and m_j^2 are divisible by D.

It follows that $\mathcal{O}_K$ is containdes in the free abelian group $B = \mathbb{Z}\frac{\alpha_1}{D} + \ldots + \frac{\alpha_n}{D}$, so we have the following corollary

Corollary 2. *$\mathcal{O}_K$ is a free abelian group of rank n.*

It means that there exits $\beta_1, \ldots, \beta_n$ in $\mathcal{O}_K$ such that every $\alpha \in \mathcal{O}_K$ has unique representation

$$m_1\beta_1 + \ldots + m_n\beta_n,$$

where $m_i \in \mathbb{Z}$. The set $\{\beta_1, \ldots, \beta_n\}$ is called **integral basis** for $\mathcal{O}_K$.

Although ring of integers has many integral basis, their discriminants are the same.

Theorem 1.8. *Let $\{\beta_1, \ldots, \beta_n\}$ and $\{\alpha_1, \ldots, \alpha_n\}$ be two integral bases for $\mathcal{O}_K$. Then*

$$D_K(\beta_1, \ldots, \beta_n) = D_K(\alpha_1, \ldots, \alpha_n).$$

Proof. It is enough to apply lemma(1). □

Definition 3. *Let K be a number field of degree n over $\mathbb{Q}$. We define the disciminant of K by*

$$D_K := D_K(\alpha_1, \ldots, \alpha_n),$$

where $\alpha_1, \ldots, \alpha_n$ is a integral basis of $\mathcal{O}_K$.

1.7 Some explicit computations I

1.8 Ring of Integers of Quadratic Number Fields

Let us consider a quadratic number field $K = \mathbb{Q}(\sqrt{d})$ with d square free. Let $\alpha = a+b\sqrt{d} \in \mathcal{O}_K$, then its conjugate $\alpha' = a-b\sqrt{d}$ is also in $\mathcal{O}_K$. We have that $\alpha+\alpha' \in \mathcal{O}_K$, but $2a \in \mathbb{Q}$, so $2a$ is in fact an integer so $a = \dfrac{a'}{2}, \in \mathbb{Z}$. Looking the equation of α over $\mathbb{Q}$

$$0 = (x-\alpha)(x-\alpha') = x^2 - (\alpha+\alpha')x + \alpha\alpha',$$

it follows that $\alpha\alpha' \in \mathbb{Z}$ (because $\alpha\alpha' \in \mathcal{O}_K \cap \mathbb{Q}$), that is,

$$\alpha\alpha' = a^2 - b^2d = \left(\frac{a'}{2}\right)^2 - b^2d \in \mathbb{Z}.$$

Then, $(a')^2 - 4b^2d \in 4\mathbb{Z}$. Because $a' \in \mathbb{Z}$, $4b^2d \in \mathbb{Z}$ and so $4b^2 \in \mathbb{Z}$ due to d is square free. Now it follows that $2b \in \mathbb{Z}$ and so $b = \dfrac{b'}{2}$, with $b' \in \mathbb{Z}$. Now, we can see that α has the following representation:

$$\alpha = \frac{a'}{2} + \frac{b'\sqrt{d}}{2}.$$

Also, because $\alpha\alpha' \in \mathbb{Z}$,

$$\left(\frac{a'}{2}\right)^2 - \left(\frac{b'}{2}\right)^2 d \in \mathbb{Z}.$$

Note that $d \not\equiv 0 \pmod 4$, so $d \equiv 1, 2, 3 \pmod 4$ and

$$(a')^2 \equiv (b')^2 d \pmod 4.$$

Therefore, a' and b' have the same parity. Let us see the two cases:

- If a' and b' are even, then $\alpha = \widetilde{a} + \widetilde{b}\sqrt{d}$, with $\widetilde{a}$ and $\widetilde{b} \in \mathbb{Z}$.
- If a' and b' are odd, then $(a')^2 \equiv (b')^2 \equiv 1 \pmod 4$, so $d \equiv 1 \pmod 4$.

Finally, we have the following proposition:

Proposition 1. *If $\mathbb{Q}(\sqrt{d})$ with d squarefree, then*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}], & \text{if } d \equiv 2, 3 \text{ (mod 4)} \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right], & \text{if } d \equiv 1 \text{ (mod 4)} \end{cases}$$

From the proposition it is clear that an integral basis, depending on d, is the following:

$$\begin{cases} \{1, \sqrt{d}\}, & \text{if } d \equiv 2, 3 \pmod 4 \\ \{1, \frac{1+\sqrt{d}}{2}\}, & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

1.9 Discriminant of Quadratic Number Fields

The complex embeddings of $\mathbb{Q}(\sqrt{d})$ are $\sigma_(a+b\sqrt{d}) = a+b\sqrt{d}$ and $\tau(a+b\sqrt{d}) = a-b\sqrt{d}$. So, $T_k(a + b\sqrt{d}) = 2a$. Let $\{1, \alpha\}$ be a integral basis of $\mathcal{O}_K$. Then,

$$D_K(1, \alpha) = \det \begin{pmatrix} T_k(1) & T_K(\alpha) \\ T_K(\alpha) & T_k(\alpha^2) \end{pmatrix} = \det \begin{pmatrix} 2 & 2a \\ 2a & 2(a^2 + b^2 d) \end{pmatrix} = 4b^2 d.$$

Finally, we have:

$$D_K = \begin{cases} 4d, & \text{if } d \equiv 2, 3 \pmod 4 \\ d, & d \equiv 1 \pmod 4 \end{cases}$$

Moreover, this discriminant satisfies the following:

$$D_K \equiv 0, 1 \pmod 4, \quad \text{Stickelgerger's criterion}$$

1.10 Ring of Integers and Discriminant of Cyclotomic Number Fields

Proposition 2. *Let $n = p^l$ with p a prime number and ζ a primitive n-th root of unity in $\mathbb{C}$. Then $\{1, \zeta, \ldots, \zeta^{\phi(n)-1}\}$ is a $\mathbb{Q}$- basis of $K = \mathbb{Q}(\zeta)$ and*

$$D_K(1, \zeta, \ldots, \zeta^{\phi(n)-1}) = \pm r^s, \quad \text{where } s = p^{l-1}(lp - l - 1).$$

Proof. The main steps are the following:

- $\Phi_n(x) = \dfrac{x^{p^l} - 1}{x^{p^{l-1}}} = x^{p^{l-1}(l-1)} + \ldots + x^{2p^{l-1}} + 1.$
- From (1.6), $D_K(1, \zeta, \ldots, \zeta^{\phi(n)-1}) = \pm N_K(\phi'(\zeta))$.
- $\Phi_n(x) = \dfrac{p^l \zeta^{p^{l-1}}}{\zeta^{n/p}}.$
- $N_K(\phi'(\zeta)) = \dfrac{N_K(p^l \zeta^{p^{l-1}})}{N_K(\zeta^{n/p})} = \dfrac{p^{l\phi(n)} N_K(\zeta^{p^{l-1}})}{N_K(\zeta^{n/p})}.$

□

Proposition 3. *Let $n = p$, with p a prime number and let ζ be a n-th primitive root of unity. If $K = \mathbb{Q}(\zeta)$, then $\{1, \zeta, \zeta^2, \ldots, \zeta^{p-2}\}$ is and integral basis for $\mathcal{O}_K$.*

Proof. The main steps are the following:

- $\Phi_p(x) = \dfrac{x^p - 1}{x - 1} = x^p + \ldots + x + 1.$
- From (1.6), $D_K(1, \zeta, \ldots, \zeta^{p-2}) = \pm \displaystyle\prod_{i=1}^{p-1} (\phi'(\zeta^i))$.
- $\Phi_(\zeta^i) = \dfrac{p\zeta^{-i}}{\zeta^i - 1}.$
- $D_K(1, \zeta, \ldots, \zeta^{p-2}) = \pm \displaystyle\prod_{i=1}^{p-1} \frac{p\zeta^{-i}}{\zeta^i - 1} = \pm \frac{p^{p-1}}{\Phi_p(1)} = \pm p^{p-2} \neq 0.$
- ζ^i are algebraic integers, so if $\{\alpha_1, \ldots, \alpha_{p-2}\}$ is an integral basis, then from (1),

  $$D_K(1, \zeta, \ldots, \zeta^{p-2}) = c^2 D_K(\alpha_1, \ldots, \alpha_{p-2}),$$

  where c is the determinant of the matrix $C = (c_{ij})$ where $\zeta^i = \displaystyle\sum_{j=1}^{p-2} c_{ij}\alpha_j$. it verifies that $c = 1$. Let us considere the following result:

Let $a_1, \ldots, a_n \in \mathcal{O}_K$ linearly independent over $\mathbb{Q}$. Let $N = \mathbb{Z}a_1 + \ldots + \mathbb{Z}a_n$ and $m = [\mathcal{O}_K : N]$. Prove that $D_K(a_1, \ldots, a_n) = m^2 D_K$.

If we fix $N = \mathbb{Z} \cdot 1 + \mathbb{Z}\zeta^2 \ldots + \mathbb{Z}\zeta^{p-1}$, then $[\mathcal{O}_K : N] = 1$, so $1, \zeta, \ldots, \zeta^{p-2}$ is an integral basis.

□

Theorem 1.9. *Let ζ be a n-th primitive root of unity. If $K = \mathbb{Q}(\zeta)$, then $\{1, \zeta, \zeta^2, \ldots, \zeta^{\phi(n)}\}$ is and integral basis for $\mathcal{O}_K$, i.e. $\mathcal{O}_K = \mathbb{Z}[\zeta]$. In particular, the discriminant of K is*

$$D_K = \frac{(-1)^{\phi(n)/2} n^{\phi(n)}}{\prod_{p|n} p^{\phi(n)/p-1}}.$$

1.11 Exercises

1. (i) Let K be a number field with $[K : \mathbb{Q}] = n$ and $\beta \in \mathcal{O}_K$. Prove that $\beta \in \mathcal{O}_K^*$ if and only if $N_K(\beta) = 1$.
   (ii) Prove that $\mathbb{Z}[\sqrt{2}]^* = \{\pm(1+\sqrt{2})^k : k \in \mathbb{Z}\}$ and $\mathbb{Z}[\sqrt{2}]^* = \{\pm 1\}$

2. If K is a number field, prove that its discriminant D_K is an integer.

3. Let $a_1, \ldots, a_n \in \mathcal{O}_K$ linearly independent over $\mathbb{Q}$. Let $N = \mathbb{Z}a_1 + \ldots + \mathbb{Z}a_n$ and $m = [\mathcal{O}_K : N]$. Prove that $D_K(a_1, \ldots, a_n) = m^2 D_K$. *(Hint: Use the following result: Let $M = \mathbb{Z}\alpha_1 + \ldots + \mathbb{Z}\alpha_n$ and N be a submodule. Then there exists $\beta_1, \ldots, \beta_m \in N$ with $m \geq n$ such that $N = \mathbb{Z}\beta_1 + \ldots + \beta_m\mathbb{Z}$ and $\beta_i = \sum_{j \geq i} p_{ij}\alpha_j$ with $1 \leq i \leq m$ and $p_{ij} \in \mathbb{Z}$)*

4. Prove the Stickelgerger's criterion.

5. Let $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ the minimal polynomial of θ. Let $K = \mathbb{Q}(\theta)$. If for each prime p such that $p^2 | D_K(\theta)$ we have $f(x)$ Eisensteinian (that is, $f(x)$ satisfies the Eisenstein's criterion for irreducibility for p) with respect to p. show that $\mathcal{O}_K = \mathbb{Z}[\theta]$. *(Hint: Use the problem 3)*

6. If the minimal polynomial of α is $f(x) = x^n + ax + b$, show that for $K = \mathbb{Q}(\alpha)$,

$$D_K(\alpha) = (-1)^{\binom{n}{2}}(n^n b^{n-1} + a^n(1-n)^{n-1}).$$

7. Determine an integral basis for $K = \mathbb{Q}(\theta)$, where $\theta^3 + 2\theta + 1 = 0$.