INTERNATIONAL ATOMIC ENERGY AGENCY
UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION
INTERNATIONAL CENTRE FOR THEORETICAL PHYSICS
I.C.T.P., P.O. BOX 586, 34100 TRIESTE, ITALY, CABLE: CENTRATOM TRIESTE

SMR.637/13

ADVANCED WORKSHOP ON ARITHMETIC ALGEBRAIC GEOMETRY

(31 August - 11 September 1992)

Algebraic Number Theory - Lecture 1

E. Nart
Departamento de Matematica
Universidad Autonoma de Barcelona
Bellaterra
08193 Barcelona
Spain

ALGEBRAIC NUMBER THEORY

Lecture 1 (by Enric Nart)

1. Algebraic Numbers

These are complex numbers which satisfy a polynomial equation with coefficients in $\mathbf{Q}$. For example, i, $\sqrt[3]{1.78}$ and $e^{\pi i/5}$ are algebraic numbers, whereas π, e and $\sum_{n=1}^{\infty} 10^{-n!}$ are transcendental (not algebraic). Each algebraic number is the root of a unic monic irreducible (over $\mathbf{Q}$) polynomial in $\mathbf{Q}[X]$, called its *minimal equation*. Two algebraic numbers having the same minimal equation are called *conjugate*. The minimal equations of the algebraic numbers above are respectively:

$$X^2+1, \quad X^3-1.78, \quad X^4-X^3+X^2-X+1.$$

By Galois Theory we know that there are algebraic numbers which cannot be formed from any set of rational numbers by a combination of sums, products and/or successive extraction of roots. By the fundamental theorem of Algebra, the algebraic numbers, modulo conjugation, are in bijection with the set of monic irreducible polynomials in $\mathbf{Q}[X]$ and this is the most common way of exhibiting algebraic numbers in practice: as the roots of a given polynomial with rational coefficients.

The subset $\bar{\mathbf{Q}}$ of $\mathbf{C}$ of all algebraic numbers is an algebraically closed subfield of $\mathbf{C}$. It is an algebraic closure of $\mathbf{Q}$.

2. Number Fields

These are finite extensions of the field $\mathbf{Q}$ of rational numbers. In other words, a number field is a field K of characteristic zero with finite dimension as a $\mathbf{Q}$-vector space (with respect to the natural structure). The number $[K:\mathbf{Q}]=\dim_{\mathbf{Q}}K$ is called the *degree* of K. Examples of number fields are:

$$K_1=\mathbf{Q}(\sqrt{15})=\{\alpha\in\mathbb{R}/\alpha=r+s\sqrt{15},\ r,s\in\mathbf{Q}\},$$

$$K_2=\mathbf{Q}[X]/f(X), \quad f(X) \text{ irreducible},$$

$$K_3=\{A\in M_2(\mathbf{Q})/A=\begin{pmatrix} a & b \\ -b & a\end{pmatrix}\},$$

with respective degrees 2, $\deg(f(X))$ and 2.

All elements (which from now on will be called simply "numbers") in a number field, are algebraic over $\mathbf{Q}$ and satisfy a minimal equation whose degree is a divisor of the degree of the number field. Reciprocally, given a finite number of elements $\alpha_1,\cdots,\alpha_m\in L$, in a field of characteristic

zero, ~~we can associate to them the number field~~ $\mathbf{Q}(\alpha_1, \cdots, \alpha_m) \subset L$ generated by the α_i. ~~This is the minimum subfield of L containing all the α_i~~ a number field. ~~Equivalently it is the subset of L of all elements of the type:~~

~~$$f(\alpha_1, \cdots, \alpha_m)/g(\alpha_1, \cdots, \alpha_m)$$~~

~~with $f(X_1, \cdots, X_m), g(X_1, \cdots, X_m)$ polynomials with rational coefficients and $g(\alpha_1, \cdots, \alpha_m) \neq 0$.~~

It is quite common (and very inconvenient) to think in number fields as subfields of $\mathbf{C}$. By field theory, if K is a number field of degree n, there are exactly n embeddings (ring homomorphisms):

$$v_i : K \hookrightarrow \mathbf{C}.$$

Thus, every number field is isomorphic to a subfield of $\mathbf{C}$, or more precisely to a subfield of $\bar{\mathbf{Q}}$, but this subfield is not uniquely determined! It is better to think of K as an abstract object and to consider the n embeddings $v_1, \cdots, v_n$ as an (important) invariant of K. They will play a significant role in what follows. An embedding $v : K \hookrightarrow \mathbf{C}$ is called *real* if $v(K) \subset \mathbf{R}$, otherwise it is called *complex*. There is always an even number of complex embeddings since for each v we have also its conjugate $\bar{v} := \bar{} \circ v$, which is different from v if v is complex. Usually, r_1, r_2 denote the number of real embeddings and pairs of non-conjugate complex embeddings. Thus, we have the relation:

$$r_1 + 2r_2 = n.$$

For the number field K_2 above, r_1 and $2r_2$ are the respective number of real and non-real roots in $\mathbf{C}$ of $f(X)$ and the embeddings are obtained sending the class of X to each of these roots. For K_1 and K_3 we have respectively: $r_1 = 2, r_2 = 0$; $r_1 = 0, r_2 = 1$.

For any number field K we have group homomorphisms:

$$Tr_{K/\mathbf{Q}} : K \longrightarrow \mathbf{Q}, \quad N_{K/\mathbf{Q}} : K^* \longrightarrow \mathbf{Q}^*,$$

defined by:

$$Tr_{K/\mathbf{Q}}(x) = \sum_{i=1}^{n} v_i(x), \quad N_{K/\mathbf{Q}}(x) = \prod_{i=1}^{n} v_i(x).$$

3. Diophantine Equations

Consider the problem of finding all integral solutions of a system of polynomial equations:

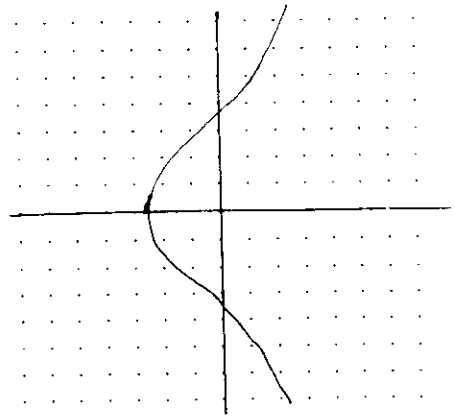
$$\left.\begin{aligned} F_1(X_1, \ldots, X_n) &= 0 \\ &\cdots\cdots \\ F_m(X_1, \ldots, X_n) &= 0 \end{aligned}\right\}$$

We speak of a *diophantine equation* to emphasize that we are interested only in the integral solutions. Usually the polynomials $F_i(X_1, \cdots, X_n)$ have also integral coefficients. This question has an obvious geometrical interpretation. For instance, equations in two variables like:

(1) $$Y^2 = X^3 + 13, \text{ or}$$

(2) $$Y^2 = X^3 - 13,$$

can be thought as a curve in the plane XY and the integral solutions are given by the intersections of the curve with the lattice of points with integral coordinates.



According to the context in which a diophantine equation appears there are three levels of *resolution* of the equation:

(A) Determine if the equation has any solution at all.
(B) If the equation has solutions, determine if it has a finite or infinite number of them.
(C) Describe the set of all solutions.

There is no general algorithm to solve (A) (even less (B) or (C)!). In general, this is a very difficult question, even for simple plane equations like (1) or (2).

As a general rule, equations can be factorized into a product of simpler ones if we are allowed to play with algebraic numbers. Thus, we could hope to have at our disposal an algebraic approach to deal with diophantine equations, provided we could develope a divisibility theory for algebraic numbers. This is the core idea behind Algebraic Number Theory. Before we proceed to see how it was exploited in full generality, let us see first the most typical illustrating example. The equation:

$$X^2 + Y^2 = Z^2, \tag{3}$$

can be expressed as:

$$(X + iY)(X - iY) = Z^2.$$

Since we are interested in the integral values of X, Y, Z satisfying (3), this last equation is a multiplicative relation in the ring $\mathbf{Z}[i]$ of the gaussian integers. Now, the divisibility theory in this ring is not too much complicated: $\mathbf{Z}[i]$ is a PID and the units are $\pm 1, \pm i$. Moreover, two integers without common divisors are coprime in $\mathbf{Z}[i]$. This arithmetic information is sufficient to solve (3). In fact, assume that X, Y, Z is a primitive ($\gcd(X, Y, Z) = 1$) solution of (3). Then, $X+iY$ and $X-iY$ are coprime in $\mathbf{Z}[i]$, since if $\pi \in \mathbf{Z}[i]$ is a prime element dividing both $X + iY$ and $X - iY$, then π would divide $2X$ and $2Y$, and this is a contradiction, since π cannot divide 2 (Z would be even and consideration of (3) modulo 4 shows that this is impossible), and π cannot divide X and Y simultaneously (else π would be a common divisor too). Thus, since $\mathbf{Z}[i]$ is a UFD, we have:

$$X + iY = u \cdot \alpha^2, \quad u, \alpha \in \mathbf{Z}[i], \ u \text{ a unit}.$$

Representatives of the units modulo squares are 1 and i.

If we put $\alpha = s + ti$, $s, t \in \mathbf{Z}$, we get the parametric description of the pythagorean triples:

$$X = s^2 - t^2, \ Y = 2st, \ Z = s^2 + t^2, \qquad \gcd(s,t) = 1.$$

The case $u = i$ just exchanges the role of X and Y.

Since any value of s, t furnishes triples X, Y, Z satisfying (3), the solution is complete.

Equations (1) and (2) admit similar factorizations:

$$(Y + \sqrt{13})(Y - \sqrt{13}) = X^3, \quad (Y + \sqrt{-13})(Y - \sqrt{-13}) = X^3,$$

where $\sqrt{-13}$ denotes any chosen of a complex square root of -13.

Unfortunately, the rings $\mathbf{Z}[\sqrt{13}]$ and $\mathbf{Z}[\sqrt{-13}]$ are no more UFD's. In fact, all elements in the following factorizations are irreducible:

$$(3 + \sqrt{13})(3 - \sqrt{13}) = -2 \cdot 2, \tag{4}$$

$$(1 + \sqrt{-13})(1 - \sqrt{-13}) = 2 \cdot 7. \tag{5}$$

4. The revolutionary idea of Kummer

was to think that unique factorization can be recovered by enlarging the system of numbers by admitting some new *ideal numbers*. Some of these ideal numbers are not "visible" and only certain products of them can be detected as ordinary numbers. For instance, in $\mathbf{Z}[\sqrt{-13}]$ one should have:

$$2 = \mathfrak{p} \cdot \mathfrak{p}', \quad 7 = \mathfrak{q} \cdot \mathfrak{q}',$$

for certain "prime" ideal numbers $\mathfrak{p}, \mathfrak{p}', \mathfrak{q}, \mathfrak{q}'$ such that:

$$1 + \sqrt{-13} = \mathfrak{p} \cdot \mathfrak{q}', \quad 1 - \sqrt{-13} = \mathfrak{p}' \cdot \mathfrak{q},$$

and we recover unique factorization in (5).

Kummer himself proposed candidates for these ideal numbers, but the theory was founded in its most consistent way by Dedekind. He defined the ideal numbers of a ring of algebraic numbers to be certain subsets of the ring satisfying certain properties. These properties define what we understand nowadays by an *ideal* of a ring.

Therefore, in order to develope a reasonable divisibility theory for algebraic numbers, "numbers" must be replaced by "ideals" and each ordinary number is just a very special type of ideal: the principal ideal generated by the number. After this, we can ask for subrings of number fields for which a fundamental theorem of arithmetic holds for ideals:

Every ideal $\mathfrak{a}$ is a product of prime ideals: $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, and the $\mathfrak{p}_i$ are uniquely determined except for the ordering.

A ring satisfying this property is called a *Dedekind ring*. The crucial question is then: what subrings of number fields are Dedekind domains? For instance, $\mathbf{Z}[\sqrt{-13}]$ is a Dedekind domain, but $\mathbf{Z}[\sqrt{13}]$ is not Dedekind.

5. Algebraic Integers

These are the numbers whose minimal equation has integral coefficients. Thus, the trace and the norm of an algebraic integer belong to $\mathbf{Z}$. The elements $\alpha_1, \cdots, \alpha_m$ of a number field K are algebraic integers if and only

if the subring $\mathbf{Z}[\alpha_1, \cdots, \alpha_m]$ of K is finitely-generated as a $\mathbf{Z}$-module. In particular, all elements in $\mathbf{Z}[\alpha_1, \cdots, \alpha_m]$ are algebraic integers too.

Thus, the set $\mathcal{O}_K$ of all algebraic integers in K is a subring of K with field of fractions the whole of K. The main theorem of Algebraic Number Theory states that these rings are Dedekind domains (see §6).

When dealing with a particular arithmetic problem involving algebraic *integers* (like equation (1), leading to the ring $\mathbf{Z}[\sqrt{13}]$), we may use divisibility theory by working in the ring of *all* algebraic integers.

For quadratic fields, $K = \mathbf{Q}(\sqrt{d})$, $d \in \mathbf{Z}$ square-free, the ring of integers is given by:

$$\mathcal{O}_K = \begin{cases} \mathbf{Z}[\sqrt{d}], & \text{if } d \not\equiv 1 (\bmod 4) \\ \{\frac{r+s\sqrt{d}}{2} / \ r, s \in \mathbf{Z},\ r \equiv s (\bmod 2)\}, & \text{if } d \equiv 1 (\bmod 4). \end{cases}$$

We see now how to overcome the [illegible] (4): $\frac{3+\sqrt{13}}{2}$ is a unit in $\mathcal{O}_K$ ($K = \mathbf{Q}(\sqrt{13})$), so that we have equality of ideals,

$$2\mathcal{O}_K = (3+\sqrt{13})\mathcal{O}_K = (3-\sqrt{13})\mathcal{O}_K.$$

For cyclotomic fields, $K = \mathbf{Q}(\zeta_m)$, $\zeta_m = e^{2\pi i/m}$, we have $\mathcal{O}_K = \mathbf{Z}[\zeta_m]$.

$\mathcal{O}_K$ is a free $\mathbf{Z}$-module of rank $[K : \mathbf{Q}]$. A $\mathbf{Z}$-basis of $\mathcal{O}_K$ is called an *integral basis* of K.

6. Dedekind Domains

are characterized by the following algebraic properties:

Theorem. A domain $\mathcal{O}$ is Dedekind if and only if it is noetherian, integrally closed and has Krull dimension one (i.e. every non-zero prime ideal is maximal).

The proof of this theorem is far from evident (see the Bibliography). It is easy to check that the ring of integers of a number field has these algebraic properties, hence, it is a Dedekind domain.

Let $\mathcal{O}$ be an arbitrary Dedekind domain and let K be its fraction field. $\mathcal{O}$ has a divisibility theory with respect to the product of ideals. Just as in the case of numbers, it is convenient to introduce the concept of inverse of an ideal.

Also, the ring of functions of an affine non-singular irreducible curve

Definition. A fractional ideal of K is a finitely-generated sub-$\mathcal{O}$-module $\mathfrak{a}$ of K, $\mathfrak{a} \neq 0$. Equivalently, it is a sub-$\mathcal{O}$-module $\mathfrak{a}$ of K, $\mathfrak{a} \neq 0$, such that $c\mathfrak{a} \subset \mathcal{O}$ for some $c \in \mathcal{O}$, $c \neq 0$.

For any element $a \in K^*$, $a\mathcal{O}$ is a fractional ideal. These fractional ideals are called *principal*. The ordinary ideals of $\mathcal{O}$ are called *integral* fractional ideals.

The set J_K of all fractional ideals of K has the structure of an abelian group with respect to the product of ideals. The unit element is $\mathcal{O}$ itself and the inverse of $\mathfrak{a}$ is:

$$\mathfrak{a}^{-1} := \{x \in K / x\mathfrak{a} \subset \mathcal{O}\}.$$

In particular, any fractional ideal of K has a unique factorization:

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}},$$

where $\mathfrak{p}$ are the non-zero integral prime ideals of $\mathcal{O}$ and $e_{\mathfrak{p}}$ are integers, vanishing for almost all $\mathfrak{p}$. In other words, J_K is the free abelian group generated by the $\mathfrak{p}$'s.

The principal fractional ideals P_K of K form a subgroup of J_K. The quotient:

$$Cl_K = J_K / P_K,$$

is the ideal *class group* of K. We have an exact sequence of abelian groups:

$$1 \to \mathcal{O}^* \to K^* \to J_K \to Cl_K \to 1,$$

where the homomorphism in the middle is $a \mapsto a\mathcal{O}$. In the process of substituting numbers by ideals, the class group Cl_K measures what we gain and the unit group $\mathcal{O}^*$ what we lose. Therefore, the description of these two groups is crucial for a good understanding of the divisibility theory of $\mathcal{O}$. For $\mathcal{O}$ the ring of integers of a number field, this will be explained in the second lecture.

7. The fundamental problems

for a number field K are:

(1) Which are the units of $\mathcal{O}_K$? How to compute them? What is the structure of $\mathcal{O}_K^*$ as an abelian group?

(2) How far is $\mathcal{O}_K$ from being an UFD? How many ideal classes has K? What is the structure of Cl_K as an abelian group?

(3) Which are the prime ideals of $\mathcal{O}_K$? Equivalently: How do the rational primes decompose in $\mathcal{O}_K$?

Before giving general answers, we finish this lecture showing how a partial [redacted] these questions for $\mathbb{Q}(\sqrt{-13})$ and $\mathbb{Q}(\sqrt{13})$ provides a complete solution of the diophantine equations (1) and (2).

Exercise. Prove the following facts:

(i) If two integers $r, s \in \mathbf{Z}$ are coprime, then the ideals $r\mathcal{O}_K$, $s\mathcal{O}_K$ are coprime in any number field K.

(ii) For $K = \mathbf{Q}(\sqrt{-13})$, we have $\mathcal{O}_K{}^* = \{\pm 1\}$. For $K = \mathbf{Q}(\sqrt{13})$, we have $\mathcal{O}_K{}^* = \{\pm\epsilon^r,\ r \in \mathbf{Z}\}$, where $\epsilon = \frac{3+\sqrt{13}}{2}$.

(iii) The class groups of $\mathbf{Q}(\sqrt{-13})$ and $\mathbf{Q}(\sqrt{13})$ are finite groups whose order is not divided by three.

Assume now that X, Y are [redacted] integers satisfying (2). Let $K = \mathbf{Q}(\sqrt{-13})$. The ideals $(Y + \sqrt{-13})\mathcal{O}_K$ and $(Y - \sqrt{-13})\mathcal{O}_K$ are coprime. In fact, a common prime divisor would divide simultaneously 2 and X (by (i) X would be even and this is impossible since -13 is not a square modulo 8), or 13 and X (by (i) 13 divides X, which is absurd). By unique factorization, since the product of these ideals is a cube, each of them must be a cube:

$$(Y + \sqrt{-13})\mathcal{O}_K = \mathfrak{a}^3.$$

Thus, the class of $\mathfrak{a}$ in Cl_K is either trivial or has order three. By (iii), it must be trivial; that is, $\mathfrak{a}$ is a principal ideal. Therefore:

$$Y + \sqrt{-13} = u \cdot \alpha^3, \quad u, \alpha \in \mathcal{O}_K, \quad u \text{ a unit}.$$

We can drop u (all units in $\mathcal{O}_K$ are cubes) and substitute α by $r + s\sqrt{-13}$. We get:

$$Y = r^3 - 39rs^2$$
$$1 = 3r^2s - 13s^3$$

From the last equation we have s=-1, $r = \pm 2$. This gives $Y = \pm 70$, $X = 17$ as the only solutions of (2).

Similarly, from a [redacted] solution X, Y of (1) we get, working in $K = \mathbf{Q}(\sqrt{13})$:

$$Y + \sqrt{13} = u \cdot \alpha^3, \quad u, \alpha \in \mathcal{O}_K, \quad u \text{ a unit}.$$

[redacted]

We can substitute α by $\frac{r+s\sqrt{13}}{2}$, with $r, s \in \mathbf{Z}$ of the same parity. There are now three [redacted]. It is trivial to check that the [redacted] case gives no solutions. The [redacted] case leads to:

$$16Y = 3r^3 + 117rs^2 + 39r^2s + 169s^3$$
$$16 = r^3 + 39rs^2 + 9r^2s + 39s^3$$

Substracting to the first equation the second multiplied by three we get:

$$4(Y - 3) = s(3r^2 + 13s^2).$$

Since the [redacted] $(3r^2 + 13s^2)$ is divisible by 8, Y must be odd, which is a contradiction. The [redacted] case is analogous, so that we have seen that the equation (1) has no solutions at all.

Bibliography

D.A. Marcus, Number Fields, Springer 1977.

J. Neukirch, Algebraische Zahlentheorie, Springer 1992.

P. Samuel, Théorie algébrique des nombres, Hermann 1967.