INTRODUCTION TO ALGEBRAIC NUMBER THEORY

Emanuele Viterbo

Dipartimento di Elettronica
Politecnico di Torino

Numbers

- $\mathbf{Z}$ ring of rational integers $(+, -, *)$
- $\mathbf{Q}$ field of rational numbers $(+, -, *, /)$
- K a field containing $\mathbf{Q}$ ($\mathbf{Q} \subset K \subset \mathbf{C}$)

Definition 1

– Let α be an element of K, we say that α is an **algebraic number** if it is a root of a monic polynomial with coefficients in $\mathbf{Q}$. Such polynomial with lowest degree is called the **minimal polynomial** of α and denoted $\mu_\alpha(x)$. If all the elements of K are algebraic we say that K is an **algebraic extension** of $\mathbf{Q}$.

∇

Definition 2

– We say that $\alpha \in K$ is an **algebraic integer** if it is a root of a monic polynomial with coefficients in $\mathbf{Z}$. The set of algebraic integers of K is a ring called the **ring of integers** of K and is indicated with O_K.

∇

Definition 3

– We define the **degree** $[K : \mathbf{Q}]$ of an algebraic extension K of $\mathbf{Q}$ as the dimension of K when considered as a vector space over $\mathbf{Q}$. An **algebraic number field** is an algebraic extension of $\mathbf{Q}$ of finite degree.

∇

Result 1

– Let K be an algebraic number field. There exists an element $\theta \in K$, called **primitive element**, such that the $\mathbf{Q}$ vector space K is generated by the powers of θ. If K has degree n then $(1, \theta, \theta^2 \dots \theta^{n-1})$ is a **basis** of K and $deg(\mu_\theta(x)) = n$. We will write $K = \mathbf{Q}(\theta)$.

∇

Result 2

– There exists a primitive element θ which is an algebraic integer of K. In other words, the minimal polynomial $\mu_\theta(x)$ has coefficients in $\mathbf{Z}$.

∇

Integral basis

Result 3
– The ring of integers O_K of K forms a $\mathbf{Z}$-module of rank n (a linear vector space of dimension n over $\mathbf{Z}$).

$\bigtriangledown$

Definition 4
– Let $(\omega_1, \omega_2, \dots \omega_n)$ be a basis of K. We say that (ω_i) is an **integral basis** of K if $O_K = \mathbf{Z}(\omega_1, \omega_2, \dots \omega_n)$, that is, if (ω_i) is a generating set of the $\mathbf{Z}$-module O_K. So that we can write any element of O_K as $\Sigma_{i=1}^{n} a_i \omega_i$ with $a_i \in \mathbf{Z}$.

$\bigtriangledown$

Dipartimento di Elettronica
Politecnico di Torino

Embeddings

Definition 5
– Let K and K' be two number fields containing $\mathbf{Q}$, we call $\phi : K \to K'$ a **$\mathbf{Q}$-homomorphism** if for each $a \in \mathbf{Q}, \phi(a) = a$. If $K' = \mathbf{C}$, the field of complex numbers, a $\mathbf{Q}$-homomorphism $\phi : K \to \mathbf{C}$ is called an **embedding** of K into $\mathbf{C}$.

$\bigtriangledown$

Result 4
– Let θ be a primitive element of K and $\mu_\theta(x)$ its minimal polynomial with roots $(\theta_1, \theta_2, \dots \theta_n)$, $\theta = \theta_1$. There are exactly n embeddings of K into $\mathbf{C}$. Each embedding $\sigma_i : K \to \mathbf{C}$, $\sigma_i(\theta) = \theta_i$, is completely identified by a root $\theta_i \in \mathbf{C}$ of $\mu_\theta(x)$.

$\bigtriangledown$

Dipartimento di Elettronica
Politecnico di Torino

Algebraic norm

Definition 6
– The elements $\sigma_1(\alpha), \sigma_2(\alpha), \dots \sigma_n(\alpha)$ are called the **conjugates** of α and

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$$

is the **algebraic norm** of α.

$\bigtriangledown$

Result 5
– For any $\alpha \in K$, we have $N(\alpha) \in \mathbf{Q}$. If $\alpha \in O_K$ we have $N(\alpha) \in \mathbf{Z}$.

$\bigtriangledown$

Dipartimento di Elettronica
Politecnico di Torino

Absolute discriminant

Definition 7
– Let $(\omega_1, \omega_2, \dots \omega_n)$ be an integral basis of K. The **absolute discriminant** of K is defined as $d_K = \det[\sigma_j(\omega_i)]^2$.

$\bigtriangledown$

Result 6
– The absolute discriminant belongs to $\mathbf{Z}$.

$\bigtriangledown$

Dipartimento di Elettronica
Politecnico di Torino

Signature

Definition 8
– Let $(\sigma_1, \sigma_2, \ldots \sigma_n)$ be the n $\mathbf{Q}$-homomorphisms of K into $\mathbf{C}$. Let r_1 be the number of $\mathbf{Q}$-homomorphisms with image in $\mathbf{R}$, the field of real numbers, and $2r_2$ the number of $\mathbf{Q}$-homomorphisms with image in $\mathbf{C}$ so that

$$r_1 + 2r_2 = n \ .$$

The pair (r_1, r_2) is called the **signature** of K. If $r_2 = 0$ we have a **totally real** algebraic number field. If $r_1 = 0$ we have a **totally complex** algebraic number field. In all other cases we will speak about complex algebraic number field.

$\bigtriangledown$

Dipartimento di Elettronica
Politecnico di Torino

Canonical embedding

Definition 9
– Let us order the σ_i's so that $\sigma_i(\alpha) \in \mathbf{R}$ for $1 \leq i \leq r_1$ and $\sigma_{j+r_2}(\alpha)$ is the complex conjugate of $\sigma_j(\alpha)$ for $r_1 + 1 \leq j \leq r_1 + r_2$. We call **canonical embedding** $\sigma : K \to \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ the isomorphism defined by

$$\sigma(\alpha) = (\sigma_1(\alpha) \ldots \sigma_{r_1}(\alpha), \sigma_{r_1+1}(\alpha), \ldots \sigma_{r_1+r_2}(\alpha)) \in \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$$

If we identify $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ with $\mathbf{R}^n$. The canonical embedding can be rewritten as $\sigma : K \to \mathbf{R}^n$,

$$\sigma(\alpha) = (\sigma_1(\alpha), \ldots \sigma_{r_1}(\alpha), \Re\sigma_{r_1+1}(\alpha), \Im\sigma_{r_1+1}(\alpha), \ldots \Re\sigma_{r_1+r_2}(\alpha), \Im\sigma_{r_1+r_2}(\alpha))$$

where $\Re$ is the real part and $\Im$ is the imaginary part.

$\bigtriangledown$

Dipartimento di Elettronica
Politecnico di Torino

Result 7
– Let $(\omega_1, \omega_2, \ldots \omega_n)$ be an integral basis of K and let d_K be the absolute discriminant of K. The n vectors $\mathbf{v}_i = \sigma(\omega_i) \in \mathbf{R}^n$ are linearly independent, so they define a full rank lattice $\Lambda = \sigma(O_K)$ with generator matrix

$$G = \begin{pmatrix} \sigma_1(\omega_1) & \ldots & \sigma_{r_1}(\omega_1) & \Re\sigma_{r_1+1}(\omega_1) & \Im\sigma_{r_1+1}(\omega_1) & \ldots & \Re\sigma_{r_1+r_2}(\omega_1) & \Im\sigma_{r_1+r_2}(\omega_1) \\ \sigma_1(\omega_2) & \ldots & \sigma_{r_1}(\omega_2) & \Re\sigma_{r_1+1}(\omega_2) & \Im\sigma_{r_1+1}(\omega_2) & \ldots & \Re\sigma_{r_1+r_2}(\omega_2) & \Im\sigma_{r_1+r_2}(\omega_2) \\ \vdots & & & \vdots & & & & \vdots \\ \sigma_1(\omega_n) & \ldots & \sigma_{r_1}(\omega_n) & \Re\sigma_{r_1+1}(\omega_n) & \Im\sigma_{r_1+1}(\omega_n) & \ldots & \Re\sigma_{r_1+r_2}(\omega_n) & \Im\sigma_{r_1+r_2}(\omega_n) \end{pmatrix} \quad (1)$$

The vectors $\mathbf{v}_i$ are the rows of G. The volume of the fundamental paralletotope of Λ is given by

$$vol(\Lambda) = |\det(G)| = 2^{-r_2} \times \sqrt{|d_K|}$$

$\bigtriangledown$

Dipartimento di Elettronica
Politecnico di Torino

Diversity

Result 8
The lattices obtained from the generator matrix (1) exhibit a diversity $L = r_1 + r_2$.

$\bigtriangledown$

Proof. Let $\mathbf{z} \neq \mathbf{0}$ be an arbitrary point of Λ

$$\mathbf{z} = (z_1, z_2, \ldots z_n) = \sum_{i=1}^{n} \lambda_i \mathbf{v}_i$$

with $\lambda_i \in \mathbf{Z}$ and $\mathbf{v}_i = (v_{ij})$ the rows of the lattice generator matrix G.

$$\prod_{i=1}^{n} |z_i| = \prod_{j=1}^{r_1} \left|\sigma_j\left(\sum_{i=1}^{n} \lambda_i\omega_i\right)\right| \times \prod_{j=r1+1}^{r_1+r_2} \left|\Re\sigma_j\left(\sum_{i=1}^{n} \lambda_i\omega_i\right)\right| \times \prod_{j=r1+1}^{r_1+r_2} \left|\Im\sigma_j\left(\sum_{i=1}^{n} \lambda_i\omega_i\right)\right|$$

- $\sigma_j\left(\Sigma_{i=1}^{n} \lambda_i\omega_i\right) \neq 0 \Rightarrow L \geq r_1 + r_2$
- $\alpha = 1 \in O_K \Rightarrow L = r_1 + r_2$

Dipartimento di Elettronica
Politecnico di Torino

The totally real case

$$G = \begin{pmatrix} \sigma_1(\omega_1) & \sigma_2(\omega_1) & \dots & \sigma_n(\omega_1) \\ \sigma_1(\omega_2) & \sigma_2(\omega_2) & \dots & \sigma_n(\omega_2) \\ \vdots & & & \vdots \\ \sigma_1(\omega_n) & \sigma_2(\omega_n) & \dots & \sigma_n(\omega_n) \end{pmatrix}$$

The lattice Λ constructed in this case attains the maximum degree of diversity $L = n$. The n-product distance of $\mathbf{z}$ from $\mathbf{0}$ is

$$\begin{aligned} d_p^n(\mathbf{0}, \mathbf{z}) &= \prod_{j=1}^{n} |z_j| = \prod_{j=1}^{n} \left| \sum_{i=1}^{n} \lambda_i v_{ij} \right| = \prod_{j=1}^{n} \left| \sum_{i=1}^{n} \lambda_i \sigma_j(\omega_i) \right| \\ &= \prod_{j=1}^{n} \left| \sigma_j \left(\sum_{i=1}^{n} \lambda_i \omega_i \right) \right| = \left| N \left(\sum_{i=1}^{n} \lambda_i \omega_i \right) \right| = |N(\alpha)| \geq 1 \end{aligned}$$

Lattice construction $\Lambda = \sigma(O_K)$

- Find an integral basis of K, which identifies O_K.
- Find the n roots of $\mu_\theta(x)$, which identify the n embeddigs $\sigma_1, \sigma_2, \dots \sigma_n$.
- Construct the generator matrix applying the canonical embedding.

References

- P. Samuel: *Algebraic theory of numbers*, Paris: Hermann 1971.
- S. Lang: *Algebraic Number Fields*, Addison Wesley, 1971.
- H. Cohn: *Advanced number theory*, Dover Publications, New York, 1980.
- T. Ono: *An introduction to algebraic number theory*, Plenum Press, New York, 1990.
- H. Hasse: *Number Theory*, Springer Verlag, 1980.
- H. Cohen: *Computational algebraic number theory*, Springer Verlag 1993.