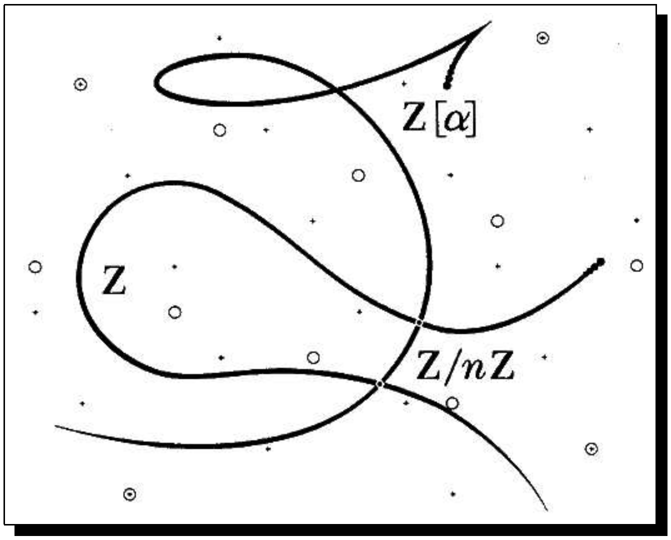
Math 129: Algebraic Number Theory
Lecture 6

William Stein

Tuesday, February 24, 2004

First we will learn how, if $p \in \mathbf{Z}$ is a prime and $\mathcal{O}_K$ is the ring of integers of a number field, to write $p\mathcal{O}_K$ as a product of primes of $\mathcal{O}_K$. Then I will sketch the main results and definitions that we will study in detail during the next 2 or 3 lectures. We will cover discriminants and norms of ideals, define the class group of $\mathcal{O}_K$ and prove that it is finite and computable, and define the group of units of $\mathcal{O}_K$, determine its structure, and prove that it is also computable.

1 Factoring Primes



A diagram from [LL93].

"The obvious mathematical breakthrough would be development of an easy way to factor large prime numbers."
–Bill Gates, *The Road Ahead*, pg. 265

Let $K = \mathbf{Q}(\alpha)$ be a number field, and let $\mathcal{O}_K$ be the ring of integers of K. To employ our geometric intuition, as the Lenstras did on the cover of [LL93], it is helpful to view $\mathcal{O}_K$ as a one-dimensional scheme

$$X = \mathrm{Spec}(\mathcal{O}_K) = \{ \text{ all prime ideals of } \mathcal{O}_K \}$$

over

$$Y = \mathrm{Spec}(\mathbf{Z}) = \{(0)\} \cup \{p\mathbf{Z} : p \in \mathbf{Z} \text{ is prime } \}.$$

There is a natural map $\pi : X \to Y$ that sends a prime ideal $\mathfrak{p} \in X$ to $\mathfrak{p} \cap \mathbf{Z} \in Y$. For much more on this point of view, see [EH00, Ch. 2].

Ideals were originally introduced by Kummer because, as we proved last Tuesday, in rings of integers of number fields ideals factor uniquely as products of primes ideals, which is something that is not true for general algebraic integers. (The failure of unique factorization for algebraic integers was used by Liouville to destroy Lamé's purported 1847 "proof" of Fermat's Last Theorem.)

If $p \in \mathbf{Z}$ is a prime number, then the ideal $p\mathcal{O}_K$ of $\mathcal{O}_K$ factors uniquely as a product $\prod \mathfrak{p}_i^{e_i}$, where the $\mathfrak{p}_i$ are maximal ideals of $\mathcal{O}_K$. We may imagine the decomposition of $p\mathcal{O}_K$ into prime ideals geometrically as the fiber $\pi^{-1}(p\mathbf{Z})$ (with multiplicities).

How can we compute $\pi^{-1}(p\mathbf{Z})$ in practice?

Example 1.1. The following Magma session shows the commands needed to compute the factorization of $p\mathcal{O}_K$ in Magma for K the number field defined by a root of $x^5 + 7x^4 + 3x^2 - x + 1$.

```
> R<x> := PolynomialRing(RationalField());
> K<a> := NumberField(x^5 + 7*x^4 + 3*x^2 - x + 1);
> OK := MaximalOrder(K);
> I := 2*OK;
> Factorization(I);
[
<Principal Prime Ideal of OK
Generator:
[2, 0, 0, 0, 0], 1>
]
> J := 5*OK;
> Factorization(J);
[
<Prime Ideal of OK
Two element generators:
[5, 0, 0, 0, 0]
[2, 1, 0, 0, 0], 1>,
<Prime Ideal of OK
Two element generators:
[5, 0, 0, 0, 0]
[3, 1, 0, 0, 0], 2>,
<Prime Ideal of OK
Two element generators:
[5, 0, 0, 0, 0]
[2, 4, 1, 0, 0], 1>
]
> [K!OK.i : i in [1..5]];
[ 1, a, a^2, a^3, a^4 ]
```

Thus $2\mathcal{O}_K$ is already a prime ideal, and

$$5\mathcal{O}_K = (5, 2+a)\cdot(5, 3+a)^2\cdot(5, 2+4a+a^2).$$

Notice that in this example $\mathcal{O}_K = \mathbf{Z}[a]$. (Warning: There are examples of $\mathcal{O}_K$ such that $\mathcal{O}_K \neq \mathbf{Z}[a]$ for any $a \in \mathcal{O}_K$, as Example 1.6 below illustrates.) When $\mathcal{O}_K = \mathbf{Z}[a]$ it is very easy to factor $p\mathcal{O}_K$, as we will see below. The following factorization gives a hint as to why:

$$x^5 + 7x^4 + 3x^2 - x + 1 \equiv (x+2)\cdot(x+3)^2\cdot(x^2+4x+2) \pmod{5}.$$

The exponent 2 of $(5, 3+a)^2$ in the factorization of $5\mathcal{O}_K$ above suggests "ramification", in the sense that the cover $X \to Y$ has less points (counting their "size", i.e., their residue class degree) in its fiber over 5 than it has generically. Here's a suggestive picture:

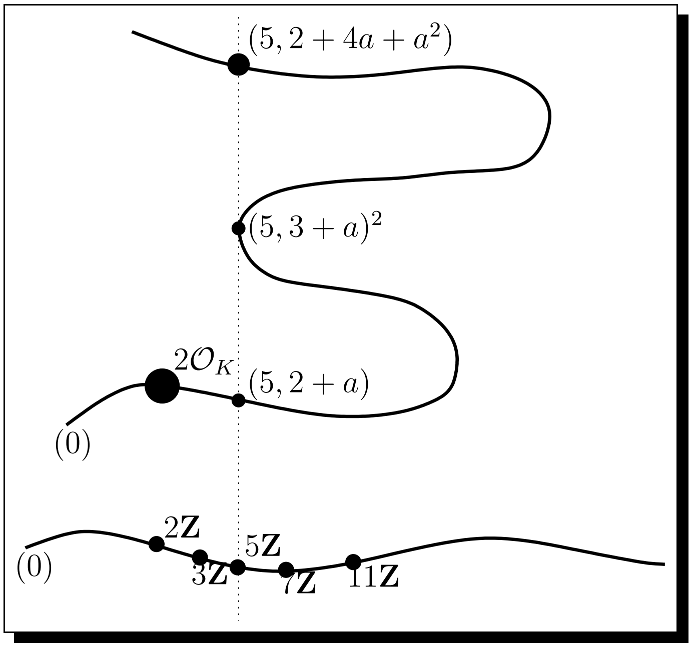


Diagram of $\text{Spec}(\mathcal{O}_K) \to \text{Spec}(\mathbf{Z})$

1.1 A Method for Factoring that Often Works

Suppose $a \in \mathcal{O}_K$ is such that $K = \mathbf{Q}(a)$, and let $g(x)$ be the minimal polynomial of a. Then $\mathbf{Z}[a] \subset \mathcal{O}_K$, and we have a diagram of schemes

$$\begin{tikzcd}
(??) \arrow[r, hook] \arrow[d] & \mathrm{Spec}(\mathcal{O}_K) \arrow[d] \\
\bigcup \mathrm{Spec}(\mathbf{F}_p[x]/(\overline{g}_i^{e_i})) \arrow[r, hook] \arrow[d] & \mathrm{Spec}(\mathbf{Z}[a]) \arrow[d] \\
\mathrm{Spec}(\mathbf{F}_p) \arrow[r, hook] & \mathrm{Spec}(\mathbf{Z})
\end{tikzcd}$$

where $\overline{g} = \prod_i \overline{g}_i^{e_i}$ is the factorization of the image of g in $\mathbf{F}_p[x]$.

The cover $\pi : \mathrm{Spec}(\mathbf{Z}[a]) \to \mathrm{Spec}(\mathbf{Z})$ is easy to understand because it is defined by the single equation $g(x)$. To give a maximal ideal $\mathfrak{p}$ of $\mathbf{Z}[a]$ such that $\pi(\mathfrak{p}) = p\mathbf{Z}$ is the same as giving a homomorphism $\varphi : \mathbf{Z}[x]/(g) \to \overline{\mathbf{F}}_p$ (up to automorphisms of the image), which is in turn the same as giving a root of g in $\overline{\mathbf{F}}_p$ (up to automorphism), which is the same as giving an irreducible factor of the reduction of g modulo p.

Lemma 1.2. *Suppose the index of $\mathbf{Z}[a]$ in $\mathcal{O}_K$ is coprime to p. Then the primes $\mathfrak{p}_i$ in the factorization of $p\mathbf{Z}[a]$ do not decompose further going from $\mathbf{Z}[a]$ to $\mathcal{O}_K$, so finding the prime ideals of $\mathbf{Z}[a]$ that contain p yields the factorization of $p\mathcal{O}_K$.*

Proof. The inclusion map $\mathbf{Z}[a] \hookrightarrow \mathcal{O}_K$ is defined by a matrix over $\mathbf{Z}$ that has determinant $\pm[\mathcal{O}_K : \mathbf{Z}[a]]$, which is coprime to p. The reduction of this matrix modulo p is invertible, so it defines an isomorphism $\mathbf{Z}[a] \otimes \mathbf{F}_p \to \mathcal{O}_K \otimes \mathbf{F}_p$. Any homomorphism $\mathcal{O}_K \to \overline{\mathbf{F}}_p$ is the composition of a homomorphism $\mathcal{O}_K \to \mathcal{O}_K \otimes \mathbf{F}_p$ with a homomorphism $\mathcal{O}_K \otimes \mathbf{F}_p \to \overline{\mathbf{F}}_p$. Since $\mathcal{O}_K \otimes \mathbf{F}_p \cong \mathbf{Z}[a] \otimes \mathbf{F}_p$, the homomorphisms $\mathcal{O}_K \to \overline{\mathbf{F}}_p$ are in bijection with the homomorphisms $\mathbf{Z}[a] \to \overline{\mathbf{F}}_p$, which proves the lemma. □

As suggested in the proof of the lemma, we find all homomorphisms $\mathcal{O}_K \to \overline{\mathbf{F}}_p$ by finding all homomorphism $\mathbf{Z}[a] \to \overline{\mathbf{F}}_p$. In terms of ideals, if $\mathfrak{p} = (g(a), p)\mathbf{Z}[a]$ is a maximal ideal of $\mathbf{Z}[a]$, then the ideal $\mathfrak{p}' = (g(a), p)\mathcal{O}_K$ of $\mathcal{O}_K$ is also maximal, since

$$\mathcal{O}_K/\mathfrak{p}' \cong (\mathcal{O}_K \otimes \mathbf{F}_p)/(g(\tilde{a})) \cong (\mathbf{Z}[a] \otimes \mathbf{F}_p)/(g(\tilde{a})) \subset \overline{\mathbf{F}}_p.$$

We formalize the above discussion in the following theorem:

Theorem 1.3. *Let $f(x)$ denote the minimal polynomial of a over $\mathbf{Q}$. Suppose that $p \nmid [\mathcal{O}_K : \mathbf{Z}[a]]$ is a prime. Let*

$$\overline{f} = \prod_{i=1}^{t} \overline{f}_i^{e_i} \in \mathbf{F}_p[x]$$

where the $\overline{f}_i$ are distinct monic irreducible polynomials. Let $\mathfrak{p}_i = (p, f_i(a))$ where $f_i \in \mathbf{Z}[x]$ is a lift of $\overline{f}_i$ in $\mathbf{F}_p[X]$. Then

$$p\mathcal{O}_K = \prod_{i=1}^{t} \mathfrak{p}_i^{e_i}.$$

We return to the example from above, in which $K = \mathbf{Q}(a)$, where a is a root of $x^5+7x^4+3x^2-x+1$. According to MAGMA, the maximal order $\mathcal{O}_K$ has discriminant 2945785:

```
> Discriminant(MaximalOrder(K));
2945785
```

The order $\mathbf{Z}[a]$ has the same discriminant as $\mathcal{O}_K$, so $\mathbf{Z}[a] = \mathcal{O}_K$ and we can apply the above theorem.

```
> Discriminant(x^5 + 7*x^4 + 3*x^2 - x + 1);
2945785
```

We have

$$x^5 + 7x^4 + 3x^2 - x + 1 \equiv (x+2)\cdot(x+3)^2\cdot(x^2+4x+2) \pmod{5},$$

which yields the factorization of $5\mathcal{O}_K$ given before the theorem.

If we replace a by $b = 7a$, then the index of $\mathbf{Z}[b]$ in $\mathcal{O}_K$ will be a power of 7, which is coprime to 5, so the above method will still work.

```
> f:=MinimalPolynomial(7*a);
> f;
x^5 + 49*x^4 + 1029*x^2 - 2401*x + 16807
> Discriminant(f);
235050861175510968365785
> Discriminant(f)/Discriminant(MaximalOrder(K));
79792266297612001     // coprime to 5
> S<t> := PolynomialRing(GF(5));
> Factorization(S!f);
[
    <t + 1, 2>,
    <t + 4, 1>,
    <t^2 + 3*t + 3, 1>
]
```

Thus 5 factors in $\mathcal{O}_K$ as

$$5\mathcal{O}_K = (5, 7a+1)^2 \cdot (5, 7a+4) \cdot (5, (7a)^2 + 3(7a) + 3).$$

If we replace a by $b = 5a$ and try the above algorithm with $\mathbf{Z}[b]$, then the method fails because the index of $\mathbf{Z}[b]$ in $\mathcal{O}_K$ is divisible by 5.

```
> f:=MinimalPolynomial(5*a);
> f;
x^5 + 35*x^4 + 375*x^2 - 625*x + 3125
> Discriminant(f) / Discriminant(MaximalOrder(K));
95367431640625    // divisible by 5
> Factorization(S!f);
[
    <t, 5>
]
```

1.2 A Method for Factoring that Always Works

There are numbers fields K such that $\mathcal{O}_K$ is not of the form $\mathbf{Z}[a]$ for any $a \in K$. Even worse, Dedekind found a field K such that $2 \mid [\mathcal{O}_K : \mathbf{Z}[a]]$ for *all* $a \in \mathcal{O}_K$, so there is no choice of a such that Theorem 1.3 can be used to factor 2 for K (see Example 1.6 below).

Most algebraic number theory books do not describe an algorithm for decomposing primes in the general case. Fortunately, Cohen's book [Coh93, §6.2]) describes how to solve the general problem. The solutions are somewhat surprising, since the algorithms are much more sophisticated than the one suggested by Theorem 1.3. However, these complicated algorithms all run very quickly in practice, even without assuming the maximal order is already known.

For simplicity we consider the following slightly easier problem whose solution contains the key ideas: *Let $\mathcal{O}$ be any order in $\mathcal{O}_K$ and let p be a prime of $\mathbf{Z}$. Find the prime ideals of $\mathcal{O}$ that contain p.*

To go from this special case to the general case, given a prime p that we wish to factor in $\mathcal{O}_K$, we find a p-maximal order $\mathcal{O}$, i.e., an order $\mathcal{O}$ such that $[\mathcal{O}_K : \mathcal{O}]$ is coprime to p. A p-maximal order can be found very quickly in practice using the "round 2" or "round 4" algorithms. (Remark: Later we will see that to compute $\mathcal{O}_K$, we take the sum of p-maximal orders, one for every p such that p^2 divides $\mathrm{Disc}(\mathcal{O}_K)$. The time-consuming part of this computation of $\mathcal{O}_K$ is finding the primes p such that $p^2 \mid \mathrm{Disc}(\mathcal{O}_K)$, not finding the p-maximal orders. Thus a fast algorithm for factoring integers would not only break many cryptosystems, but would massively speed up computation of the ring of integers of a number field.)

Algorithm 1.4. Suppose $\mathcal{O}$ is an order in the ring $\mathcal{O}_K$ of integers of a number field K. For any prime $p \in \mathbf{Z}$, the following (sketch of an) algorithm computes the set of maximal ideals of $\mathcal{O}$ that contain p.

Sketch of algorithm. Let $K = \mathbf{Q}(a)$ be a number field given by an algebraic integer a as a root of its minimal monic polynomial f of degree n. We assume that an order $\mathcal{O}$ has been given by a basis $w_1, \ldots, w_n$ and that $\mathcal{O}$ that contains $\mathbf{Z}[a]$. Each of the following steps can be carried out efficiently using little more than linear algebra over $\mathbf{F}_p$. The details are in [Coh93, §6.2.5].

1. [Check if easy] If $p \nmid \mathrm{disc}(\mathbf{Z}[a])/\mathrm{disc}(\mathcal{O})$ (so $p \nmid [\mathcal{O} : \mathbf{Z}[a]]$), then by a slight modification of Theorem 1.3, we easily factor $p\mathcal{O}$.

2. [Compute radical] Let I be the *radical* of $p\mathcal{O}$, which is the ideal of elements $x \in \mathcal{O}$ such that $x^m \in p\mathcal{O}$ for some positive integer m. Using linear algebra over the finite field $\mathbf{F}_p$, we can quickly compute a basis for $I/p\mathcal{O}$. (We never compute $I \subset \mathcal{O}$.)

3. [Compute quotient by radical] Compute an $\mathbf{F}_p$ basis for

   $$A = \mathcal{O}/I = (\mathcal{O}/p\mathcal{O})/(I/p\mathcal{O}).$$

   The second equality comes from the fact that $p\mathcal{O} \subset I$, which is clear by definition. Note that $\mathcal{O}/p\mathcal{O} \cong \mathcal{O} \otimes \mathbf{F}_p$ is obtained by simply reducing the basis $w_1, \ldots, w_n$ modulo p.

4. [Decompose quotient] The ring A is a finite Artin ring with no nilpotents, so it decomposes as a product $A \cong \prod \mathbf{F}_p[x]/g_i(x)$ of fields. We can quickly find such a decomposition explicitly, as described in [Coh93, §6.2.5].

5. [Compute the maximal ideals over p] Each maximal ideal $\mathfrak{p}_i$ lying over p is the kernel of $\mathcal{O} \to A \to \mathbf{F}_p[x]/g_i(x)$.

The algorithm finds all primes of $\mathcal{O}$ that contain the radical I of $p\mathcal{O}$. Every such prime clearly contains p, so to see that the algorithm is correct, we must prove that the primes $\mathfrak{p}$ of $\mathcal{O}$ that contain p also contain I. If $\mathfrak{p}$ is a prime of $\mathcal{O}$ that contains p, then $p\mathcal{O} \subset \mathfrak{p}$. If $x \in I$ then $x^m \in p\mathcal{O}$ for some m, so $x^m \in \mathfrak{p}$ which implies that $x \in \mathfrak{p}$ by primality of $\mathfrak{p}$. Thus $\mathfrak{p}$ contains I, as required.

1.3 Essential Discriminant Divisors

Definition 1.5. A prime p is an *essential discriminant divisor* if $p \mid [\mathcal{O}_K : \mathbf{Z}[a]]$ for *every* $a \in \mathcal{O}_K$.

Since $[\mathcal{O}_K : \mathbf{Z}[a]]$ is the absolute value of $\mathrm{Disc}(f(x))/\mathrm{Disc}(\mathcal{O}_K)$, where $f(x)$ is the characteristic polynomial of $f(x)$, an essential discriminant divisor divides the discriminant of the characteristic polynomial of any element of $\mathcal{O}_K$.

Example 1.6 *(Dedekind).* Let $K = \mathbf{Q}(a)$ be the cubic field defined by a root a of the polynomial $f = x^3 + x^2 - 2x + 8$. We will use MAGMA, which implements the algorithm described in the previous section, to show that 2 is an essential discriminant divisor for K.

```
> K<a> := NumberField(x^3 + x^2 - 2*x + 8);
> OK := MaximalOrder(K);
> Factorization(2*OK);
[
<Prime Ideal of OK
Basis:
[2 0 0]
[0 1 0]
[0 0 1], 1>,
<Prime Ideal of OK
Basis:
[1 0 1]
[0 1 0]
[0 0 2], 1>,
<Prime Ideal of OK
Basis:
[1 0 1]
[0 1 1]
[0 0 2], 1>
]
```

Thus $2\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, with the $\mathfrak{p}_i$ distinct. Moreover, one can check that $\mathcal{O}_K/\mathfrak{p}_i \cong \mathbf{F}_2$. If $\mathcal{O}_K = \mathbf{Z}[a]$ for some $a \in \mathcal{O}_K$ with minimal polynomial g, then $\overline{g}(x) \in \mathbf{F}_2[x]$ must be a product of three *distinct* linear factors, which is impossible.

2 The Chinese Remainder Theorem

Let $\mathcal{O}_K$ be the ring of integers of a number field.

Theorem 2.1 (Chinese Remainder Theorem). *Suppose $I_1, \ldots, I_n$ are ideals of $\mathcal{O}_K$ such that $I_j + I_k = (1)$ for any $i \neq j$. Then the natural map $\mathcal{O}_K \to \prod \mathcal{O}_K/I_j$ induces an isomorphism*

$$\mathcal{O}_K/\left(\prod I_j\right) \to \prod \mathcal{O}_K/I_j.$$

Thus if we choose $a_j \in I_j$ then there exists $a \in \mathcal{O}_K$ such that $a \equiv a_j \pmod{I_j}$ for $j = 1, \ldots, n$.

Lemma 2.2. *Suppose I, J are nonzero integral ideals in $\mathcal{O}_K$. Then there exists $a \in I$ such that $(a)/I$ is coprime to J.*

The next proposition asserts that every ideal of the ring of integers of a number field can be generated, as an ideal, by two elements.

Proposition 2.3. *Suppose I is called an ideal in the ring $\mathcal{O}_K$ of integers of a number field. Then there exist $a, b \in \mathcal{O}_K$ such that $I = (a, b)$.*

3 Discriminants

Let K be a number field of degree n. Then there are n embeddings

$$\sigma_1, \ldots, \sigma_n : K \to \mathbf{C}.$$

Reorder these embeddings so the first r have image $\mathbf{R}$ and the remaining $s = n - r$ have image $\mathbf{C}$. Let σ by the product map $a \mapsto (\sigma_1(a), \ldots, \sigma_n(a))$.

Definition 3.1 (Discriminant). Suppose $a_1, \ldots, a_n$ is a $\mathbf{Q}$-basis of K. The *discriminant* of $a_1, \ldots, a_n$ is

$$\mathrm{Disc}(a_1, \ldots, a_n) = \det(\mathrm{Tr}(a_i a_j)_{i,j=1,n}).$$

4 Norms of Ideals

Definition 4.1 (Norm of Fractional Ideal). Suppose I is a fractional ideal of $\mathcal{O}_K$. The *norm* of I is the lattice index

$$\mathrm{Norm}(I) = [\mathcal{O}_K : I] \in \mathbf{Q}_{\geq 0}.$$

This lattice index is by definition the absolute value of the determinant of any $\mathbf{Q}$-linear automorphism of K that sends $\mathcal{O}_K$ onto I, or 0 if $I = (0)$.

Proposition 4.2. *If I and J are fractional ideals, then*

$$\mathrm{Norm}(IJ) = \mathrm{Norm}(I)\,\mathrm{Norm}(J).$$

5 The Class Group

Definition 5.1 (Class Group). Let $\mathcal{O}_K$ be the ring of integers of a number field K. The *class group* C_K of K is the group of nonzero fractional ideals modulo the sugroup of principal fractional ideals (a), for $a \in K$.

If we let $\mathrm{Div}(K)$ denote the group of nonzero fractional ideals, then there is an exact sequence

$$0 \to \mathcal{O}_K^* \to K^* \to \mathrm{Div}(K) \to C_K \to 0.$$

Theorem 5.2 (Finiteness of the Class Group). *Every ideal class in C_K contains an integral ideal of norm at most*

$$\sqrt{|\,\mathrm{Disc}(K)|} \cdot \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n},$$

where s is the number of complex conjugate embeddings of K. Thus the class group C_K of any number field K is finite.

The bound in the theorem is called the Minkowski bound, and I think it is the best known unconditional general bound (though there are better bounds in certain special cases).

5.1 The Group of Units

Definition 5.3 (Unit Group). The *group of units* U_K associated to a number field K is the group of elements of $\mathcal{O}_K$ that have an inverse in $\mathcal{O}_K$.

Proposition 5.4. *An element $a \in K$ is a unit if and only if* $\mathrm{Norm}(a) = \pm 1$.

Theorem 5.5. *The group U_K of units of $\mathcal{O}_K$ is the product of a finite cyclic group of roots of unity with a free abelian group of rank $r + s - 1$, where r is the number of real embeddings of K and s is the number of complex conjugate pairs of embeddings.*

Example 5.6 *(Pell's Equation).* The classical Pell's equation is, given square-free $d > 0$, to find all positive integer solutions (x, y) to the equation $x^2 - dy^2 = 1$. Note that if $x + y\sqrt{d} \in \mathbf{Q}(\sqrt{d})$, then

$$\mathrm{Norm}(x + y\sqrt{d}) = (x + y\sqrt{d})(x - y\sqrt{d}) = x^2 - dy^2.$$

The solutions to Pell's equation thus form a finite-index subgroup of the group of units in the ring of integers of $\mathbf{Q}(\sqrt{d})$. Theorem 5.5 implies that for any d the solutions to Pell's equation form an infinite cyclic group, a fact that takes substantial work to prove using only elementary number theory (for example, using continued fractions).

References

[Coh93] H. Cohen, *A course in computational algebraic number theory*, Springer-Verlag, Berlin, 1993. MR 94i:11105

[EH00] D. Eisenbud and J. Harris, *The geometry of schemes*, Springer-Verlag, New York, 2000. MR 2001d:14002

[LL93] A. K. Lenstra and H. W. Lenstra, Jr. (eds.), *The development of the number field sieve*, Springer-Verlag, Berlin, 1993. MR 96m:11116