Updated: *May 17, 2010*

Diophantine approximation, irrationality and transcendence

Michel Waldschmidt

Course N°9, *May 17, 2010*

These are informal notes of my course given in April – June 2010 at IMPA (*Instituto Nacional de Matematica Pura e Aplicada*), Rio de Janeiro, Brazil.

This course was devoted to

- Proposition 94 of Mollin and Srinivasan on the negative Pell's equation $x^2 - Dy^2 = -1$.
- The proof of Legendre's Theorem 111 according to which an approximation p/q of an irrational number x satisfying $|x - p/q| \le 1/q^2$ is a convergent of x.
- The proof of Corollary 100 on the continued fraction expansion of the square root of a rational number.
- An introduction to number fields and the connexion between Pell's equation and Dirichlet's unit Theorem.

Dirichlet's unit Theorem

A number field is a finite algebraic extension of $\mathbf{Q}$, which means a field containing $\mathbf{Q}$ as a subfield and which is a $\mathbf{Q}$–vector space of finite dimension.

In a finite extension, any element is algebraic.

An example of a number field is $\mathbf{Q}(\alpha)$ (the smallest field containing α, or the field generated by α), when α is an algebraic number. In this case $\mathbf{Q}(\alpha) = \mathbf{Q}[\alpha]$, which means that the ring $\mathbf{Q}[\alpha]$ generated by α over $\mathbf{Q}$ is a field. According to the *Theorem of the primitive element*, any number field can be written $\mathbf{Q}(\alpha)$ for some algebraic number α.

Let $f \in \mathbf{Q}[X]$ be the (monic) irreducible polynomial of α. The degree d of f is the dimension of the $\mathbf{Q}$–vector space $\mathbf{Q}(\alpha)$, it is called the *degree of α over* $\mathbf{Q}$ and also the *degree of the extension* $k/\mathbf{Q}$, it is denoted by $[\mathbf{Q}(\alpha) : \mathbf{Q}]$.

When we factorize the polynomial f over $\mathbf{R}$, we get a certain number, say r_1, of degree 1 polynomials, and a certain number, say r_2, of degree 2 polynomials with negative discriminant. Hence $0 \leq r_1 \leq d$, $0 \leq r_2 \leq d/2$ and $r_1 + 2r_2 = d$. In $\mathbf{C}$, f has d distinct roots, r_1 of which are real, say $\alpha_1, \ldots, \alpha_{r_1}$, and $2r_2$ of which are not real and pairwise complex conjugates, say $\alpha_{r_1+1}, \ldots, \alpha_{r_1+r_2}$, $\overline{\alpha}_{r_1+1}, \ldots, \overline{\alpha}_{r_1+r_2}$. There are exactly d fields homomorphisms (also called *embeddings*) $\sigma_i : k \longrightarrow \mathbf{C}$, where, for $1 \leq i \leq d$, σ_i is uniquely determined by $\sigma_i(\alpha) = \alpha_i$. For γ in k, the elements $\sigma_i(\gamma)$ are the conjugates of γ (that means the complex roots of the irreducible polynomial of γ), n of them are distinct, where $n = [\mathbf{Q}(\gamma) : \mathbf{Q}]$ divides d, say $d = nk$, and

$$\prod_{i=1}^{d}(X - \sigma_i(\gamma))$$

is the k–th power of the irreducible polynomial of γ.

The norm $\mathrm{N}_{k/\mathbf{Q}}$ is the homomorphism between the multiplicative groups $k^\times = k \setminus \{0\} \longrightarrow \mathbf{Q}^\times$ defined by

$$\mathrm{N}_{k/\mathbf{Q}}(\gamma) = \sigma_1(\gamma) \cdots \sigma_d(\gamma).$$

The *canonical embedding* of k is $\underline{\sigma} = (\sigma_1, \ldots, \sigma_{r_1+r_2}) : k \longrightarrow \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$.

An algebraic number α is called an *algebraic integer* is it satisfies the following equivalent conditions.
(i) The irreducible (monic) polynomial of α in $\mathbf{Q}[X]$ has its coefficients in $\mathbf{Z}$.
(ii) There exists a monic polynomial with rational integer coefficients having α as a root.
(iii) The subring $\mathbf{Z}[\alpha]$ of $\mathbf{C}$ generated by α is a finitely generated $\mathbf{Z}$–module.
(iii) There exists a subring of $\mathbf{C}$ containing $\mathbf{Z}[\alpha]$ which is a finitely generated $\mathbf{Z}$–module.

For instance, the algebraic integers in $\mathbf{Q}$ are the rational integers.

The set of algebraic integers is a subring of $\mathbf{C}$. Its intersection with a number field k is the *ring of integers of* k, which we denote by $\mathbf{Z}_k$. For instance, when $k = \mathbf{Q}(\sqrt{D})$,

$$\mathbf{Z}_k = \begin{cases} \mathbf{Z}[\sqrt{D}] & \text{if } D \equiv 2 \text{ or } 3 \pmod 4, \\ \mathbf{Z}[(1+\sqrt{D})/2] & \text{if } D \equiv 1 \pmod 4. \end{cases}$$

It is easy to check that the image $\underline{\sigma}(\mathbf{Z}_k)$ of the ring of integers of k under the canonical embedding is discrete in $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$.

The group of units $\mathbf{Z}_k^\times$ of $\mathbf{Z}_k$ is also called *the group of units* of the number field k (this terminology is standard but should not yield to a confusion: recall that the units in a field k are the non–zero elements of k!). An integer in k is a unit if and only if it has norm ± 1. The torsion elements of $\mathbf{Z}_k^\times$ are the roots of unity in k, it is easy to check that they form a finite cyclic group $k_{\text{tors}}^\times$.

The *logarithmic embedding* is the map $\lambda : k^\times \longrightarrow \mathbf{R}^{r_1+r_2}$ obtained by composing the restriction of $\underline{\sigma}$ to $k^\times$ with the map

$$(z_n)_{1\le n\le r_1+r_2} \longmapsto (\log|z_n|)_{1\le n\le r_1+r_2}$$

from $(\mathbf{R}^\times)^{r_1} \times (\mathbf{C}^\times)^{r_2}$ to $\mathbf{R}^{r_1+r_2}$:

$$\lambda(\alpha) = (\log|\sigma_n(\alpha)|)_{1\le n\le r_1+r_2}.$$

The image $\lambda(\mathbf{Z}_k^\times)$ of the group of units of k is a subgroup of the additive group $\mathbf{R}^{r_1+r_2}$, it is contained in the hyperplane H of equation

$$x_1 + \cdots + x_{r_1+r_2} = 0,$$

and $\lambda(\mathbf{Z}_k^\times)$ is discrete in H. From these properties , one easily deduces that as a $\mathbf{Z}$–module, $\mathbf{Z}_k^\times$ is finitely generated of rank $\le r$, where $r = r_1 + r_2 - 1$ is the dimension of H as a $\mathbf{R}$–vector space.

Dirichlet's units Theorem states:

Theorem. *The group of units of an algebraic number field k of degree d with r_1 real embeddings and $2r_2$ conjugate complex embeddings is a finitely generated group of rank $r := r_1 + r_2 - 1$.*

In other terms, there exists a system of fundamental units $(u_1, \dots, u_r)$ in $\mathbf{Z}_k^\times$, such that any unit $u \in \mathbf{Z}_k^\times$ can be written in a unique way as $\zeta u_1^{m_1} \dots u_r^{m_r}$, where $\zeta \in k$ is a root of unity and $m_1, \dots, m_r$ are rational integers:

$$\mathbf{Z}_k^\times \simeq k_{\text{tors}}^\times \times \mathbf{Z}^r.$$

In the special case of a real quadratic field $\mathbf{Q}(\sqrt{D})$ with $D \equiv 2$ or $3 \pmod 4$, the fact that the group of units is a finitely generated group of rank 1 means that the set of solution of Pell's equation $X^2 - Dy^2 = \pm 1$ is the set of $\pm(x_m, y_m)$, $m \in \mathbf{Z}$, where x_m and y_m are defined by $x_m + y_m\sqrt{D} = (x_1 + y_1\sqrt{D})^m$, where (x_1, y_1) denotes the fundamental solution of Pell's equation.

The proof of the existence of a system of r fundamental units rests on Minkowski's geometry of numbers.

There are plenty of references on this subject. Lists of *online number theory lecture notes and teaching materials* are available on the internet. For instance

`http://www.numbertheory.org/ntw/lecture_notes.html`