Binary quadratic forms and quadratic number fields

Prof. G. Wüstholz

Contents

1 Introduction and Motivation
  (Febr. 20, 2012)..............2

2 Sums of two squares
  (Febr. 24, 2012)...............6

3 Number rings
  (Febr. 26, 2012)..............8

4 Factorization
  (March 4, 2012)..............11

5 Primes in Gaussian numbers rings
  (March 12, 2012)............15

6 Ideals in quadratic number rings
  (March 19, 2012)...........18

7 Ideal factorization
  (March 26, 2012)............22

8 Prime ideals
  (March 26, 2012)............25

9 Fractional ideals
  (April 2, 2012)...............27

10 The three squares theorem
    (April 16, 2012)...........30

11 The four squares theorem
    (April 20, 2012)...........31

12 Binary quadratic forms
    (April 30, 2012)...........33

13 Class groups
    (May 7, 2012)...............36

14 Representations of integers by binary quadratic forms
    (May 14, 2012)............39

List of Abbreviations

1
In this course we connect different areas from algebra and number theory in order to obtain deeper knowledge; the common theme is “quadraticity”. The notes were typed by C. Fuchs; for comments and corrections send an email to clemens.fuchs@math.ethz.ch.
1 Introduction and Motivation
(Febr. 20, 2012)

A binary quadratic form is a polynomial
\[ q(x, y) = ax^2 + bxy + cy^2 \]
with coefficients \( a, b, c \) which we assume to be in \( \mathbb{Z} \). Writing \( x = (x, y) \) the form \( q \) can be expressed as
\[ (x, y)Q \begin{pmatrix} x \\ y \end{pmatrix} = x^T Q x \]
with
\[ Q = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}, \quad a, b, c \in \mathbb{Z}; \]
and discriminant \( d_Q = d_q = b^2 - 4ac = -4 \det Q \). We say that \( q \) is primitive if and only if \( (a, b, c) = 1 \).

Binary quadratic forms come up naturally in the context of quadratic number fields. Let \( d \) be a square-free integer and put \( K = \mathbb{Q}(\sqrt{d}) \). Then
\[ q_K(x, y) = \begin{cases} x^2 - dy^2, & d \not\equiv 1 \pmod{4}, \\ x^2 + xy + (1 - d)y^2/4, & d \equiv 1 \pmod{4}. \end{cases} \]
is a canonical binary quadratic form associate with the field \( K \).

There is a natural action of \( SL(2, \mathbb{Z}) \) on the space of binary quadratic forms which is deduced from the natural action on \( \mathbb{Z} \times \mathbb{Z} \) given by \( (x, y) \mapsto (\alpha x + \beta y, \gamma x + \delta y) \) for
\[ g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) \]
and this leads to an equivalence relation with
\[ q \sim q^g \iff \exists g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) : q^g(x, y) = (gq)(x, y) = q(\alpha x + \beta y, \gamma x + \delta y). \]

Since the discriminant of a binary quadratic form is invariant under the action of \( SL(2, \mathbb{Z}) \) it is clear that \( q \sim q^g \Rightarrow d_q = d_{q^g} \). However the important fact is that \( "\Rightarrow" \) is not true and this leads to a rich mathematical theory.
As an example we may take the forms \( q_1 = x^2 + 6y^2, q_2 = 2x^2 + 3y^2 \) with \( d_1 = d_2 = -24 \). Then \( 5 = q_2(1, 1) \) but \( q_1(x, y) = x^2 + 6y^2 \) never takes the value 5. This means that the two forms are not equivalent though they have the same discriminant. The example shows that the set of values of a quadratic form gives important information about the form and its class.

Since centuries one of the main questions about binary quadratic forms was which numbers are represented by the form. We say that \( q \) represents an integer \( n \) if and only if \( \exists x, y \in \mathbb{Z} : n = q(x, y) \). It is obvious that if \( q \sim q^g \) then \( n \) is represented by \( q \iff n \) is represented by \( q^g \). As a consequence we see that the set of values of a quadratic form is independent of the form in the equivalence class under \( \text{SL}_2(\mathbb{Z}) \). It remains to give a characterization of the value set and this is where the theory of genera came up. We shall discuss and explain this in the final lecture.
There is a close relation between quadratic forms and fractional ideals. Let $K = \mathbb{Q}(\sqrt{d}) \supset b$ be a fractional ideal. This means that there exists an ideal $a \subseteq \mathbb{Q}(\sqrt{d})$ and some $c \in K^\times$ such that

$$b = a : c = \{ x \in K; cx \in a \}.$$ 

Let $b_1, b_2$ be fractional ideals, then $b_1 \sim b_2 \iff \exists \alpha \in K^\times : b_2 = (\alpha)b_1$. We denote by $C_K$ the group of equivalence classes of fractional ideals in $K$.

Let $b_1, b_2$ be fractional ideals, then $b_1 \sim b_2 \iff \exists \alpha \in K^\times : b_2 = (\alpha)b_1$. We denota by $C_K$ the group of equivalence classes of fractional ideals in $K$.

Let $a$ be a fractional ideal and let $\text{Gal}(K/\mathbb{Q}) = \{1, \sigma\}$ be the Galois group of $K$ over $\mathbb{Q}$. We associate with $a = Z(a_1 + Za_2)$ the binary quadratic form

$$q_a(x, y) = N(a)^{-1}(xa_1 + ya_2)(xa_1^\sigma + ya_2^\sigma)$$

with $1 \neq \sigma \in \text{Gal}(K/\mathbb{Q})$. The rational number $N(a)$ is defined as follows:

- $a \subset O_K \Rightarrow N(a) = O_K/a$
- $a, b \subset O_K \Rightarrow N(ab) = N(a)N(b)$
- extend to fractional ideals.

The form $q_a(x, y) = N(a)^{-1}(a_1a_2^\sigma x^2 + (a_1a_2^\sigma + a_1^\sigma a_2)x y + a_2a_2^\sigma y^2)$ is called the quadratic form associated with $a$.

We denote by $\mathcal{Q}(d)$ the set of equivalence classes of binary quadratic forms with discriminant $d$ and if $d$ is the discriminant of a quadratic number field $K$ then we also write $\mathcal{Q}_K$. The question is whether there exists a bijection

$$\kappa : C_K \rightarrow \mathcal{Q}_K.$$ 

We shall see that this is not always the case and that the group $C_K$ is too small in general. In other words, the equivalence relation is not quite the right one. One needs a more narrow equivalence relation and gets a new group $C_K^+$, called narrow class group, which in some cases coincides with the class group $C_K$ and in some cases it is an extension

$$0 \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow C_K^+ \rightarrow C_K \rightarrow 0$$

of the class group by the group $\mathbb{Z}/2\mathbb{Z}$. One shows that there is a bijection

$$\kappa : C_K^+ \rightarrow \mathcal{Q}_K.$$ 

In particular the number of equivalence classes of quadratic forms with discriminant $d$ is the order of the group $C_K^+$.

The group $C_K^+$ gives much information about whether a given integer $n$ is represented by the norm form $q_K$. As an example we shall deal with the case that $|C_K^+| = 1$. Then we say that $n$ is (properly) represented by the norm form $q_K$ if there exist $x, y \in \mathbb{Z}$ with $(x, y) = 1$ and $n = q_K(x, y)$. We shall show that this is the case if and only if the congruence

$$x^2 \equiv d_K \mod 4n$$

has a solution and if $d_K < 0$ in the case $n < 0$. The congruence is solvable if and only if $(\frac{d_K}{4n}) = 1$; here $(\frac{m}{n})$ stands for the Kronecker symbol.

Another related question is, whether a given quadratic form represents a prime number $p$. Let $q(x, y) \in \mathcal{Q}_K$ be such a form with discriminant $d_K$. Then it is possible to show that $q$ represents $p$ if and only if the class (corresponding to) $q$ under $\kappa$ is of the form $c^+(p)$ for some prime ideal
\( p \subseteq \mathcal{O}_K \) with \( N(p) = p \). This leads immediately to the question, which prime ideals have a prime norm. The answer is given by the theory of fractional ideals in \( K \). One has to study the question how a prime \( p \in \mathbb{Q} \) decomposes in \( K \). It can be shown that the following possibilities come up:

(i) \( (p) \) is prime
(ii) \( (p) = p \cdot p^\sigma \) (\( \text{Gal}(K/\mathbb{Q}) = \langle \sigma \rangle \))
(iii) \( (p) = p^2 \)

In the first case \( p \) is called inert, in the second case \( p \) is called split and in the third case \( p \) is called ramified. The norms are

- \( p^2 = N((p)) \)
- \( p^2 = N(p) \cdot N(p^\sigma) = N(p)^2 \)
- \( p^2 = N(p)^2 \)

and in the last two cases \( p = N(p) \). The question is then: when do the cases (ii) and (iii) come up. The answer is given in terms of the discriminant and the Legendre symbol.

This leads us to an old problem: which numbers are of the form \( x^2 + ny^2 \). The question goes back at least to Fermat who asserted in 1640 that an odd prime \( p \) is a sum of square

\[
p = x^2 + y^2, \quad x, y \in \mathbb{Z}
\]

\( \Leftrightarrow p \equiv 1 \pmod{4} \). He did not give a proof but announced it in a letter to Mersenne dated December 25, 1640. A first proof was given by Euler (Letter to Goldbach on April 12, 1749), another proof by Lagrange in 1775 based on his work on quadratic forms, simplified in the Disquisitiones Arithmeticae, and by Dedekind using the field \( \mathbb{Q}[i] \). The general question when an integer \( n \) can be represented as a sum of squares

\[
n = x^2 + y^2, \quad x, y \in \mathbb{Z}
\]

can be answered by reducing it to primes.

Fermat extended the assertion (Letter to Pascal, September 25, 1654) and announced that for odd primes

\[
p = x^2 + 2y^2 \Leftrightarrow p \equiv 1, 3 \pmod{8}
\]
\[
p = x^2 + 3y^2 \Leftrightarrow p \equiv 1 \pmod{3}
\]

and Euler added as a conjecture

\[
p = x^2 + 5y^2 \Leftrightarrow p \equiv 1, 9 \pmod{29}
\]

The statements were established by Lagrange.

In 1798 Legendre stated that a positive integer \( n \) can be expressed as \( n = x^2 + y^2 + z^2 \Leftrightarrow n \neq 4^a(8m + 7) \). His proof was incomplete and Gauss gave a complete proof in the Disquisitiones.

The first “universal” result on representations of integers as a sum of squares is Lagrange’s four-square theorem (Lagrange, 1770): Every positive integer is a sum of four squares. The theorem had been conjectured by Bachet.

The four-squares theorem leads us to a very interesting question: Which diagonal forms

\[
q = ax^2 + by^2 + cz^2 + dw^2
\]
\(a, b, c, d \in \mathbb{N}\) coprime, are universal in the sense that they represent each positive integer \(n\)? The answer was given by Ramanujan by writing down a complete list of 55 forms. Ramanujan's list had to be corrected later since the diagonal form \(x^2 + 2y^2 + 5z^2 + 5w^2\) had to be eliminated.

More recently a very interesting and surprising series of papers were published. It concerns the question whether the four-squares theorem also holds generally for arbitrary quaternary positive definite form. The answer is the Conway-Schneeberger Fifteen Theorem: If a positive definite quaternary quadratic form has an integer matrix representation and represents all positive integers up to 15 then it represents all positive integers.

Here the distinction concerning the matrix representation is essential. There is a difference between integer valued quadratic forms and quadratic forms with associated matrix having integers as coefficients as in the theorem. If we are in the case of integer valued quaternary forms then Manjul Bhargava and Jonathan P. Hanke proved that: If a positive definite quadratic form with integer coefficients represents the 29 integers 1, 2, 3, 5, 6, 7, 10, 13, 14, 15, 17, 19, 21, 22, 23, 26, 29, 30, 31, 34, 35, 37, 42, 58, 93, 110, 145, 209, 290 then it represents all positive integers.
2 Sums of two squares  
(Febr. 24, 2012)

In this lecture we turn to the question under which condition a given non-negative integer can be written as a sum of 2 squares.

**Theorem 2.1.** Every prime \( p \equiv 1 \pmod{4} \) is a sum of two squares.

**Theorem 2.2.** A positive integer \( n \) is a sum of two squares \( \iff \) \( n = 2^a \prod_{p \mid n} p^{b_p} \prod_{q \mid n} q^{c_q}, \ c \equiv 0 \pmod{2} \).

The proof of Theorem 2.1 will be given later. At the end of this lecture we shall shortly describe how the proof works. There are many other and quite different proofs in the literature. Here we shall show how it implies Theorem 2.2. This is done by a sequence of lemmata.

**Lemma 2.1.** \( m, n \) sums of squares then \( mn \) sums of squares.

*Proof.* This is a simple application of an identity about sum of squares going back to Euler:

\[
(a_1 x_1^2 + bx_1 y_1 + a_2 c y_1^2)(a_2 x_2^2 + bx_2 y_2 + a_1 c y_2^2) = a_1 a_2 X^2 + bXY + cY^2
\]

for

\[
X = x_1 x_2 - cy_1 y_2, \quad Y = a_1 x_1 y_2 + a_2 y_1 x_2 + by_1 y_2.
\]

We choose \( x_1, y_1 \in \mathbb{Z} \) such that \( m = x_1^2 + y_1^2 \) and \( x_2, y_2 \in \mathbb{Z} \) such that \( n = x_2^2 + y_2^2 \) and get \( mn = X^2 + Y^2 \). //

The next lemma is a priori a statement about quadratic residues and follows from the first supplement to the quadratic reciprocity law. We give an elementary proof of it not making use of the Legendre symbol.

**Lemma 2.2.** \( x^2 \equiv -1 \pmod{p}, p \) odd prime has a solution \( \iff \pmod{4} \).

*Proof.* This is a simple application of Wilson’s theorem. “\( \Rightarrow \)”: \( x^2 \equiv -1 \pmod{p} \) implies that

\[
1 \equiv x^{p-1} = (x^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2} = \begin{cases} 1, & p \equiv 1 \pmod{4} \\ -1, & p \equiv 3 \pmod{4} \end{cases}
\]

and this shows that \( p \equiv 1 \pmod{4} \). “\( \Leftarrow \)”: By Wilson

\[
-1 \equiv (p - 1)! = (1 \cdot 2 \cdot \ldots \cdot \frac{p}{2})(\frac{p + 1}{2} \cdot \ldots \cdot (p - 1)) = \left(\frac{p - 1}{2}\right)!(p - \frac{p - 1}{2})\ldots(p - 1) \\
\equiv \left(\frac{p - 1}{2}\right)!(-1)^{(p-1)/2} \left(\frac{p - 1}{2}\right)! = (-1)^{(p-1)/2} \left(\frac{p - 1}{2}\right)^2
\]

(mod \( p \)) and gives the solution \( x = ((p - 1)/2)! \). //

The next lemma is the main step in the proof of Theorem 2.2 on the basis of Theorem 2.1.

**Lemma 2.3.** \( 0 \neq n = x^2 + y^2, q \equiv 3 \pmod{4}, n = q^a m \) with \( (q, m) = 1 \). Then \( a \equiv 0 \pmod{2} \).
Proof. We first show that \( q | n \) implies that \( q | x \) and \( q | y \). Otherwise wlog \((q, x) = 1\). and this means that \( x \) is invertible mod \( q \) and we get \((yx^{-1})^2 \equiv -1 \pmod{q}\). By Lemma 2.2 we conclude that \( q \equiv 1 \pmod{4} \), a contradiction. This proves our assertion.

Let now \( q^a \) be the highest power of \( q \) with \( q^a | x, q^a | y \). Then \( q^{2a} | n \) and we claim that \( q^{2a+1} \nmid n \).

To see that write

\[
X = x/q^a, \quad Y = y/q^a, \quad N = n/q^{2a}.
\]

Then \( N = X^2 + Y^2 \) and \((X, q) = 1 \) or \((Y, q) = 1\). If \( q | N \) we get again \((YX^{-1})^2 \equiv -1 \pmod{q}\) and once again Lemma 2.3 gives \( q \equiv 1 \pmod{4} \), a contradiction. This proves the lemma.

We show that Theorem 2.1 implies Theorem 2.2.

\( \Rightarrow \): This is Lemma 2.3.

\( \Leftarrow \): For \( p = 2 \) or \( p \equiv 1 \pmod{4} \) we take \( 2 = 1^2 + 1^2 \) and \( p^2 = p^2 + 0^2 \). For \( p \equiv 3 \pmod{4} \) we use Theorem 2.1.

As mentioned at the beginning we briefly give the main idea of the proof of Theorem 2.1. We work over the field \( \mathbb{Q}[i] \) with \( \mathbb{Z}[i] \) euclidean and therefore a unique factorization domain and show that \( p = N(\alpha) \) for some \( \alpha = x + iy \). Then \( p = (x + iy)(x - iy) = x^2 + y^2 \).
3 Number rings  
(Febr. 26, 2012)

We take a square-free integer $d$ and consider the set

$$Q(\sqrt{d}) = \{ r + s\sqrt{d}; r, s \in Q \} = Q[T]/(T^2 - d).$$

This is a priori only a vector space over over $Q$ of dimension 2 with basis 1, $\sqrt{d}$, but it is an easy exercise (do it!) that this is indeed a field, a quadratic number field. For $d > 0$ we call the field real quadratic, for $d < 0$ imaginary quadratic.

a) Determination of the ring of integers $O_d$

A quadratic number field is an extension of degree two of $Q$ and is therefore Galois over $Q$. Its Galois group is $\text{Gal}(Q(\sqrt{d})/Q) = \{1, \sigma\}$ with $\sigma \neq 1$ and $\sigma^2 = 1$. We introduce several operations on $Q[\sqrt{d}]$ related to $\text{Gal}(Q(\sqrt{d})/Q)$:

- **conjugation**: $\sigma: \xi = r + s\sqrt{d} \mapsto \xi^\sigma = r - s\sqrt{d} = (r + s\sqrt{d})^\sigma$
- **norm**: $N_{Q(\sqrt{d})/Q}: Q(\sqrt{d})^\times \to Q^\times , \xi \mapsto N(\xi) := \xi \cdot \xi^\sigma$. The norm is a (multiplicative) group homomorphism.
- **trace**: $Tr_{Q(\sqrt{d})/Q}: Q(\sqrt{d}) \to Q, \xi \mapsto Tr(\xi) := \xi + \xi^\sigma$. The trace is a (additive) group homomorphism.

One calculates $N(\xi) = r^2 - ds^2, Tr(\xi) = 2r$ and one sees that the minimal polynomial for $\xi$ is $(T - \xi)(T - \xi^\sigma) = T^2 - Tr(\xi)T + N(\xi)$. Using norm and trace we make the following

**Definition.** $\xi \in Q[\sqrt{d}]$ is called integral $\iff N(\xi), Tr(\xi) \in Z$.

It is easy to determine the integral elements of $Q[sqrt{d}]$. It is clear that

$$N(\xi), Tr(\xi) \in Z \iff r^2 - ds^2, 2r \in Z.$$  

We write $r = a/c, s = b/c, (a, b, c) = 1$ and find that

$$2r, r^2 - ds^2 \in Z \iff c \mid 2a \land c^2 \mid (a^2 - db^2).$$

Now, if $e = (a, c)$, then $e|b \Rightarrow e|(a, b, c) = 1 \Rightarrow e = 1$. This gives $(a, c) = 1$, whence $c \in \{1, 2\}$.

We shall show that

$$O_d = \{ \frac{u + v\sqrt{d}}{2} ; u, v \in Z, u^2 - dv^2 \equiv 0 \pmod{4} \}.$$

To verify this we denote by $U$ the right hand side and first show that it contains $O_d$. Let $\xi$ be in $O_d$. Then

$$\xi = \begin{cases} 
  a + b\sqrt{d}, & \text{if } c = 1 \\
  (a + b\sqrt{d})/2, & a^2 + b^2d \equiv 0 \pmod{4}, \text{ if } c = 2.
\end{cases}$$

Writing $u = 2a/c, v = 2b/c$ we find that

$$\xi = (u + v\sqrt{d})/2, u^2 - dv^2 \equiv 0 \pmod{4}.$$
which leads to $\xi \in U$. For the inclusion $U \subseteq \mathcal{O}_d$ we just take the norm $N(\xi)$ and the trace $Tr(\xi)$ and the congruence condition shows that they are both integers.

we have to solve the congruence $u^2 - dv^2 \equiv 0 \pmod{4}$. The solution depends on the congruence class of $d$ modulo 4. In the case case $d \equiv 2, 3 \pmod{4}$ we get $u^2 - 2v^2 \equiv 0 \pmod{4}$ if $d \equiv 2 \pmod{4}$ and $u^2 + v^2 \equiv 0 \pmod{4}$ if $d \equiv 3 \pmod{4}$. If $d \equiv 1 \pmod{4}$ we have to solve the congruence $u^2 - v^2 \equiv 0 \pmod{4}$. In the case $d \equiv 2 \pmod{4}$ we have $u^2 \equiv 0 \pmod{2}$ and $v^2 \equiv 0 \pmod{2}$ and this leads to $u \equiv v \pmod{2}$. If $d \equiv 3 \pmod{4}$, since squares are either congruent to 0 or to 2 modulo 4, we conclude that the first alternative occurs and then again $u \equiv v \pmod{2}$. In the case $d \equiv 1 \pmod{4}$ we have

$$u^2 - v^2 \equiv 0 \pmod{4} \iff u \equiv v \pmod{2},$$

that is $u = v + 2w$ for some $w \in \mathbb{Z}$. We conclude that $\xi = \frac{1}{2}(v + 2w + v\sqrt{d}) = w + v(1 + \sqrt{d})/2$ and this is in $\mathcal{O}_d$. The final result is

**Theorem 3.1.** The integers in $\mathbb{Q}[\sqrt{d}]$ are

(i) $\mathcal{O}_d = \{a + b\sqrt{d}; a, b \in \mathbb{Z}\}$, if $d \equiv 2, 3 \pmod{4}$

(ii) $\mathcal{O}_d = \{a + b\frac{1+\sqrt{d}}{2}; a, b \in \mathbb{Z}\}$, if $d \equiv 1 \pmod{4}$.

We shall write

$$\omega = \begin{cases} \frac{1+\sqrt{d}}{2}, & d \equiv 1 \pmod{4}, \\ \sqrt{d}, & d \equiv 2, 3 \pmod{4}. \end{cases}$$

and the $\mathcal{O}_d$ can be written uniformly as $\mathcal{O}_d = \mathbb{Z} + \mathbb{Z}\omega$. We also may replace $\omega$ by $(d - \sqrt{d})/2$ with the same effect. The discriminant becomes

$$d_K = \det \left( \begin{array}{cc} 1 & \omega \\ 1 & \omega^\sigma \end{array} \right)^2 = \begin{cases} d, & d \equiv 1 \pmod{4}, \\ 4d, & d \equiv 2, 3 \pmod{4}. \end{cases}$$

We see then that either $d_K$ is odd or of the form $d_K = 8\delta$ and $d_K = 4\delta$ respectively with $\delta$ odd.

b) **Determination of units:**

We denote by $U_d = \mathcal{O}_d^\times$ the group of invertible elements in $\mathcal{O}_d$. By definition

$$\varepsilon = \frac{1}{2}(a + b\sqrt{d}) \in U_d \iff \exists \varepsilon^\sigma \in \mathcal{O}_d : \varepsilon \varepsilon^\sigma = 1.$$ 

On taking the norm we get $1 = N(\varepsilon \varepsilon^\sigma) = N(\varepsilon)N(\varepsilon^\sigma)$ which leads to $N(\varepsilon) = \pm 1$ which is equivalent to the famous Pell’s equation

$$a^2 - db^2 = \pm 4.$$  (Pell’s equation).

Let $\mathcal{P}(d)$ be the set of solutions of the Pell equation.

**Theorem 3.2.** $(u, v) \mapsto \frac{1}{2}(u + v\sqrt{d})$ gives bijection $\mathcal{P}(d) = \{(u, v); u^2 - dv^2 = \pm 4\} \mapsto U_d$.

A famous theorem, Dirichlet’s unit theorem says that $U_d$ is a finitely generated abelian group and this means that $U_d \cong \mathbb{Z}^r \times U_{d,tor}$ with $r$ the rank of $U_d$ which is 0 if $d < 0$ and 1 if $d > 0$ in which case $U_{d,tor}$ is finite. Unfortunately Dirichlet’s Unit Theorem does not give a constructive way to find the units in $\mathcal{O}_d$. In the case of a real quadratic number field – and this is the only interesting case for quadratic number fields – there is an alternative way through the theory of continued fractions. (see [10]). However we can easily determine the torsion subgroup in both, the real and imaginary quadratic case. This gives all units in the imaginary quadratic.
Theorem 3.3. The torsion group \( U_{d,\text{tor}} \) is \( \mu_2 \) except in the case \( d = -1 \) and \( d = -3 \) where \( U_{-1,\text{tor}} = \mu_4 \) and \( U_{-3,\text{tor}} = \mu_6 \).

Proof. We know from algebra that a subgroup of the multiplicative group of a field is a group of roots of unity. This shows that \( U_{d,\text{tor}} \supseteq \mu_2 \) and we have to determine, if any, the remaining roots of unity. In the case \( d > 0 \) the only roots of unity are \( \pm 1 \). If \( d \leq -5 \) then we must have \( \pm 4 = u^2 - dv^2 \geq u^2 + 5v^2 \) and this immediately leads to \( v = 0, u^2 = 4 \) and then to \( v = 0, u = \pm 2 \). An application of Theorem 3.2 then gives \( U_d = \{ \pm 1 \} = \mu_2 \). In the case \( d = -1 \) one gets \( u^2 + v^2 = 4 \) and in the case \( d = -3 \) one has to solve \( u^2 + 3v^2 = 4 \). In the first case this gives \( u = \pm 2, v = 0 \) or \( u = 0, v = \pm 2 \) and then \( U_{-1,\text{tor}} = \{(u + v\sqrt{-1})/2 = \{\pm 1, \pm i\} = \mu_4 \). In the second case \( d = -3 \) one has \( u = \pm 1, v = \pm 1 \) implying that \( U_{-3,\text{tor}} = \{(u + v\sqrt{-3})/2; u, v = \pm 1\} = \mu_6 \). //
4 Factorization
(March 4, 2012)

In \( \mathbb{Z} \) there are two different possibilities to define a prime number \( p \), namely to say that \( p \)
satisfies one of

a) \( p \) prime number \( \iff (p = ab \Rightarrow a \text{ unit or } b \text{ unit}), \)
b) \( (p) \) prime ideal \( \iff (ab \in (p) \Rightarrow a \in (p) \text{ or } b \in (p)) \).

For \( \mathbb{Z} \) both definitions are equivalent, i.e. \( p \) prime number \( \iff (p) \) prime ideal. One immediately
deduces that in \( \mathbb{Z} \) we have unique factorization.

Now we replace \( \mathbb{Z} \) by a quadratic number ring \( \mathcal{O} \) and ask whether we have unique factorization
as well and if not why? Some light onto the problem is put by an example.

Example: We take \( \mathcal{O}_{-5} \) which is equal to \( \mathbb{Z}[\sqrt{-5}] \) by Theorem 3.1 since \(-5 \equiv 3 \pmod{4} \).
Clearly \( 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \). The number 2 satisfies the first condition a) since \( 2 = ab \)
implies \( 4 = N(a)N(b) \). This gives \( N(a) = 1 \) or \( N(a) = 4 \) (since \( N(x + y\sqrt{-5}) = x^2 + 5y^2 = \)
\( 1, 4, 5, 9, 10, \ldots \)). In the first case \( a \) is a unit, in the second case we write \( a = x + y\sqrt{-5} \)
and then \( N(a) = x^2 + 5y^2 \). If \( x^2 + 5y^2 = N(a) = 4 \), then \( y = 0 \) and \( x = \pm 2 \) which shows that
\( b = \pm 1 \) is a unit and that 2 is a prime in the sense a). However
\[
6 = (1 + \sqrt{5})(1 - \sqrt{5}) \in (2).
\]

We next show that \( 1 + \sqrt{-5} \notin (2) \) and \( 1 - \sqrt{-5} \notin (2) \). Since \( 1 + \sqrt{-5} \in (2) \iff 1 - \sqrt{-5} \in (2) \) by
Galois conjugation we conclude that if \( 1 + \sqrt{-5} \in (2) \) then \( 1 + \sqrt{-5} = 2a \) for some \( a \in \mathcal{O}_{-5} \) and
then \( \alpha = \frac{1}{2} + \frac{1}{2}\sqrt{-5} \in \mathcal{O}_{-5} = \mathbb{Z} + \mathbb{Z}\sqrt{-5} \), a contradiction. Therefore \( (1 + \sqrt{-5})(1 - \sqrt{-5}) \in (2) \)
but \( 1 + \sqrt{-5} \notin (2) \) and \( 1 - \sqrt{-5} \notin (2) \).

As a conclusion we see that in \( \mathcal{O}_{-5} \) the definitions are not equivalent. Therefore they define
different notions.

Definition 4.1. Let \( \mathcal{O}_d \) be a quadratic number ring. An element \( 0 \neq a \in \mathcal{O}_d \) is called irreducible
if it is not a unit and if \( a = bc \) implies \( b \in U_d \) or \( c \in U_d \). It is called a prime if the ideal \( (a) \) is
a prime ideal, i.e. \( bc \in (a) \Rightarrow b \in (a) \text{ or } c \in (a) \).

As seen before, in \( \mathbb{Z} \) an element is irreducible if and only if it is prime. In the case \( \mathcal{O}_{-5} = \mathbb{Z}[\sqrt{-5}] \)
the element 2 is irreducible but not prime. Similarly 3 is irreducible (look as before at norms).

Now let \( \mathcal{O}_d \) be a quadratic number ring. Then prime elements are irreducible: suppose that \( a \)
is prime, and let \( a = bc \). Then \( b \) or \( c \in (a) \). Without loss of generality \( b \in (a) \Rightarrow b = ua \Rightarrow a =
uc \Rightarrow (1 - ac)a = 0 \Rightarrow uc = 1 \Rightarrow c \in U_d \).

We say that \( b \) divides \( a \) and write \( b | a \) if there exists \( c \in \mathcal{O}_d \) such that \( a = bc \).

Lemma 4.1. If \( \pi_1, \ldots, \pi_n \) are irreducible elements and \( \pi \) is irreducible and divides \( \pi_1 \cdots \pi_n \)
then there exists an index \( k \) and a unit \( \epsilon \) such that \( \pi_k = \epsilon \pi \).

Proof: Since \( \pi \) divides the product we deduce that \( \pi_1 \cdots \pi_n = \alpha \pi \) and this means that
\( \pi_1 \cdots \pi_n \in (\pi) \). Since \( \pi \) is irreducible it is prime and this implies that there exists an index \( k \)
such that \( \pi_k \in (\pi) \). In other words \( \pi_k = \alpha \pi \). This shows that \( \pi | \pi_k \). Since \( \pi_k \) is irreducible, \( \pi \)
not a unit it follows that \( \alpha \) is a unit and therefore \( \pi_k = \epsilon \pi \) for some unit \( \epsilon \in \mathcal{O}_K \) as stated. \( \square \)

In \( \mathcal{O}_d \) there are two ways to factorize:
• into irreducible elements  
• into prime elements

The next theorem shows that a factorization into irreducible elements is always possible.

**Theorem 4.1.** Let \( \mathcal{O} \) be a quadratic number ring. Then every \( 0 \neq a \in \mathcal{O} \) can be expressed as \( a = \varepsilon \pi_1 \cdots \pi_r \) with \( \varepsilon \) a unit and \( \pi_i \) irreducible.

**Proof:** We prove the assertion by induction on \( N = |N(a)| \). For \( N = 1 \) we have \( N(a) = \pm 1 \), hence \( a \) is a unit and there is nothing more to show in this case. Let now \( N > 1 \) and assume that the claim holds for all \( 0 \neq b \in \mathcal{O} \) with \( |N(b)| < N \). If \( a \) is irreducible, then we are done again (since \( a = a \) is a factorization as claimed in the statement). Otherwise we can factor \( a = bc \) with \( b, c \) not units and not associated to \( a \); hence \( 1 < |N(b)|, |N(c)| < N \). By the induction hypothesis we can factor \( b \) and \( c \) as wanted. But then the same is true for \( a \) since \( a = bc \). This proves the claim. \( \square \)

**Definition 4.2.** We call \( \mathcal{O}_d \) a unique factorization domain if every \( 0 \neq a \in \mathcal{O}_d \) can be written as \( a = \varepsilon \pi_1 \cdots \pi_r \) with a unit \( \varepsilon \) and with irreducible elements \( \pi_i \), and if this factorization is unique in the sense that if \( a = \varepsilon' \pi'_1 \cdots \pi'_s \) is a second factorization, then \( r = s \) and up to permutation \( \pi'_i = \varepsilon_i \pi_i \) with \( \varepsilon_i \) unit.

If we take prime elements instead of irreducible elements we get

**Definition 4.3.** \( \mathcal{O}_d \) is factorial if for all \( 0 \neq a \in \mathcal{O} \) there exist a unit \( \varepsilon \in U_d \) and primes \( \pi_1, \ldots, \pi_r \) in \( \mathcal{O}_d \) such that \( a = \varepsilon \pi_1 \cdots \pi_r \).

It is not difficult to show that if \( \mathcal{O}_d \) is factorial then the factorization is unique up to some unit. We see this by taking two factorizations

\[
\varepsilon \pi_1 \cdots \pi_r = \varepsilon' \pi'_1 \cdots \pi'_s
\]

as a product of prime elements and applying Lemma 4.1 recursively.

The last two definitions define a priori two different notions, but in fact they turn out to be the same as can be deduced from the subsequent discussion. We begin with a technical lemma which is used in the proof of our next theorem.

**Lemma 4.2.** Let \( p \) be a rational prime. Then \( p \) is reducible in \( \mathcal{O}_d \) if and only if there is an \( a \in \mathcal{O}_d \) with \( N(a) = \pm p \). In this case \( a \) is a prime element in \( \mathcal{O}_d \).

**Proof:** “\( \Rightarrow \)” If \( p \) is reducible, then \( p = ab \) with \( 1 < |N(a)|, |N(b)| < |N(p)| \). Taking norms we get \( p^2 = N(p) = N(a)N(b) \) and therefore \( N(a) = \pm p \), which is what we want.

“\( \Leftarrow \)” Assume that \( N(a) = \pm p \) for some \( a \in \mathcal{O}_d \). Then \( \pm aa\sigma = p \) with \( 1 < |N(a)| < |N(p)| \). This means that \( p \) is reducible. We prove the additional statement: Observe that \( p\mathcal{O}_d \subset a\mathcal{O}_d \subset \mathcal{O}_d \cong \mathbb{Z} \times \mathbb{Z} \omega \) and, by looking at norms, that these inclusions are strict. Thus \( \mathcal{O}_d/a\mathcal{O}_d \) is a proper subring of \( \mathcal{O}_d/p\mathcal{O}_d \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \). Hence \( \mathcal{O}_d/a\mathcal{O}_d \cong \mathbb{Z}/p\mathbb{Z} \) is a field. It follows that \( p\mathcal{O}_d = (p) \) is a prime ideal (even a maximal ideal), hence \( a \) is prime. \( \square \)

**Theorem 4.2.** Let \( \mathcal{O}_d \) be a quadratic number ring. Then \( \mathcal{O}_d \) is factorial if and only if every rational prime \( p \) remains prime in \( \mathcal{O}_d \) or is reducible.
Proof: By the last theorem the direction from left to right is easy since either the rational prime remains prime in \( \mathcal{O}_d \) and then there is nothing anymore to prove. Or, \( \mathcal{O}_d \) being factorial, it can be decomposed as a product of at least two prime elements and then \( p \) can be written as \( ab \) with \( a \) and \( b \) not a unit.. This shows that \( p \) becomes reducible in \( \mathcal{O}_d \). We just have to prove the converse. Let \( a \in \mathcal{O}_d \) be irreducible and let \( p \) be a (rational) prime dividing \( N(a) = aa^\sigma \). If \( p \) remains prime as an element of \( \mathcal{O}_d \), then \( p | aa^\sigma \) implies that \( p | a \) or \( p | a^\sigma \); in the second case it follows that \( p = p^\sigma | a^\sigma = a \). Hence \( p | a \) in both cases, which means (since \( a \) is irreducible) that \( a \) is associated to a prime and therefore is prime itself. If \( p \) is not prime, then by assumption it is reducible. Hence by Lemma 4.2 there is a prime \( b \in \mathcal{O}_d \) with \( N(b) = \pm p \). It follows that \( b | aa^\sigma \). Thus either \( b | a \) or \( b^\sigma | a \). In either case, as before, \( a \) is associated to a prime and hence prime itself. □

**Theorem 4.3.** Suppose that \( \mathcal{O}_d \) is a domain in which every element different from 0 and not a unit can be written up to a unit as a product of irreducible elements. Then the factorization is unique \( \iff \) irreducible elements are prime.

**Proof:** “\( \Rightarrow \)” Assume that irreducible elements are prime and let

\[ \varepsilon \pi_1 \cdots \pi_r = \varepsilon' \pi_1' \cdots \pi_s' \]

be two factorizations. Then \( \pi_1' \cdots \pi_s' \in (\pi_1) \). Since \( (\pi_1) \) is a prime ideal we deduce that up to numeration \( \pi_i' \in (\pi_1) \). This implies that \( \pi_i' = \varepsilon \pi_1 \) and since \( \pi_i' \) is irreducible and \( \pi_1 \) is not a unit we conclude that \( \varepsilon \) is a unit. Induction then shows that \( r = s \) and up to units that \( \pi_i = \pi_i' \) as stated.

“\( \Leftarrow \)” If the factorization is unique, \( \pi \) irreducible and \( ab \in (\pi) \) then \( ab = \alpha \pi \) for some \( \alpha \in \mathcal{O}_d \). Write \( a, b \) and \( r \) as a product of irreducible elements to see that by the unique factorization property \( \pi | a \) or \( \pi | b \) and this means that \( a \in (\pi) \) or \( b \in (\pi) \). □

**Corollary 4.1.** The ring \( \mathcal{O}_d \) is a unique factorisation domain of and only if it is factorial.

**Proof:** Since prime elements are irreducible factorial rings are unique factorisation domains. Conversely if the ring is a unique factorisation domain then by Theorem 4.3 irreducible elements are prime and then uniqueness of the factorization into irreducible elements implies unique factorization into prime elements. □

**Theorem 4.4.** A principal ideal domain \( \mathcal{O}_d \) is an unique factorization domain.

**Proof:** We first show that in \( \mathcal{O}_d \) every element can be written up to a unit as a finite product of irreducible elements. We let \( S \) be the set of principal ideals \( \{(a), 0 \neq a \in \mathcal{O}_d\} \) such that \( a \) does not have this property. We show that the set is empty. Otherwise let \( (a) \) be a maximal element. Such an element exists for otherwise for each \( (b) \in S \) there would exist a \( (c) \in S \) such that \( (b) \subseteq (c) \) and one would be able to construct a strictly increasing infinite sequence of ideals \( (a_1) \subseteq (a_2) \subseteq \cdots \subseteq (a_n) \subseteq \cdots \) with union an ideal in \( \mathcal{O}_d \). Since \( \mathcal{O}_d \) is a principal ideal domain we may express the union as \( (a) \) for some \( a \in \mathcal{O}_d \). The element \( a \) must be contained in \( (a_n) \) for some \( n \) which implies that \( (a_n) \subseteq (d) \subseteq (a_n) \). This means that \( (a_{n+k}) = (a_n) \) for all \( k \), a contradiction. Our \( a \) cannot be irreducible and therefore there exist non-units \( b \) and \( c \) in \( \mathcal{O}_d \) with \( a = bc \) and neither \( (b) \) nor \( (c) \) are in \( S \). therefore \( b \) and \( c \) can be written up to units as a finite product of irreducible elements. The same holds then for the product \( a = bc \) which means that \( (a) \not\subseteq S \), a contradiction, and \( S = \emptyset \).
To complete the proof we show that irreducible elements are prime. Let \( p \) be irreducible and suppose that \( bc \in (p) \). If \( b \notin (p) \) then \( (b, p) = \mathcal{O}_d \). This means that 1 = \( rb + sp \) with \( r, s \in \mathcal{O}_d \). Multiplication with \( c \) gives \( c = crb + csp \) and we conclude that \( c \in (p) \). Now we apply Theorem 4.3. \( \square \)

A very important question is now: For which \( d \) is the number ring \( \mathcal{O}_d \) a principal ideal domain? An answer is in general unknown. Special cases are euclidean rings: here an analogue of euclidean algorithm exists and this shows that such rings are principal and by Theorem 4.4 they are unique factorization domains.

To give an example we mention the ring \( \mathbb{Z}[i] \) which is euclidean and therefore also a unique factorization domain. We come to this back in Lecture 5.
5 Primes in Gaussian numbers rings  
(March 12, 2012)

In the introduction we have asked the question which integers can be written as a sum of two squares. The answer was given in Lecture 2. We also asked the question which primes can be written as a sum of two squares. As an example we mention that

\[
2 = 1 + 1, 5 = 1 + 4, 13 = 4 + 9, 17 = 1 + 16, 29 = 4 + 25, 37 = 1 + 36, 41 = 16 + 25
\]

In all these examples up to the first we deduce from \( p = a^2 + b^2 \) that \( p \equiv 1 \pmod{4} \). Squares are either \( \equiv 0 \pmod{4} \) or \( \equiv 1 \pmod{4} \). Since a prime \( p \neq 2 \) is \( \equiv 1 \pmod{2} \) and and if \( p \) is a sum \( p = a^2 + b^2 \) of squares we may assume without loss of generality that \( a^2 \equiv 0 \pmod{2} \) and \( b^2 \equiv 1 \pmod{2} \) and this implies that \( a^2 \equiv 0 \pmod{4} \) and \( b^2 \equiv 1 \pmod{4} \) and finally \( p \equiv 1 \pmod{4} \). The converse is also true.

**Theorem 5.1.** \( 2 \neq p \). Then

\[
p = a^2 + b^2 \iff p \equiv 1(4).
\]

The proof uses the Gaussian number ring which we have to introduce first. We consider the field \( \mathbb{Q}_- = \mathbb{Q}[i] = \{r + si; r, s \in \mathbb{Q}\} \). In this case \( d = -1 \equiv 3 \pmod{4} \) and therefore \( \mathcal{O}_- = \mathbb{Z} + \mathbb{Z} \omega \) which is \( \mathbb{Z}[i] \) since we can take \( \omega \) as \( i \). Furthermore \( U_- = \mu_4 \) and the norm is

\[
\begin{align*}
N_{\mathbb{Q}_-/\mathbb{Q}} : \mathbb{Q}_- & \to \mathbb{Q}, \\
\alpha = a + ib & \mapsto \alpha \bar{\alpha} = a^2 + b^2.
\end{align*}
\]

**Theorem 5.2.** The ring of integers \( \mathcal{O}_- \) in \( \mathbb{Q}_- \) is euclidean.

**Proof:** We define an euclidean algorithm, i.e. given \( \alpha, \beta \in \mathcal{O}_- \) with \( \beta \neq 0 \) we show that there exist \( \gamma, \rho \in \mathcal{O}_- \) such that \( \alpha = \gamma \beta + \rho \) and \( N(\rho) < N(\beta) \). Consider the lattice \( \mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}[i] \subseteq \mathbb{C} \) and write

\[
\frac{\alpha}{\beta} = \xi = [\xi] + \{\xi\}
\]

with \( [\xi] \in \mathcal{O}_- \) and \( \{\xi\} = a + bi \) chosen so that \(-1/2 \leq a < 1/2, -1/2 \leq b < 1/2\). Then

\[
N([\xi]) = a^2 + b^2 \leq \frac{1}{2}.
\]

Write \( \gamma = [\xi] \) and since \( \alpha, \beta, \gamma \in \mathcal{O}_- \) we see that \( \alpha = \gamma \beta + \rho \) and therefore \( \rho = \{\xi\} \cdot \beta \in \mathcal{O}_- \). Furthermore \( N(\rho) = N([\xi]) \cdot N(\beta) < N(\beta) \) and this shows the existence of the desired division with remainder term. \( \square \)

We are now ready to prove Theorem 5.1.

**Proof:** We begin with showing that every prime \( p \equiv 1 \pmod{4} \) is in the image under the norm function of prime elements in \( \mathcal{O}_- \). Our first step is to prove that if \( p \equiv 1 \pmod{4} \) then \( p \) is not a prime element in \( \mathbb{Z}[i] \). Since \( p = 1 + 4n \) and since by Wilson’s theorem we have \( (p - 1)! \equiv -1 \pmod{p} \) we get

\[
-1 \equiv (p - 1)! \equiv 1 \cdot 2 \cdots (2n)(p - 1)(p - 2) \cdots (p - 2n) \equiv (2n)!(-1)^{2n}(2n)! \equiv (2n)!^2
\]

This shows that \( x = (2n)! \) is a solution of \( x^2 \equiv -1 \pmod{p} \) and therefore

\[
(x + i)(x - i) = x^2 + 1 \in (p).
\]
If $p$ would be a prime in $\mathbb{Z}[i]$ then $x+i$ or $x-i$ would be in (p) and this would mean that $x+i = \alpha p$ with some $\alpha \in \mathbb{Z}[i]$ or that $x-i = \alpha p$. But then
\[
\alpha = \frac{x}{p} \pm \frac{i}{p} \notin \mathbb{Z}[i]
\]
in contradiction to the definition of $\alpha$. Therefore $p$ is not a prime element in the ring $\mathcal{O}_{-1}$ which, being euclidean, is a principal ideal domain. By Theorem 4.4 it is a unique factorization domain. Theorem 4.3 tells us that in this situation primes are irreducible and therefore which, being euclidean, is a principal ideal domain. By Theorem 4.4 it is a unique factorization domain. Theorem 4.3 tells us that in this situation primes are irreducible and therefor $p$ is not irreducible. It follows that $p = \alpha \beta$ for some elements $\alpha, \beta \notin \mathcal{O}_{-1}$. Taking norms gives $p^2 = N(\alpha)N(\beta)$ with $N(\alpha), N(\beta) > 1$, and this implies that $N(\alpha) = p = N(\beta)$. If we write $\alpha = a + ib$ with $a, b \in \mathbb{Z}$, then $p = N(\alpha) = a^2 + b^2$ as stated in Theorem 5.2. □

We determine now the prime elements in $\mathbb{Z}[i]$, i.e. the elements $\pi$ such that $(\pi)$ is a prime ideal. Note that this amounts to the same as to determine the irreducible elements because in our situation the irreducible elements are exactly the prime elements.

**Theorem 5.3.** The prime elements $\pi$ of $\mathbb{Z}[i]$ are given (up to units) by
1) $\pi = 1 + i$
2) $\pi = a + bi$ with $a^2 + b^2 \equiv p$, $p \equiv 1 \pmod{4}$ and $a > |b| > 0$
3) $\pi = p$ with $p \equiv 3 \pmod{4}$.

**Proof:** "$\Leftarrow$": The elements $\pi$ listed in 1) and 2) are prime elements since $\pi = \alpha \beta$ with $\alpha, \beta \in \mathbb{Z}[i]$ implies $p = N(\pi) = N(\alpha)N(\beta)$ and this gives $N(\alpha) = 1$ or $N(\beta) = 1$ and therefore $\alpha \in U_{-1}$ or $\beta \in U_{-1}$. This shows that $\pi$ is irreducible and therefore prime. If $\pi$ is as in 3) and $\pi = \alpha \beta$ then $p^2 = N(p) = N(\pi) = N(\alpha)N(\beta)$. If $\alpha, \beta \notin U_{-1}$ then $N(\alpha) = N(\beta) = p$ and we may express $\alpha$ as $\alpha = a + ib$ with $p = N(\alpha) = a^2 + b^2$ and this would imply that $p \equiv 1 \pmod{4}$ contrary to the assumption.

"$\Rightarrow$": We show that any $\pi$ prime is (up to unit) one of the prime elements in 1), 2) or 3). First write
\[
N(\pi) = \pi \cdot \overline{\pi} = p_1^{\epsilon_1} \cdots p_r^{\epsilon_r}
\]
with $p_1, \ldots, p_r$ distinct rational primes. Then $p_1 \cdots p_r \in (\pi)$ and $\pi$ being prime we find that $p \in (\pi)$ i.e. $p|\pi$ for some $p \in \{p_1, \ldots, p_r\}$. This gives $N(\pi) \in \{p, p^2\}$. If $N(\pi) = p$ we get $p = a^2 + b^2$ and therefore $\pi$ is of type 2), unless $p = 2$ and then of type 1). If $N(\pi) = p^2$ then $N(\pi/p) = p^2/p^2 = 1$ and from $p \in (\pi)$ we deduce that $\epsilon = p/p \in \mathcal{O}_{-1}$. This implies that $\pi/p \in U_{-1}$ which shows that $\pi = cp$ is a prime in $\mathcal{O}_{-1}$.

It remains to show that $p \equiv 3 \pmod{4}$. If not then $p = 2$ and then equal to $(1+i)(1-i)$ or $p \equiv 1 \pmod{4}$ and then by Theorem 5.1 of the form $p = a^2 + b^2 = (a + bi)(a - bi)$. But this would mean that $\pi$ would not be a prime element. □

We end this lecture with determining how a rational prime decomposes in $\mathbb{Z}[i]$.

**Theorem 5.4.** Rational primes $p \in \mathbb{Z}$ remain prime in $\mathbb{Z}[i]$ or decompose in $\mathbb{Z}[i]$ as $p = \pi \pi^\sigma$ with $\pi^\sigma$ conjugate to $\pi$ and $\pi, \pi^\sigma$ prime. Conversely every prime element $\pi$ in $\mathbb{Z}[i]$ divides a uniquely determined rational prime $p$.

**Proof:** Let $\pi \in \mathbb{Z}[i]$ be prime. Then
\[
\pi|N(\pi) = \pi \pi^\sigma \in \mathbb{Z}
\]
and therefore there exists a rational prime $p$ such that $\pi|p$. If $q$ is another prime with this property then $\pi|(p, q) = 1$ and this would mean that $\pi$ is a unit. This is not the case. Therefore $\pi$
is (up to unit) unique.
Assume now that \( p \) is not prime in \( \mathbb{Z}[i] \). Then \( p = \pi \pi^* \) for \( \pi, \pi^* \in \mathbb{Z}[i] \) and not a unit. We deduce that \( p^2 = N(\pi)N(\pi^*) \) and then \( N(\pi) = p = N(\pi^*) \). This gives a decomposition \( p = \pi \pi^\sigma \) with \( \pi \) a prime as stated. □

**Definition 5.1.** A rational prime \( p \) is called inert if \( p \) remains prime in \( \mathbb{Z}[i] \), it is called split if \( p = \pi \pi^\sigma \) and \( \pi^\sigma \) is not \( \varepsilon \pi \) for some unit \( \varepsilon \) and it is ramified iff it is up to a unit of the form \( \pi^2 \) for some prime element \( \pi \) in \( \mathbb{Z}[i] \).

The latter is the case iff \( p = 2 \) since then \( 2 = (1 + i)(1 - i) \), \( 1 \pm i \) prime and \( 1 - i = -i(1 + i) \) and then \( 2 = -i(1 + i)^2 \) is up to unit a square. We conclude that 2 is ramified. The discriminant \( d_K \) of \( \mathbb{Q}[i] \) is \(-4\) and therefore 2, a divisor of the discriminant \( d_{\mathbb{Q}[i]} \), is the only prime which divides the discriminant. It can be shown that the prime number \( p \) is ramified in \( K = \mathbb{Q}(\sqrt{d}) \) if and only if \( p | d_K \) with \( d_K = d \) in the case that \( d \equiv 1 \mod 4 \) and with \( d_K = 4d \) if \( d \equiv 2, 3 \mod 4 \). We formulate this in

**Theorem 5.5.** In \( \mathbb{Z}[i] \) the prime number \( p \) is inert \( \iff \) \( p \equiv 3 \pmod{4} \), it is split \( \iff \) \( p \equiv 1 \pmod{4} \) and \( p \) is ramified \( \iff \) \( p = 2 \).

There are many very interesting questions which come up in this context. By Theorem 5.5 ramified primes divide the discriminant. Therefore their number is finite. For example one may ask what about inert and split primes? (The answer is that they have density \( 1/2 \) (see [8], p. 346, Cor.4 and Cor. 5).)
6 Ideals in quadratic number rings  
(March 19, 2012)

In the last lecture we have studied in an example, the ring of Gaussian integers, the question how in a principal ideal the factorization theory from \( \mathbb{Z} \) extends to the number ring. This is a very particular situation since in general this is not possible anymore. Instead one has to follow a new concept in which irreducible elements are replaced by ideals and factorization will be in terms of ideals. Quadratic number rings are the easiest case of a very general theory which ends in abstract commutative algebra or algebraic geometry. Since we are very much interested in number theoretical properties our approach is slightly extended towards particular number theoretical concepts.

One of the main objects concerning ideals will be the class group of the quadratic number field. As a first step towards this goal we introduce the set \( \mathcal{M}_d \) of ideals in \( \mathcal{O}_d \). We begin with recalling, so to say as a warming up, the definition of an ideal. We take a quadratic number field \( \mathbb{Q}(\sqrt{d}) \) with ring of integers \( \mathcal{O}_d \) which we may write as \( \mathbb{Z} + \mathbb{Z}\omega \). Given \( \mathbb{Q}(\sqrt{d}) \) its ring of integers \( \mathcal{O}_d = \mathbb{Z} + \mathbb{Z}\omega \) is a free \( \mathbb{Z} \)-module.

**Definition 6.1.** A subset \( a \subset \mathcal{O}_d \) is an ideal if and only if the following properties are satisfied:
- \( a \) is an additive subgroup
- \( \lambda a \subseteq a \) for all \( \lambda \in \mathcal{O}_d \).

The set of ideals is an additive as well as a multiplicative monoid with neutral element. To see this we have to define the addition and the multiplication of two ideals \( a \) and \( b \) in \( \mathcal{M}_d \).

**Definition 6.2 (Sum and Product of Ideals).** The sum and product of two ideals \( a, b \subseteq \mathcal{O}_d \) are defined as

\[
a + b := \{a + b; \ a \in a, b \in b\}
\]

and

\[
a \cdot b := \left\{ \sum_{i=1}^{r} a_i b_i; \ a_i \in a, b_i \in b; r \in \mathbb{N} \right\}.
\]

One sees easily that the product of two ideals is an ideal.

Let \( 0 \neq a \subseteq \mathcal{O}_d \) be an ideal. Then \( [\mathcal{O}_d : a] < \infty \). To see this we take \( 0 \neq a \in a \cap \mathbb{Z} \) and then \( (a) := a\mathcal{O}_d \subseteq a \subseteq \mathcal{O}_d \) implies that \( [\mathcal{O}_d : a] \leq [\mathcal{O}_d : (a)] \). Since \( (a) = Za + Z\omega \) and since \( (\mathbb{Z} + \mathbb{Z}\omega)/(Za + Z\omega) \simeq (\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/a\mathbb{Z}) \) we have \( [\mathcal{O}_d : a\mathcal{O}_d] = a^2 < \infty \).

For an ideal \( a = Z\alpha + Z\beta \subseteq \mathcal{O}_d \) we introduce the norm of \( a \) as \( N(a) := [\mathcal{O}_d : a] \) and the discriminant as

\[
D(a) := \det \begin{pmatrix} \alpha & \beta \\ \alpha^\sigma & \beta^\sigma \end{pmatrix}^2.
\]

A transformation \( \alpha = a + b\omega, \beta = c + d\omega \) of the basis leads to

\[
\begin{pmatrix} \alpha & \alpha^\sigma \\ \beta & \beta^\sigma \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ \omega & \omega^\sigma \end{pmatrix}
\]
and gives \( D(a) = (\det T)^2 D(\mathcal{O}_d) \) and \( \det T = N(a) \) for
\[
T = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.
\]

We deduce that \( D(a) = N(a)^2 D(\mathcal{O}_d) \). In the special case of a principal ideal \( a = (\xi) = \xi \mathcal{O}_d \) we get
\[
D((\xi)) = \det \begin{pmatrix} \xi & \xi \omega \\ \xi \sigma \omega & \xi \sigma \end{pmatrix}^2 = (\xi \xi^\sigma)^2 \det \begin{pmatrix} 1 & \omega \\ 1 & \omega^\sigma \end{pmatrix}^2 = N(\xi)^2 D(\mathcal{O}_d)
\]
and this implies that \( N((\xi))^2 = N(\xi)^2 \). We conclude that the ideal norm of the ideal generated by \( \xi \) and the norm of \( \xi \) are related by \( N((\xi)) = |N(\xi)| \). The norm for ideals is multiplicative, i.e. \( N(ab) = N(a)N(b) \).

We deduce from this property the very useful proposition which allows us to define the inverse of an ideal.

**Proposition 6.1.** If \( a \subseteq \mathcal{O}_d \) is an ideal then
\[
a \cdot a^\sigma = (N(a)) = N(a)\mathcal{O}_d.
\]

**Proof:** We write \( a = Z\alpha + Z\beta \) and get \( a^\sigma = Z\alpha^\sigma + Z\beta^\sigma \) This gives
\[
a a^\sigma =ZN(\alpha) + ZN(\beta) + Z\alpha^\sigma + Z\alpha^\sigma \beta.
\]

Let \( m = (N(\alpha), N(\beta), Tr(\alpha\beta^\sigma)) > 0 \) be the greatest common divisor of the integers \( N(\alpha), N(\beta), Tr(\alpha\beta^\sigma) \) and introduce \( \gamma = \alpha\beta^\sigma/m \). Then
\[
Tr(\gamma) = \gamma + \gamma^\sigma = \frac{Tr(\alpha\beta^\sigma)}{m} \in \mathbb{Z},
\]
\[
N(\gamma) = \gamma \gamma^\sigma = \frac{N(\alpha) N(\beta)}{m} \in \mathbb{Z}
\]
and this implies that \( \gamma \) is integral. By definition there exist \( r, s, t \in \mathbb{Z} \) such that
\[
m = rN(\alpha) + sN(\beta) + tTr(\alpha\beta^\sigma)
\]
and we conclude that
\[
1 = \frac{N(\alpha)}{m} + \frac{sN(\beta)}{m} + \frac{tTr(\alpha\beta^\sigma)}{m}.
\]

This leads to \( 1 \in Z\frac{N(\alpha)}{m} + Z\frac{N(\beta)}{m} + Z\frac{Tr(\alpha\beta^\sigma)}{m} \) whence
\[
a a^\sigma = m \left( Z\frac{N(\alpha)}{m} + Z\frac{N(\beta)}{m} + Z\frac{Tr(\alpha\beta^\sigma)}{m} \right) = m\mathbb{Z}.
\]

Taking norms gives \( m^2 = N(m) = N(m\mathcal{O}_d) = N(aa^\sigma) = N(a)N(a^\sigma) = N(a)^2 \), which implies that \( m = N(a) \). \( \square \)

From the Proposition it easily follows that the norm is a homomorphism from the monoid of ideals into \( \mathbb{N} \).

**Corollary 6.1.** The norm satisfies \( N(ab) = N(a)N(b) \).
Proof: We apply the proposition to $ab$ and get

$$(\mathcal{N}(a)\mathcal{O}_d)(\mathcal{N}(b)\mathcal{O}_d) = aa^\sigma bb^\sigma = (aa^\sigma)(bb^\sigma) = (\mathcal{N}(a)\mathcal{N}(b))\mathcal{O}_d$$

and the claim follows. □

In the next proposition we shall determine the structure of an ideal in a quadratic number ring. We do it in a slightly more general situation by looking at arbitrary $\mathbb{Z}$-modules, not only at ideals which are $\mathcal{O}_d$-modules.

**Proposition 6.2.** Let $a \subseteq \mathcal{O}_d$ be a $\mathbb{Z}$-module different from $(0)$. Then the following properties are satisfied:

(i) there exist integers $a, m, n \in \mathbb{N}$ such that

$$a = (n, a + m\omega)$$

and $0 \leq a < n$ if the rank of $a$ is two,

(ii) if $a$ is an ideal $\neq 0$ then $m|n, m|a$ and

$$a = (m)(n/m, a/m + \omega),$$

(iii) the integer $n$ divides $m\mathcal{N}(a/m + \omega)$.

**Proof:** The set $H = \{s \in \mathbb{Z}; \exists r \in \mathbb{Z} : r + s\omega \in a\}$ is easily seen to be a subgroup of $\mathbb{Z}$ and therefore there exists an integer $m \geq 0$ such that $H = m\mathbb{Z}$. By the definition of $m$ there exists an integer $a \in \mathbb{Z}$ such that $a + m\omega \in a$. The intersection $a \cap \mathbb{Z}$ is a subgroup of $\mathbb{Z}$ and can be written as $a \cap \mathbb{Z} = n\mathbb{Z}$ for some integer $n \geq 0$. To prove (i) it is sufficient to show that $a \subseteq (n, a + m\omega)$. If $r + s\omega \in a$ then by the definition of $H$ we have $s \in H = m\mathbb{Z}$ so that $s = mu$ for some $u \in \mathbb{Z}$. This means that

$$r - ua = r + s\omega - (s\omega + ua) = r + s\omega - u(a + m\omega) \in a$$

and since also $r - ua \in \mathbb{Z}$, that is in $a \cap \mathbb{Z} = n\mathbb{Z}$, we conclude that

$$r + s\omega = r - ua + u(a + m\omega) \in n\mathbb{Z} + (a + m\omega)\mathbb{Z},$$

which proves the first part of (i). If the rank of $a$ is two then $n \neq 0$ and division of $a$ by $n$ with remainder gives the second part.

To prove (ii) we assume in addition that $a$ is an ideal which is a module of rank two and by (i) contains $n$. Then $\omega a \subseteq a$ and therefore $n\omega \in \omega a \subseteq a$ which, again by the definition of $H$, implies that $n \in H = m\mathbb{Z}$. This means that $m|n$ and this is the first part of the assertion in (ii). For the second part we show that $m|a$ which will follow if we prove that $a \in H$ since then $a \in m\mathbb{Z}$.

We express $\omega^2$ as $k + l\omega$ and then

$$mk + (a + ml)\omega = a\omega + m(k + l\omega) = a\omega + m\omega^2 = \omega(a + m\omega) \in a$$

and we deduce from the definition of $H$ that $a + ml \in H$. This implies that $a \in H$ as stated. It follows that

$$a = (n, a + m\omega) = (m)(n/m, a/m + \omega)$$

and the second assertion of (ii) is established.

For (iii) we put $\alpha = a + m\omega$ which is in $a$ and then, by (i), we have $\alpha^\sigma/m = (a/m) + \omega^\sigma \in \mathcal{O}_d$. This shows that $N(a/m) \in \mathbb{Z}$. Together with

$$mN(\alpha/m) = \alpha(\alpha^\sigma/m) \in \alpha\mathcal{O}_d \subseteq a$$
we conclude that \(mN(\alpha/m) \in \mathfrak{a} \cap \mathbb{Z} = n\mathbb{Z}\) and this gives \(n|mN(a/m + \omega)\). □

From (i) one sees that if \(0 \neq a \subseteq \mathcal{O}_d\) is an ideal it can be generated by at most two elements.

Let \(a \neq 0\) be an ideal. By Proposition 6.2 we have \(a = (n, m\alpha)\) with \(\alpha = m^{-1}(a + m\omega) = b + \omega\).

**Proposition 6.3.** The norm of the ideal \(a = (n, a + m\omega)\) is \(N(a) = mn\).

**Proof:** We first show that \(mn|N = N(a)\). We have \(a^\sigma = (n, m\alpha^\sigma)\) and therefore

\[
\begin{align*}
aa^\sigma &= (n^2, nma, nma^\sigma, m^2N(\alpha)) = (nm)(\frac{n^2}{nm}, \alpha, \alpha^\sigma, \frac{m}{n}N(\alpha)) = (nm)b.
\end{align*}
\]

for some ideal \(b\). Proposition 6.2 shows that \(b\) is an ideal in \(\mathcal{O}_d\) and therefore \((N) = (N(a)) = \aa^\sigma \subseteq (nm)\) which gives the first assertion. Secondly we show that \(N|nm\) and this then gives the desired statement. Since \(ma \in \mathfrak{a}\) and \(n \in \mathfrak{a}^\sigma\) we have \(nma \in \aa^\sigma = (N)\) and therefore

\[
\begin{align*}
\frac{nm}{N}(b + \omega) &= \frac{nm}{N}\alpha \in \mathcal{O}_d.
\end{align*}
\]

This gives \(\frac{nm}{N}(b + \omega) = u + v\omega, u, v \in \mathbb{Z}\), and \(v = nm/N \in \mathbb{Z}\). It follows that \(N|nm\). □

**Corollary 6.2.** The norm of a prime ideal \(p\) is \(p\) or \(p^2\) for some rational prime in \(p\) and a prime ideal \(p\) contains a rational prime element \(p\).

**Proof:** Let \(p\) be a prime ideal. Then by Proposition 6.2 it takes the form \(p = (m)(u, v + \omega)\) for some integers \(u, v \geq 0\). By Proposition 6.3 its norm is \(N(p) = um\). Since \(p\) is prime either \((m) = (1)\) or \((u, v + \omega) = (1)\) and this implies that \(p = (m)\) or \(p = (u, v + \omega)\) respectively. From \(N(p) \in pp^\sigma \subseteq p\) we see that if \(p = (u)\) and \(u = ab\) for integers \(a, b\) then, \(p\) being prime, we may assume that \(a \in p = (u)\). This gives \(u|a\) and together with \(a|u\) leads to \(u = \pm a\). Therefore \(u\) is a rational prime \(p\) contained in \(p\) and shows that \(p = (p)\).

If \(p = (u, v + \omega)\) then Proposition 6.3 shows that \(N(p) = u\) and if \(u = ab\) then as above we get \(a \in p\) and this shows that \(a = ku + l(v + \omega)\) for integers \(k\) and \(l\). Since \(a \in \mathbb{Z}\) we conclude that \(l = 0\) and that \(u|a\). This together with \(a|u\) shows that \(u = \pm a\) and therefore that \(u\) is some rational prime \(p\) and that \(p = (p, v + \omega)\). This proves the second part of the corollary. The first part then follows from Proposition 6.3. □

We are now able to give the general shape of a prime ideal in \(\mathcal{O}_d\).

**Proposition 6.4.** Let \(p\) be a prime ideal. Then there is a rational prime such that \(p = (p)\) or \(p = (p, \epsilon + \omega)\) with \(\epsilon = 0\) or \(\epsilon = \pm 1\).

**Proof:** From Corollary 6.2 together with Proposition 6.2 and Proposition 6.3 we deduce that \(p = (p, v + \omega)\) with \(0 \leq v < p\). If \(v = 0\) we get \(\epsilon = 0\) otherwise \((v, p) = 1\) and then \(1 = kp + lv\) and so \(p = (p, 1 + l\omega)\) with \(l \in \mathbb{Z}\). But \(l|1\) by Proposition 6.2 and this gives the assertion. □
We recall that an ideal \( 0 \neq p \subset \mathcal{O}_d \) is a prime ideal if and only if \( ab \in p \) implies \( a \in p \) or \( b \in p \). It is easy to see that equivalently an ideal \( p \) is prime if and only if \( \mathcal{O}_d \) is entire.

**Lemma 7.1.** An ideal \( p \) is prime if and only if \( p \supseteq ab \) for some ideals \( a \) and \( b \) implies that \( p \supseteq a \) or \( p \supseteq b \).

**Proof:** "\( \Leftarrow \)" If \( ab \subseteq p \) and \( a \not\subseteq p \) and \( b \not\subseteq p \) we choose \( \alpha \in a \) and \( \beta \in b \) but not in \( p \). Then \( \alpha \beta \in p \) but none of \( \alpha \) and \( \beta \). This means that \( p \) is not prime.

"\( \Rightarrow \)" Suppose that \( \alpha \beta \in p \). Then \( (\alpha)(\beta) \subseteq p \) and this implies that \( (\alpha) \subseteq p \) or \( (\beta) \subseteq p \) on assuming that \( p \) is prime. □

We come back to \( \mathcal{O}_{-5} = \mathbb{Z} + \mathbb{Z}\sqrt{-5} \). There we have seen that
\[
6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})
\]
and we have seen that 2 is irreducible but not prime and 3 has the same property. If however we allow prime ideals as factors then factorization has a chance. Write
\[
(2) = p_1p_2, \quad (3) = p_3p_4, \quad (1 + \sqrt{-5}) = p_1p_3, \quad (1 - \sqrt{-5}) = p_2p_4.
\]
Then
\[
(6) = (2)(3) = p_1p_2p_3p_4
\]
and everything would work. There cannot be more then 2 factors in (2) or (3) by norm considerations. This implies
\[
N(p_1) = N(p_2) = 2, \quad N(p_3) = N(p_4) = 3.
\]
The prime ideals in that decomposition can be explicitly determined using the results of the last section. From there it follows that \( p_1 = (2, 1 + \sqrt{-5}), p_2 = (2, 1 - \sqrt{-5}), p_3 = (3, 1 + \sqrt{-5}), p_4 = (3, 1 - \sqrt{-5}) \).

We show this for the ideal \( p = p_1 \). By Proposition 6.2 we have \( p = (n, a + mw) \) and from Proposition 6.3 we deduce that \( 2 = N(p) = nm \). This gives \( n = 2 \) and \( m = 1 \) for \( n = 1 \) can be excluded. By Proposition 6.2 the integer \( a \) can take only the values 0 or 1. The value 0 is not possible for otherwise \( \sqrt{-5} \) would be in \( p \) and then \( 5|2 = N(p) \). This shows that the ideal \( p \) has the form given above.

**Definition 7.1.** An ideal \( m \) is called maximal if \( m \subseteq a \subseteq \mathcal{O}_d \) for an ideal \( a \) implies that \( a = m \) or \( a = \mathcal{O}_d \).

**Remark 7.1.** It is easy to see that an ideal \( p \) is maximal if and only if \( \mathcal{O}_d \) is a field.

The goal of this lecture is to show that in \( \mathcal{O}_d \) we have unique factorization of an ideal \( a \) as a product of prime ideals
\[
a = p_1 \cdots p_r, \quad p_i \text{ prime}.
\]
From the remark we deduce that every maximal ideal is prime. To see this directly we take \( m \subset \mathcal{O}_d \) maximal and choose \( r \in \mathcal{O}_d \) such that \( r \not\in m \). Then \( (m, r) \supseteq m \) is an ideal different from \( m \) and therefore \( (m, r) = \mathcal{O}_d \supsetneq 1 \). We write \( 1 = m + rs, r \in \mathcal{O}_d, m \in m \) and deduce that \( 1 \equiv rs \pmod{m} \). This shows that \( r \) is invertible modulo \( m \) and therefore that \( \mathcal{O}_d/m \) is a field. We conclude that \( m \) is prime. The converse is also true and we get
Theorem 7.1. The ideal $0 \neq p \subset O_d$ is prime if and only if $p$ is maximal.

Proof: Let $pZ = p \cap Z$ and $(p) = pO_d$. Then $(p) \subseteq p \subset O_d$ and we show that $O_d/p$ is a field. To show this we take $\overline{\alpha} \in O_d/p$ and choose some $\alpha \in \pi$. It satisfies a quadratic relation $\alpha^2 + a\alpha + b = 0$ with $a, b, \in Z$. Taking residues gives

$$\overline{\alpha^2} + \overline{a\alpha} + \overline{b} = 0$$

(1)

where $\overline{\alpha}, \overline{b} \in Z/pZ$. If $\overline{b} \neq 0$ then it is is invertible and we find some $\overline{c} \in Z/pZ$ such that $\overline{bc} = 1$. The relation (1) multiplied by $\overline{c}$ leads to

$$1 = (-\overline{\alpha\overline{c}} - \overline{a\overline{c}})\overline{\alpha}$$

and this shows that $\overline{\alpha}$ has an inverse. If $\overline{b} = 0$ then from (1) we deduce that either $\overline{\alpha} = 0$ or $\overline{\alpha} = -\overline{\alpha}$. In the latter case $0 \neq \overline{\alpha} \in Z/pZ$ and since $Z/pZ$ is a field it follows that $\overline{\alpha}$ has an inverse as well. This shows that $O_d/p$ is a field and therefore that $p$ is maximal. \(\square\)

We next introduce irreducible ideals. Let $a, b \subseteq O_d$ be ideals. Then we say that $a|b$ if there exists an ideal $c \subset O_d$ such that $b = a \cdot c$. Then $b = ac \subseteq a$. Also the converse is true. If $b \subseteq a$ then multiplication by $a^\sigma$ and applying Proposition 6.1 shows that

$$a^\sigma b \subseteq a^\sigma a = (N(a)) = (N)$$

and $c := N^{-1}a^\sigma b \subseteq O_d$. We get $ac = N^{-1}aa^\sigma b = b$ and finally that $a|b$. From Lemma 7.1 it follows at once that $p \neq 0$ is prime if $a|bc \Rightarrow a|b$ or $a|c$

The next definition takes up the discussion at the beginning of section 7.

Definition 7.2. An ideal $a \neq O_d$ is called irreducible if $a = bc$ implies $b = O_d$ or $c = O_d$.

Proposition 7.1. An ideal in $O_d$ is irreducible if and only if it is maximal.

Proof: To see that $a$ be irreducible and suppose that $b \supseteq a$ is an ideal. Then $b|a$ and irreducibility implies $b = O_d$ or $b = a$. For the converse let $m$ be maximal and assume that $m = bc$. We have to show that $b = O_d$ or $c = O_d$. We have $m = bc \subseteq b$ and if $b \neq O_d$ we find that $m = b$ by maximality of $m$ and this gives $m = mc$. We want to conclude that $c = O_d$. This follows from the subsequent Lemma. \(\square\)

Lemma 7.2. Let $a, b$ and $c$ be ideals in $O_d$ all different from $(0)$. Then $ab = ac$ implies $b = c$.

Proof: This holds for principle ideals $a = (\alpha)$ because $\alpha b = ab = ac = \alpha c$. Let $\beta$ be in $b$. Then $\alpha \beta \in \alpha c$ and there exists $\gamma \in c$ such that $\alpha \beta = \alpha \gamma$. This shows that $\beta = \gamma \in c$. We conclude that $b \subseteq c$ and by symmetry also that $c \subseteq b$.

If $a$ is arbitrary we multiply by $a^\sigma$ and get

$$(N(a))b = a^\sigma ab = a^\sigma ac = (N(a))b.$$  

Since $(N(a))$ is principal we conclude that $b = c$. \(\square\)

We deduce that the set of ideals of $O_d$ is a monoid. Furthermore we have shown that

$$a \text{ irreducible } \iff a \text{ maximal } \iff a \text{ prime.}$$

We are now ready to prove the following:
Theorem 7.2. \((0) \neq a \subset \mathcal{O}_d\) ideal. Then up to permutation of the factors we can write

\[ a = p_1 \cdots p_s \]

with \(p_i\) prime and unique.

Proof: Let \(S\) be the set of ideals which do not have the property. If \(S \neq \emptyset\) then there exists a maximal element \(c\) in \(S\) which by the definition of \(S\) has to be reducible. Therefore we can write \(m = ab\) with \(a \supset c, b \supset c\) and \(a, b \notin S\). But then \(c\) is the product of the prime factors of \(a\) and \(b\) and cannot be in \(S\). It follows that \(S = \emptyset\). Uniqueness follows from Lemma 7.2. \(\square\)
8 Prime ideals
(March 26, 2012)

Let \( p \subset O \) be a prime ideal. Then there exists a rational prime \( p \) such that \( p|(p) = pO \). In fact we have \( p|(N(p)) = pp\sigma \) (since \( p \supset pp\sigma = (N(p)) \)). We now factorize \( N(p) = p_1 \cdots p_s \) in \( \mathbb{Z} \) and deduce that \( p|(p_1 \cdots (p_s) \) It follows that there exists an \( i \) such that \( p|(p_i) \) and this proves our claim. As a consequence we have \( N(p)|N((p)) = p^2 \) and therefore \( N(p) \in \{ p, p^2 \} \).

Lemma 8.1. Prime ideals in \( O_d \) take the form \( (p) \) or \( (p,v+\omega) \) with \( p \) a rational prime and \( 0 \leq v \leq p-1 \).

Proof: By Proposition 6.2 we may write \( p \) as

\[
p = (n,a+m\omega) = (m)\left(\frac{n}{m},a/m+\omega\right)
\]

and \( n|mN(a/m+\omega) \). We want to determine \( m, n \) and \( a \). First note that since \( p \) is prime we must have either \( m = 1 \) and then \( p = (u,v+\omega) \) or \( (n/m,a/m+\omega) = (1) \) and \( (m) = p \). The latter gives \( m = p \) and \( p = (p) \). If \( p = (u,v+\omega) \), as in the first case, we deduce that \( u = N(p) \in \{ p, p^2 \} \).

If \( u = p^2 \) then \( p^2 = u \in p \) and since \( p \) is prime we find that \( p \in p \) and therefore \( p = (p,v+\omega) \). □

Theorem 8.1. Let \( d_K \) be the discriminant of \( \mathbb{Q}_d \) and \( p \neq 2 \) a prime. Then

\[
(p) = \begin{cases} 
p & \text{if } \left(\frac{d}{p}\right) = -1 \\
p\sigma & \text{if } p \neq p\sigma \text{ and } \left(\frac{d}{p}\right) = 1 \\
p^2 & \text{if } p|d_K
\end{cases}
\]

(2)

Proof: \( p \neq 2 \) and \( p|d_K \) implies \( p|d \). Now

\[
(p,\sqrt{d})^2 = (p^2,p\sqrt{d},d) = (p)(p,\sqrt{d},\frac{d}{p}) = (p)
\]

since \( d \) is square-free and therefore \( 1 = kp + ld/p \in (p,\sqrt{d},d/p) \) whence \( (p,\sqrt{d},d/p) = O_d \).

Assume now that \( \left(\frac{d}{p}\right) = 1 \). Then either \( \left(\frac{4d}{p}\right) = \left(\frac{d}{p}\right) = 1 \) or \( \left(\frac{4d}{p}\right) = \left(\frac{d}{p}\right)^2 = 1 \) and therefore there exists an integer \( x \) with \( x^2 \equiv d_K \mod p \). We put \( p = (p, x + \sqrt{d}) \). Then

\[
pp\sigma = (p^2, p(x + \sqrt{d}), p(x - \sqrt{d}), (x^2 - d)) = (p)(p, x + \sqrt{d}, p - \sqrt{d}, (x^2 - d)/p) = (p)(p, x + \sqrt{d}, 2\sqrt{d}, (x^2 - d)/p) = (p)b.
\]

Now \( 2\sqrt{d} \in b \) implies \( (2\sqrt{d})^2 = 4d \in b \) therefore \( 1 = (p, 4d) \subset b \) and this gives \( pp\sigma = (p) \).

Assume next that \( (d/p) = -1 \). Lemma 8.1 shows that \( p = (p) \) or \( p = (p,v+\omega) \). In the latter case we have \( N(v+\omega) = (v+\omega)(v+\omega^\sigma) \in pp\sigma = (p) \). This implies that \( p|N(v+\omega) = v^2 + Tr(\omega)v + N(\omega) \). Now \( \omega = \sqrt{d} \) and then \( Tr(v+\omega) = 0 \) or \( 1 + \sqrt{d}/2 \) and then \( Tr(v+\omega) = 1 \). This gives \( v^2 \equiv d \mod (p) \) which is equivalent to \( (d/p) = 1 \) or \( N(\omega) = (d - 1)/4 \) and \( Tr(\omega) = 1 \). In the latter case \( v^2 + v - (d - 1)/4 \equiv 0 \mod p \) and this implies \( (2v + 1)^2 = 4v^2 + 4v + 1 \equiv d \mod p \) and again \( (d/p) = 1 \). In both cases we get a contradiction. This shows that \( p = (p) \). □
We make now a short deviation into Galois theory. First note that in the case \( K = \mathbb{Q}(\sqrt{d}) \) we have \( G = \text{Gal}(K/\mathbb{Q}) = \langle \sigma \rangle, \sigma \neq \text{id}, \sigma^2 = \text{id} \) with \( \sigma \alpha = \alpha^\sigma \). We define now the decomposition group and the inertia group. Let \( p \) be a prime ideal. Then

\[ D_p = \{ \tau \in G; p^\tau = p \} \]

is the decomposition group. Let \( k(p) = \mathcal{O}/p \) be the residue field of \( p \). It is an extension of \( \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \) of degree 1 or 2 and we get a homomorphism \( \pi: D_p \to \text{Gal}(k(p)/\mathbb{F}_p) \).

**Lemma 8.2.** \( \pi \) is surjective.

**Proof.** If \( k(p) = \mathbb{F}_p \) there is nothing to show. Otherwise we have \( k(p) = \mathbb{F}_p(\theta) \) where \( \theta = \theta + p \). Let \( \overline{\theta} \in \text{Gal}(k(p)/\mathbb{F}_p) \) and let \( F(T) \in \mathbb{Z}[T] \) be the minimal polynomial of \( \theta \) over \( \mathbb{Z} \). Let also \( G(T) \in \mathbb{Z}[T] \) be a polynomial such that \( G(\overline{T}) \) is the minimal polynomial of \( \overline{\theta} \). We may choose \( G \) of degree \( \leq 2 \). Then \( G|F \) and if \( F(T) = (T - \theta)(T - \theta^\sigma) \) with \( \theta, \theta^\sigma \in \mathcal{O} \) we have \( G(T) = (T - \theta^\sigma)(T - \theta^\sigma) \). Then \( \overline{\pi(\theta)} = \overline{\xi} \) for some \( \xi \in \{ \theta, \theta^\sigma \} \) and we define \( \pi(\theta) = \xi \). Then \( \overline{\pi} = \pi(\tau) \).

From the lemma we get an exact sequence

\[ 1 \to I_p \to D_p \to \text{Gal}(k(p)/\mathbb{F}_p) \to 1 \]

with \( I_p = \ker \pi \) the inertia group.

**Theorem 8.2.** The following properties of a prime ideal \( p \) are equivalent

(i) \( p \) is unramified,
(ii) \( p \nmid d_K \),
(iii) \( I_p = \langle 1 \rangle \).

**Proof.** The equivalence of (i) and (ii) has already been shown. We show now that (i) and (iii) are equivalent. If \( p \) is unramified then \( (p) = pp^\sigma \) with \( p \neq p^\sigma \) or \( (p) = p \). Consider first the case \( (p) = pp^\sigma \): Then \( D_p \neq G \) and this implies that \( D_p = \langle 1 \rangle \) and therefore \( I_p \subseteq D_p = \langle 1 \rangle \). Now consider the case \( (p) = p \): Then \( D_p = G \) and \( [k(p) : \mathbb{F}_p] = 2 \). Therefore \( \text{Gal}(k(p)/\mathbb{F}_p) \neq \langle 1 \rangle \) and this implies \( I_p \nsubseteq D_p = G \). But then \( I_p = \langle 1 \rangle \).

We illustrate this in the following table:

<table>
<thead>
<tr>
<th>( D_p )</th>
<th>( p = (p) )</th>
<th>( pp^\sigma = (p) )</th>
<th>( p^2 = (p) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( I_p )</td>
<td>( \langle 1 \rangle )</td>
<td>( \langle 1 \rangle )</td>
<td>( G )</td>
</tr>
</tbody>
</table>
9 Fractional ideals
(April 2, 2012)

In this lecture we shall study the set of ideals in \( \mathcal{O}_d \). We have seen that it is a multiplicative unitary monoid. The main aspect will be to make out of it a commutative group and to introduce the associated class group. We shall prove that the class group is finite and introduce the two aspects of its order, the class number.

**Definition 9.1.** A fractional ideal of \( K \) is a finitely generated \( \mathcal{O}_d \)-submodule of \( K \).

**Examples.**
1) Let \( r \in K \), then \((r) := r\mathcal{O}_d \) is a fractional ideal.
2) Every ideal \( a \subset \mathcal{O}_d \) is a fractional ideal.

We give now a very simple characterization of fractional ideals.

**Lemma 9.1.** A \( \mathcal{O}_d \)-submodule \( 0 \neq a \) of \( K \) is a fractional ideal if and only if there exists an element \( c \in \mathcal{O}_d \), different from \( 0 \) and with \( ca \subset \mathcal{O}_d \).

**Proof.** A fractional ideal \( a \) is finitely generated and can therefore be written as \( a = (r_1, \ldots, r_s) \) with \( r_i \in K \). There exists an element \( c \in \mathcal{O}_d \) such that \( cr_i \in \mathcal{O}_d \) for all \( i \) and this implies that \( ca \subset \mathcal{O}_d \). Conversely let \( a \subset K \) be a \( \mathcal{O}_d \)-submodule such that there exists an element \( c \in \mathcal{O}_d \) such that \( ca \subset \mathcal{O}_d \). Then \( ca \) is a submodule of \( \mathcal{O}_d \) which by Proposition 6.2 can be written as \( n\mathcal{O}_d + (a + m\omega)\mathcal{O}_d \) and this is a finitely generated \( \mathcal{O}_d \)-submodule of \( K \). \( \square \)

We have seen that the set of ideals \( a \subset \mathcal{O}_d \) form a multiplicative monoid. We define

\[ \mathcal{J}_K = \{ a; \text{ fractional ideal} \}. \]

Then the monoid of integral ideals \( a \subset \mathcal{O}_d \) becomes a submonoid of \( \mathcal{J}_K \). The latter is a group if we define for \( a \neq 0, a \in \mathcal{J}_K \)

\[ a^{-1} = \frac{1}{N(a)} a^\sigma \]

since \( aa^\sigma = N(a) \) by Proposition 6.1. We let \( \mathcal{P}_K \) be the set of principal fractional ideals, i.e. \( \mathcal{P}_K = \{(r); r = a/b, a, b \in \mathcal{O}_d\} \).

**Definition.** The quotient group \( C_K = Cl(K) := \mathcal{J}_K/\mathcal{P}_K \) is called the ideal class group of \( K \). The number \( h_K = \#Cl(K) \) is called the class number of \( K \).

We get an exact sequence \((U_K = \text{units of } K)\)

\[ 1 \rightarrow U_K \rightarrow K^\times \rightarrow \mathcal{J}_K \rightarrow Cl(K) \rightarrow 1 \]

where \( r \in K^\times \mapsto (r) \in \mathcal{J}_K \) and \( a \in \mathcal{J}_K \mapsto [a] = \text{class of } a \).

We also introduce the narrow class group. In the case of quadratic fields the narrow class group differs from the class group only when \( K \) is a real field or, equivalently to that, if \( d_K > 0 \). To define it we consider the homomorphism

\[ \text{sign} : K^\times \rightarrow \mu_2 = \{ \pm 1 \} \]

\[ r \mapsto \frac{r}{|r|} \]
and the embeddings $\sigma_1, \sigma_2 : K \to \mathbb{R}$. This gives

$$s : K^x \to \mu_2 \times \mu_2.$$ 

The kernel of $s$ is called the subgroup of totally positive elements. Let $\mathcal{P}_K^+ \subset \mathcal{P}_K$ be the subgroup of principal ideals generated by totally positive elements. Then $C_K^+ = \text{Cl}(K)^+ = J_K/\mathcal{P}_K^+$ is the narrow class group. Let $\varepsilon$ be a fundamental unit of $K$. Then

$$h_K^+ = \#\text{Cl}(K)^+ = \begin{cases} 2h_K, & N(\varepsilon) = 1, \\ h_K, & \text{otherwise.} \end{cases}$$

This gives the relation between the narrow class group and the class group. The proof is not difficult but we omit it. (See Fröhlich-Taylor, pp. 180-181).

So far we do not know whether the class number is finite. Of course the above relation holds also in the case when the class number is infinite. That this is not the case is the statement of the following

**Theorem 9.1.** Let $d$ be square-free and put

$$\mu_K = \begin{cases} \sqrt{\frac{4}{3}d}, & d > 0 \\ \sqrt{-\frac{4}{3}d}, & d < 0 \end{cases}$$

Then each class contains an ideal $a \subseteq \mathcal{O}_d, a \neq 0$ with $N(a) \leq \mu_K$.

**Proof:** Let $a \in [a]$ be an integral ideal in its class. Then by Proposition 6.2(ii) it takes the form $(m)(u, \beta)$ with $\beta = v + \omega$. We may replace $a$ by $(u, \beta)$ since both are in $[a]$ and assume that $a = (u, v + \omega)$ with $0 < u = N(a)$. Taking into account that $\omega = \sqrt{d}$ or $\omega = (1 + \sqrt{d})/2$ and defining in the latter case $\beta'$ as $v' + \sqrt{d}$ where $v' = v + 1/2$ we may write $a = (u, \beta)$ and $a = (u, \beta')$ respectively. We shall now show that there exists an integral ideal $a' \in [a]$ such that $N(a') \leq \mu_K$. Division by $u$ with remainder allows us to assume that

$$|v|, |v'| \leq u/2 \text{ if } d < 0$$

and

$$u/2 \leq |v|, |v'| \leq u \text{ if } d > 0.$$ 

Furthermore we assume that

$$u^2 > \mu_K^2.$$ 

We first deal with the case that $d < 0$ where $-d = 3\mu_K^2/4 < 3u^2/4$ and then (3) gives

$$N(\beta) = v^2 - d = u^2/4 - d < u^2.$$

Our assumption (5) implies that $u^2 > -4d/3 > -d/3$ and again from (3) we deduce that

$$N(\beta') = (v')^2 - d/4 \leq u^2/4 - d/4 < u^2$$

and we conclude that $N(\beta) < u^2$ and $N(\beta') < u^2$. 

29
If \( d > 0 \) we get from (5) together with (4) that
\[
-u^2 = \frac{u^2 - 5u^2}{4} < v^2 - 5\mu_k^2/4 = v^2 - d < u^2
\]
if \( \omega = \sqrt{d} \) and
\[
-u^2 = \frac{u^2 - 5u^2}{4} \leq (v')^2 - \frac{d}{2} < u^2
\]
if \( \omega = (1 + \sqrt{d})/2 \). This leads to
\[
N(\beta), N(\beta') < u^2.
\]
Define \( a' = u^{-1}\beta a \) or \( a' = u^{-1}(\beta')a \). Then \( a' \sim a \) and
\[
N(a') < N(a).
\]
Since we may assume that \( a \) has smallest norm in its class we get a contradiction provided that
\( a' \subseteq O_d \). This means that our assumption (5) is wrong and, as a consequence, that \( u = N(a) \) is bounded by \( \mu_K \).

It remains to show that \( a' \subseteq O_d \). If \( a' = u^{-1}\beta a \) then \( a' \subseteq O_d \iff \beta a \subseteq uO_d = aa' \iff \beta(\sigma(N(a))) \subseteq a^\sigma(N(a)) \iff \beta^\sigma = \beta \in a \) and this is the case. In the same way we deal with the case \( a' = u^{-1}(\beta')a \). \( \square \)

Complements:
1. decomposition of 2 in \( K = \mathbb{Q}(\sqrt{d}) \)
   - \((2) = (2, \sqrt{d})^2 \iff d \equiv 2 \pmod{4}\)
   - \((2) = (2, 1 + \sqrt{d})^2 \iff d \equiv 3 \pmod{4}\)
   - \(d = 1 \pmod{4} \Rightarrow -d \equiv 1 \pmod{8} \iff 2 = pp', p = (2, (1 + \sqrt{d}/2), p \neq p' \)
   - \(d = 5 \pmod{8} \iff (2) = p\).
2. calculation of \( P_k^+ / P_K \): We define \( ([\sqrt{d}]_+) \) the subgroup of the class group \( Cl^+(K) \). Then
   \[
   1 \rightarrow ([\sqrt{d}]_+ ) \rightarrow Cl^+(K) \rightarrow Cl(K) \rightarrow 1
   \]
   is exact; call the injection \( \iota \) and the surjection \( \pi \). Let \([a]_+ \in ker \pi \). Then \( a = aO_K, a \in K \).
   - \(N(\alpha) > 0 \Rightarrow \alpha > 0 \) or \( \alpha < 0 \). (Because: \( \alpha > 0 \) or \( \alpha < 0 \) \Rightarrow \( N(\alpha) = \alpha \alpha^\sigma > 0 \). Conversely if \( N(\alpha) > 0 \) we have \( \alpha \alpha^\sigma > 0 \) and this means that \( \alpha > 0, \alpha^\sigma > 0 \) or \( \alpha < 0, \alpha^\sigma < 0 \). We choose \( \alpha > 0 \) and find \([a]_+ = 1\).
   - \(N(\alpha) < 0 \Rightarrow \alpha > 0, \alpha^\sigma < 0 \). Then \( \alpha / \sqrt{d} > 0 \) and \( \alpha^\sigma / \sqrt{d} = \alpha^\sigma / (\sqrt{d}) > 0 \) and this gives \( a = \alpha O_K = \alpha / \sqrt{d}(\sqrt{d}) \) and then \([a]_+ = [\sqrt{d}]_+ \) in \( n \).
3. totally positive elements in \( \mathbb{Q}(\sqrt{d}), d > 0 \): \( \alpha = k + l\sqrt{d}, \alpha^\sigma = k - l\sqrt{d}; \alpha > 0 \) and \( \alpha^\sigma > 0 \iff k > -l\sqrt{d} \) and \( k > l\sqrt{d} \).
4. \( Cl(K) \) is a finite group of order \( h_K \Rightarrow \forall [a] \in Cl(K): [a]^h = [1] \Rightarrow a^h = (r), r \in K \).
5. \( K = \mathbb{Q}(\sqrt{d}), (p) = pp', p \neq p' \Rightarrow \exists x, y \in \mathbb{N}: 4p^h = x^2 - dy^2 \). In fact: \( p^h = (x + y\sqrt{d})/2 \) with \( x \equiv y \pmod{2} \). This gives \( p^h = N(p^h) = N((x + y\sqrt{d})/2) = (x^2 - dy^2)/4 \) and then \( 4p^h = x^2 - dy^2 \). In particular, if \( h = 1: 4p = x^2 - dy^2 \).
6. class number 1 for \( d < 0 \): \( d = -1, -2, -3, -7, -11, -19, -43, -67, -163 \)
10 The three squares theorem  
(April 16, 2012)

One of the entries in Gauss’ diary is the mysterious “Eureka!num = \Delta + \Delta + \Delta” i.e. for every positive integer \( n \) we have \( n = x(x + 1)/2 + y(y + 1)/2 + z(z + 1)/2 \) with \( x, y, z \in \mathbb{Z} \). This the same as \( 8n + 3 = (2x + 1)^2 + (2y + 1)^2 + (2z + 1)^2 \). This theorem is much deeper than Lagrange’s theorem that every positive integer \( n \) can be expressed as a sum of 4 squares of integers.

We next prove (in order to give a new proof of Gauss’ assertion):

Lemma 10.1 (Cassel’s Lemma). If the positive integer \( M \) can be expressed as a sum of 3 squares of rational numbers then it can also be expressed as a sum of 3 squares of integers.

Proof. From now on all letters denote integers. Suppose we have \( x_1^2 + x_2^2 + x_3^2 = Ma^2 \) (i.e. \( M \) is a sum of 3 squares of rational numbers). We write this as \( Q(x) = Ma^2 \). Set \( x_i = ay_i + z_i, |z_i|a/2 \) for \( i = 1, 2, 3 \). Briefly \( x = ay + z \). Then we have \( a^2Q(y) + 2aQ(y, z) + Q(z) = Ma^2 \) where \( Q(y, z) = y_1z_1 + y_2z_2 + y_3z_3 \). Clearly \( Q(z) \equiv 0 \) (mod \( a \)). So write \( Q(z) = -ab \) where \( |b| \leq 3a/4 < a \) (since \( |z| \leq a/2 \)). It follows \( 2Q(y, z) - b = a(M - Q(y)) \). Next we shall choose an integer \( t \) such that \( Q(by + tz) = Mb^2 \) or \( b^2Q(y) + 2btQ(y, z) + t^2Q(z) = Mb^2 \). It is easy to see that we can take \( t = M - Q(y) \). (We reject \( t = b/a \), since this is numerically less than 1, and \( b = 0 \) since this implies \( z = 0 \) and so \( a|x; the latter would make \( M \) a sum of 3 integral squares.) Thus we get \( Q(by + tz) = Mb^2 \) with \( |b| < a \). Continuing, we finally get \( M = a \) sum of 3 squares of integers. //

We next use an argument suggested by A. Selberg to deduce from Cassel’s Lemma that for \( M \equiv 3 \) (8), we have \( M = a^2 + v^2 + w^2, u, v, w \in \mathbb{Z} \). By the lemma it is enough to show the existence of \( x, y, z, f \in \mathbb{Z} \) such that \( x^2 + y^2 + z^2 = Mf^2, f \) odd, or \( x^2 + y^2 = Mf^2 - z^2 \). Necessarily \( x, y, z \) have to be odd. Set \( f = (p + q)/2, z = (p - q)/2 \). Then
\[
x^2 + y^2 = 2 \left( \frac{M - 1}{2} \right) (p^2 + q^2) + (M + 1)pq.
\]

It now follows that \( p \) and \( q \) have opposite parity.

Consider the primitive (i.e. the coefficients have no common factor) binary quadratic form \( \left( \frac{M - 1}{2} \right) (p^2 + q^2) + (M + 1)pq \).

It represents (by a know but deep theorem of analytic number theory) infinitely many primes. Since \( M \equiv 3 \) (8), if it represents a prime \( \rho \) then \( p \) and \( q \) have opposite parity. But then this \( \rho \equiv 1 \) (4). Hence \( \rho = \alpha^2 + \beta^2, \alpha \beta \in \mathbb{Z} \). It follows \( x^2 + y^2 = 2\rho = (\alpha + \beta)^2 + (\alpha - \beta)^2 \). But then the original assertion is satisfied with \( x = \alpha + \beta, y = \alpha - \beta \). We have now proved Gauss’ assertion that \( M \equiv 3 \) (8) \( \Rightarrow M = \) sum of 3 squares. //

There is still another proof of the three squares theorem suggested by A. Weil in his course “300 years of number theory” at the IAS Princeton. Apply the so-called “Hasse Principle” to the form \( (x^2 + y^2 + z^2) - Muw^2 \) where \( M > 0, M \equiv 3 \) (8). Since this form represents 0 in every \( p \)-adic field \( (p \) a prime) it represents 0 over \( \mathbb{Q} \). Apply Cassel’s Lemma. //
11 The four squares theorem
(April 20, 2012)

In this lecture we give Euler’s proof of the famous “Four squares theorem” of Lagrange. The basic tool is the identity for products of sums of four squares which he discovered in 1770.

Lemma 11.1. Let $a, b, c, d$ and $p, q, r, s$ be 2 pairs of independent variables and put $m = a^2 + b^2 + c^2 + d^2$ and $n = p^2 + q^2 + r^2 + s^2$. Define $A = ap + bq + cr + ds, B = aq - bp - cs + dr, C = ar + bs - cp - dq, D = as - br + cq - dp$. Then $mn = A^2 + B^2 + C^2 + D^2$.

Proof. Tedious checking. //

The next lemma is a simple application of the Legendre symbol.

Lemma 11.2. Let $p$ be any prime, $\lambda, \nu, \mu$ integers prime to $p$. Then the congruence $\lambda x^2 + \mu y^2 + \nu z^2 \equiv 0 \pmod{p}$ has a non-trivial solution $(x, y, z)$ in integers.

Proof. Consider the group $(\mathbb{Z}/p\mathbb{Z})^\times$ which has order $p - 1$. There is a homomorphism $\lambda_p : (\mathbb{Z}/p\mathbb{Z})^\times \rightarrow \mu_p = \{\pm 1\}$ given by $\lambda_p(a) = (a/p)$, the Legendre symbol, which gives an exact sequence:

$$1 \rightarrow \ker \lambda_p \rightarrow (\mathbb{Z}/p\mathbb{Z})^\times \rightarrow \mu_p \rightarrow 1$$

therefore the function $\sigma : \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}, \bar{x} \mapsto (x \pmod{p} \mapsto \bar{x}^2$ takes $(p - 1)/2$ distinct values, the quadratic residues which are in $\ker \lambda_p$, together with $\bar{0}$. The functions $\bar{x} \mapsto \lambda \bar{x}^2, \bar{x} \mapsto -\mu \bar{x}^2 - \nu$ are affine transformations from $\mathbb{F}_p$ to $\mathbb{F}_p$ and restricted to $\ker \lambda_p$ take also $(p - 1)/2 = (p - 1)/2 + 1$ distinct values. This means that there exists $\bar{x}, \bar{y} \in \mathbb{Z}/p\mathbb{Z}$ such that $\lambda \bar{x}^2 = -\mu \bar{y}^2 - \nu$ with $(\bar{x}, \bar{y}) \neq (\bar{0}, \bar{0})$. Take $x \in \bar{x}, y \in \bar{y}$ and $z = 1$ to get $\lambda x^2 + \mu y^2 + \nu z^2 \equiv 0 \pmod{p}$. //

Lemma 11.3. Let $a_1, a_2, a_3, a_4$ be coprime integers and $p$ a prime such that $a_1^2 + a_2^2 + a_3^2 + a_4^2 \equiv 0 \pmod{p}$. Then $p$ is a sum of four squares.

Proof. Let $p$ be an odd divisor of $a_1^2 + a_2^2 + a_3^2 + a_4^2$. Then we may assume that $a_i \geq 0$ and $a_i < p/2$ for $1 \leq i \leq 4$. We write

$$N = \sum a_i^2 = pm.$$ 

If $m = 2$ then two of the $a_i$ must be odd, say $a_1$ and $a_2$. Then

$$a_1^2 + a_2^2 = \left(\frac{a_1 - a_2}{2}\right)^2 + \left(\frac{a_1 + a_2}{2}\right)^2, \quad a_3^2 + a_4^2 = \left(\frac{a_3 - a_4}{2}\right)^2 + \left(\frac{a_3 + a_4}{2}\right)^2$$

and this gives

$$p = \left(\frac{a_1 - a_2}{2}\right)^2 + \left(\frac{a_1 + a_2}{2}\right)^2 + \left(\frac{a_3 - a_4}{2}\right)^2 + \left(\frac{a_3 + a_4}{2}\right)^2.$$ 

therefore $p$ is a sum of four squares.

If $m > 2$ then we write $a_i = b_i + mc_i$ with $|b_i| \leq m/2$. Then $\sum b_i^2 \equiv 0 \pmod{m}$ and so $\sum b_i^2 = mn$. Since the $a_i$ are coprime not all of the $b_i$ can be 0 or greating $m/2$ which shows that

$$0 < \sum b_i^2 = mn < m^2$$

and $0 < n < m$. By Lemma 11.1 we get

$$\left(\sum a_i^2\right) \left(\sum b_i^2\right) = (pm)(mn) = m^2pn = \sum A_i^2$$
with

\[ A_1 = \sum a_i b_i \]
\[ A_2 = a_1 b_2 - a_2 b_1 - a_3 b_4 + a_4 b_3 = m(c_1 b_2 - c_2 b_1 - c_3 b_4 + c_4 b_3) = mB_2 \]
\[ A_3 = m(c_1 b_3 + c_2 b_4 - c_3 b_1 - c_4 b_2) = mB_3 \]
\[ A_4 = m(c_1 b_4 - c_2 b_3 + c_3 b_2 - c_4 b_1) = mB_4 \]

Since \( A_1^2 + A_2^2 + A_3^2 + A_4^2 \equiv 0 \pmod{m^2} \) we find that \( A_1^2 \equiv 0 \pmod{m} \) and this gives \( A_1 \equiv 0 \pmod{m} \) and we write \( A_1 = mB_1 \). We deduce that \( pm = B_1^2 + B_2^2 + B_3^2 + B_4^2 \). Let \( d = (B_1, B_2, B_3, B_4) \) be the common divisor such that \( B_i = da'_i \). Then \( d | pm \). Since \( 0 < n < m < p \) we conclude that \( (d, p) = 1 \) and so \( d^2 | n \) and we write \( n = d^2 m' \) and \( pm' = \sum a_i^2, m' < m \). After a finite number of steps we find that \( p \) is a sum of four squares. //
12 Binary quadratic forms
(April 30, 2012)

In this lecture we begin to study quadratic forms in two variables \( x \) and \( y \) with integral coefficients, called binary quadratic forms,

\[
f(x, y) = ax^2 + bxy + cy^2,
\]

\( a, b, c \in \mathbb{Z} \). We call \( f \) primitive if \((a, b, c) = 1\).

Its discriminant is

\[
d(f) = -4 \det A, \quad M(f) = A = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}
\]

and then

\[
4af(x, y) = (2ax + by)^2 - d(f)y^2.
\]

We shall now discuss some basic problems which lead to study binary quadratic forms. Then we shall study definiteness and reducible forms (reducible over \( \mathbb{Z} \)) and the notions of equivalence (equivalence and proper equivalence). We end with showing the finiteness of the class number.

1) Basic problems \( f = (a, b, c) \leftrightarrow M(f) \):

a) Representation of integers: Given \( n \in \mathbb{Z} \), find \( x, y \in \mathbb{Z} \times \mathbb{Z} \): \( f(x, y) = n \). If representation exists: \( (x, y) \) proper \( \Leftrightarrow (x, y) = 1 \); otherwise improper.

Example: \( f(x, y) = x^2 - y^2, n = 113 \): \( x^2 - y^2 = 113 \Leftrightarrow (x + y)(x - y) = 113 \); \( (x, y) \) solution \( \Rightarrow (±x, ±y) \) solution. It therefore suffices to solve with \( x \geq 0, y \geq 0 \). \( x = 0 \) or \( y = 0 \) not a solution since 113 is not a square. Assume \( x > y > 0 \). Since 113 is a prime: \( x + y = 113, x - y = 1 \) or \( x + y = 1, x - y = 113 \) (latter not possible since otherwise \( x = 0 \) or \( y = 0 \)). Thus \( 2x = 114 \Rightarrow x = 57 \Rightarrow y = 56 \Rightarrow (x, y) = (±57, ±56) \).

b) number of representations

c) finding minimum: \( \lambda_1(f) = \inf_{0 \neq (x, y) \in \mathbb{Z}^2} \{ |f(x, y)|^{1/2} \} \)

Example: \( f = (269, 164, 25), f(x, y) = 269x^2 + 164xy + 25y^2 = (10x + 3y)^2 + (13x + y)^2 \). Clearly \( |f(x, y)| \geq 1 \) for \( (x, y) \neq (0, 0) \). We show: \( \lambda_1(f) = 1 \). Solve \( 10x + 3y = 0, 13x + 4y = 1 \Leftrightarrow x = 3, y = -10 \). Thus \( f(x, y) = 1 \).

d) representation problem for \( d(f) < 0 \): \( ax^2 + bxy + cy^2 = n; d(f) < 0 \Rightarrow ac > 0 \). Now \( 4an = (2ax + by)^2 + |\Delta|y^2 \geq 0 \) or \( 4cn = (2cy + bx)^2 + |\Delta|x^2 \geq 0 \). Thus \( 4an, 4cn \geq 0 \). If \( n = 0 \) then \( x = y = 0 \); otherwise \( x^2 + 4an/\Delta, y^2 \leq 4an/\Delta \). It follows that there are only finitely many solutions.

2) Positive definite, negative definite, etc.:

Definition.

\[
\begin{align*}
& f > 0 \Leftrightarrow \forall (x, y) \neq (0, 0): f(x, y) > 0 \\
& f < 0 \Leftrightarrow \forall (x, y) \neq (0, 0): f(x, y) < 0 \\
& f \geq 0 \Leftrightarrow \forall (x, y) \neq (0, 0): f(x, y) \geq 0 \\
& f \leq 0 \Leftrightarrow \forall (x, y) \neq (0, 0): f(x, y) \leq 0 \\
& f \text{ indefinite } \Leftrightarrow \exists (x, y), (x', y'): f(x, y) > 0 \text{ and } f(x', y') < 0.
\end{align*}
\]

Proposition 12.1. i) \( f > 0 \Leftrightarrow d(f) < 0 \) and \( a(f) > 0 \).
Proof. We have $4a(f)f = (2a(f)x + b(f)y)^2 - d(f)y^2$ and i) and ii) follow. But also iii) follows since there exist $(x, y)$ with $(2a(f)x + b(f)y) > d(f)y^2$ and $(2a(f)x + b(f)y) < d(f)y^2$. //

3) Reducible forms:

Proposition 12.2. The following statements are equivalent:

i) $d(f) = n^2$,

ii) $f = L_1 \cdot L_2$, $L_1 = k_1x + l_1y$, $L_2 = k_2x + l_2y$ and $k_1, k_2, l_1, l_2 \in \mathbb{Z}$.

Proof. $a = 0 \iff d(f) = b^2 \Rightarrow f(x, y) = y(bx + cy)$. $a \neq 0$: $4af = (2ax + by)^2 - dy^2 = (2ax + by - \sqrt{d})(2ax + by + \sqrt{d}) = L_1L_2$. Then $L_1, L_2$ integral $\iff \sqrt{d} \in \mathbb{Z} \iff d = n^2$ and $4a$ $\text{cont}(f) = \text{cont}(L_1)\text{cont}(L_2)$. This implies $4a = a_1 \cdot a_2$ with $a_1|\text{cont}(L_1)$ and $a_2|\text{cont}(L_2)$.

We write $M_1 = L_1/a_1$, $M_2 = L_2/a_2$ and then $f = M_1M_2$. //

4) Equivalence of forms:

For

$$B = \begin{pmatrix} u & u'' \\ v & v'' \end{pmatrix} \in \text{GL}_2(\mathbb{Z})$$

define $B(x, y) = (ux + u''y, vx + v''y) \sim f(B(x, y)) = f(u, v)x^2 + (2(auu'' + cvv'') + b(uu'' + u''v))xy + f(u'', v'')y^2$. Define $f_B := \text{det}(B \circ B); M(f_B) = \text{det} B \cdot B^{T}M(f)B$. We get action $\text{GL}_2(\mathbb{Z}) \times \mathbb{Q} \to \mathbb{Q}, (B, f) \mapsto f_B$ (check that this is an action).

Definition. a) $f \sim g \iff g = f_B$ for some $B \in \text{GL}_2(\mathbb{Z})$.

b) $f$ and $g$ properly equivalent $\iff g = f_B$ for some $B \in \text{SL}_2(\mathbb{Z})$.

Example: $f = -13x^2 - 36xy - 25y^2, g = x^2 + y^2$. Take

$$B = \begin{pmatrix} -4 & 3 \\ 3 & -2 \end{pmatrix}$$

and get $f \circ B = -x^2 - y^2$ so that $f_B = \text{deg} B f \circ B = x^2 + y^2 = g$. $B \in \text{GL}_2(\mathbb{Z})$ but not in $\text{SL}_2(\mathbb{Z})$ since $\text{deg}B = 8 - 9 = -1$.

5) Find equivalence classes of binary quadratic forms:

We define the class number for $d$ as

$$h(d) = \begin{cases} 
\#	ext{ equiv. classes of primitive quadratic forms of discriminant } d, \\
\#	ext{ equiv. classes of positive definite primitive quadratic forms of discriminant } d,
\end{cases}$$

if $d > 0$ (indefinite case),

if $d < 0$ (definite case).

Lemma 12.1. $h(d) \geq 1$ for all $d$ with $d \equiv 0, 1 \pmod{4}$.

Proof. Put

$$f(x, y) = \begin{cases} 
x^2 - \frac{d}{4}y^2, & d \equiv 0 \pmod{4}, \\
x^2 + xy + \frac{1 + d}{4}y^2, & d \equiv 1 \pmod{4}.
\end{cases}$$

Then $d(f) = d$ in both cases. //
**Theorem 12.1.** For \( 0 \neq d \in \mathbb{Z}, \) \( d \) not a square, we have \( h(d) < \infty. \)

**Proof.** We show that \( f = ax^2 + bxy + cy^2 \) is equivalent to a form \( g = a''x^2 + b''xy + c''y^2 \) with

\[
|b''| \leq |a''| \leq |c''|.
\]

The statement follows since there are only finitely many triples \( a'', b'', c'' \) which satisfy this condition subject to \( b''^2 - 4a''c'' = d. \) Indeed \(|d| = |b''^2 - 4a''c''| \geq 4|a''c''| - b''^2 \geq 4a''^2 - a''^2 = 3a''^2. \)

Also \(|a''| \leq \sqrt{|d|/3}, \) \(|b''| \leq |a''|, c'' = (b''^2 - d)/(4a''). \) This leaves only finitely many possibilities for \( a'', b'', c''. \)

Define \( a'' \) the smallest integer in absolute value such that there exist \( u, v \in \mathbb{Z} \) with \( a'' = f(u, v). \)

We have \( 1 = (u, v) \) for otherwise \( a''/r \) for \( r = f(u, v) \) could be represented by \( f. \) Choose \( u'', v'' \) such that \( 1 = u''u + v''v \) and write

\[
A = \begin{pmatrix} u & u'' \\ v & v'' \end{pmatrix}.
\]

We write

\[
\begin{pmatrix} x'' \\ y'' \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ux + u''y \\ vx + v''y \end{pmatrix}
\]

and \( f(x'', y'') = f(uu' + uu''y, vu + v''y) = g(x, y) = a''x^2 + b''xy + c''y^2 \) with \( a'' = f(u, v), b'' = 2auu'' + b(uu'' + uu'') + 2cvv'', c'' = auu'' + bu''v'' + cvv'' = f(u'', v''). \) We now choose \( n \) such that \( b'' = b'' - 2a''n, |b''| \leq |a''|. \) Since \( a''(x - ny)^2 + b''(x - ny)y + c''y^2 = a''x^2 + (b'' - 2a''n)xy + (a''n^2 - b''n + c'')y^2 \) we see that \( g = a''x^2 + b''xy + c''y^2 \sim ga''x^2 + b''xy + c''y^2 \) with \(|b''| \leq |a''|. \)

By choice of \( a'' \) we have \(|c''| \geq |a''| \) (since \( g(-n, 1) = c'' \) and \(|c''| \geq |a''| \) by minimality of \( a''). \) //
13 Class groups
(May 7, 2012)

We recall some notations and definitions. $K \supset \mathbb{Q}$ quadratic, $K = \mathbb{Q}(\sqrt{d})$ with $d$ square-free,

$$d_K = \begin{cases} 
4d, & d \equiv 2, 3 \pmod{4}, \\
1, & d \equiv 1 \pmod{4}.
\end{cases}$$

We define $\sqrt{d_K}$ as the positive square root if $d_K > 0$ and the root with positive imaginary part if $d_K < 0$. We have

$$\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\omega, \quad \omega = \begin{cases} 
\sqrt{d}, & d \equiv 2, 3 \pmod{4}, \\
\frac{1+\sqrt{d}}{2}, & d \equiv 1 \pmod{4},
\end{cases}$$

and

$$d_K = \begin{vmatrix} 1 & \omega \\
1 & \omega^2 \end{vmatrix}^2.$$

Note: We may take also $\omega^* = (d_K + \sqrt{d_K})/2$ and then $\mathcal{O}_K = \mathbb{Z}[\omega^*].$

Let $a = (a_1, a_2)$ be a fractional ideal. If $a, b \subset \mathcal{O}_K$ then $N(a) := |\mathcal{O}/a|$ and $N(ab^{-1}) = N(a)N(b)^{-1}$. One has

$$\begin{vmatrix} a_1 & a_2 \\
a_1^2 & a_2^2 \end{vmatrix}^2 = d_K N(a)^2.$$

This gives

$$\begin{vmatrix} a_1 & a_2 \\
a_1^2 & a_2^2 \end{vmatrix} = \pm \sqrt{d_K} N(a)$$

and we call the basis $a_1, a_2$ normalized iff the sign is positive

$$\begin{vmatrix} a_1 & a_2 \\
a_1^2 & a_2^2 \end{vmatrix} = \sqrt{d_K} N(a).$$

Put $a_1^* = a_2$ and $a_2^* = a_1$. Then either the basis $a_1, a_2$ or $a_1^*, a_2^*$ is normalized.

We attach to any fractional ideal $a$ a binary quadratic form as follows: Let $a : \{1, 2\} \to a$ be a normalized basis in the sense that $a_1 = a(1), a_2 = a(2)$ is a normalized basis as defined. Then

$$q_a(x, y) := N(a)^{-1} N_{K/\mathbb{Q}}(a_1x + a_2y).$$

Since $\alpha = a_1x + a_2y \in a$ for $x, y \in \mathbb{Z}$ we find that $N_{K/\mathbb{Q}}(\alpha)|N(a)$ so that $q_a(x, y) \in \mathbb{Z}$.

We need two lemmata:

**Lemma 13.1.** A positive integer $n$ is represented by $q_a \iff n$ norm of an integral ideal $b$ in the class of $a$.

**Proof.** Suppose that $n = N(b)$ with $b$ integral and $b = (\gamma)a$ for $\gamma$ totally positive. Then $b^\sigma = (\gamma^\sigma)a^\sigma = (\gamma^\sigma N(a))a^{-1} = (\alpha)a^{-1}$ with $\alpha = \gamma^\sigma N(a)$ and totally positive; here we used that for any fractional ideal $0 \neq c \subset K$ we have $c^\sigma = (N(c))c^{-1}$. We get $n = N(b) = N(a)N(\alpha)^{-1} = N_{K/\mathbb{Q}}(\alpha)N(a)^{-1}$ where $\alpha$ is totally positive and therefore $N_{K/\mathbb{Q}}(\alpha) > 0$. This leads to $n = N(a)^{-1} N_{K/\mathbb{Q}}(a_1x + a_2y) = q_a(x, y)$. Conversely we assume that $n = q_a(x, y)$.
Then there exists \( \alpha = a_1 x + a_2 y \in a \) such that \( n = N_{K/Q}(\alpha)^{-1} N(a)^{-1} \). By assumption \( n > 0 \) which leads to \( N_{K/Q}(\alpha) > 0 \) and to \( N_{K/Q}(\alpha) = N((\alpha)) \). therefore \( n = N((\alpha)) \) with \( \alpha \) either totally positive or totally negative. Since \( (\alpha)a^{-1} \) is integral iff \( \alpha a^{-1} \subseteq \mathcal{O}_K \) which is the same as \( \alpha \in a \) we can put \( b = (\alpha)a^{-1} \subseteq \mathcal{O}_K \). Now \( b^* = N(b)b^{-1} = N(b)(\alpha^{-1})a \) and therefore \( n = N(b) = N(b^*) \) with \( e(b^*) = e(a) \). This proves the claim. 

\[
\begin{align*}
q_a &= N(a)^{-1}(N_{K/Q}(a_1)x^2 + Tr_{K/Q}(a_1a_2^2)xy + N_{K/Q}(a_2)y^2) \\
d_{q_a} &= N(a)^{-2}(Tr_{K/Q}(a_1a_2^2)^2 - 4N_{K/Q}(a_1)N_{K/Q}(a_2)) = N(a)^{-2}(a_1a_2^2 - a_1^2a_2)^2 \\
&= N(a)^{-2} \begin{vmatrix} a_1 & a_2 \\ a_1^2 & a_2^2 \end{vmatrix} = d_K.
\end{align*}
\]

Note: Coefficient of \( x^2 \) is \( N(a)^{-1}N_{K/Q}(a_1) \). If \( d_K < 0 \) we have for \( 0 \neq \xi = x + \sqrt{d}y \) that \( N(\xi) = \xi^* = x^2 - dy^2 > 0 \) and so \( N_{K/Q}(a_1) > 0 \).

Change of normalized basis: \( b : \{1, 2\} \to a \) different basis, then \( b = a \cdot g \) for

\[
g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \text{SL}_2(\mathbb{Z})
\]

(easy calculation). Let \( \mathcal{Q}_K \) be the set of equivalence classes of binary quadratic forms with discriminant \( d_K \). We constructed a map \( \kappa : \mathcal{Q}_K^+ \to \mathcal{Q}_K \) by mapping the class of \( a \) to the class of \( q_a \) where \( a \) is a normalized basis for \( a \).

**Theorem 13.1.** \( \kappa : \mathcal{Q}_K^+ \to \mathcal{Q}_K \) is a bijection.

**Proof.** Surjective: Given \( q = (a, b, c) \) we define the \( \mathbb{Z} \)-module \( a = a\mathbb{Z} + ((b - \sqrt{d_K})/2)\mathbb{Z} = (a, (b - \sqrt{d_K})/2) \) and show that \( a \) is a fractional ideal, i.e. \( \mathcal{O}_K a \subseteq a \). It suffices to verify that \( \omega a \subseteq a \) for \( \omega = (d_K + \sqrt{d_K})/2 \) since a basis for \( \mathcal{O}_K \) is \( 1, \omega \). Since \( d_K = b^2 - 4ac \equiv b^2 \equiv b = -b \pmod{2} \) we get

\[
\frac{d_K + \sqrt{d_K}}{2} \equiv -b + \frac{\sqrt{d_K}}{2} \pmod{1}
\]

and this shows that \( a\omega \in a \). Further

\[
\omega \frac{b - \sqrt{d_K}}{2} = \frac{d_K + \sqrt{d_K}}{2} \frac{b - \sqrt{d_K}}{2} = \frac{d_K b - \sqrt{d_K}}{2} + \frac{b + \sqrt{d_K}}{2} \frac{d_K - b - \sqrt{d_K}}{2} = \frac{d_K - bb - \sqrt{d_K}}{2}
\]

(mod \( a \)) again since \( d_K \equiv b^2 \pmod{4a} \). This proves that \( \omega (b - \sqrt{d_K})/2 \in a \) and together that \( \mathcal{O}_K a \subseteq a \).

The norm of the ideal \( a \) is \( a \). To see this we calculate

\[
N(a) = a a^* = (a^2, b - \sqrt{d_K}/2, a, b + \sqrt{d_K}/2, b^2 - d_K/4) = (a^2, ab, a, b + \sqrt{d_K}/2, ac) \subseteq (a)
\]

and also contains \((a)(a, b, c) = (a) \) since \( q \) is primitive. therefore \( N(a) = N((a)) = |a| \). The basis \( a, (b - \sqrt{d_K})/2 \) is not necessarily normalized:

\[
\begin{vmatrix} a & (b - \sqrt{d_K})/2 \\ a & (b + \sqrt{d_K})/2 \end{vmatrix} = a \sqrt{d_K} = \frac{a}{|a|} N(a) \sqrt{d_K}
\]
unless } a > 0 \text{ which is implied by } d_κ < 0. \text{ If } a < 0 \text{ then } d_κ > 0 \text{ and so } \lambda = \sqrt{d_κ} \text{ is real, which implies that } x^a = -\lambda \text{ and then } N_{K/Q}(\lambda) = -d_κ. \text{ Then the ideal } \lambda a \text{ has normalized basis:}

\[
\begin{vmatrix}
\lambda a & \lambda^b \sqrt{d_κ} \\
x^a & \lambda^b \sqrt{d_κ}
\end{vmatrix} = N_{K/Q}(\lambda) \frac{|a|}{N(a)} \sqrt{d_κ} = -N(\lambda) \frac{|a|}{|q|} N(a) \sqrt{d_κ} = N(\lambda) \sqrt{d_κ}.
\]

Now

\[
q_κ = N(a\lambda)^{-1} N_{K/Q}(\lambda a x + \lambda \frac{b - \sqrt{d_κ}}{2} y) = \frac{N_{K/Q}(\lambda)}{N(\lambda a)} (a^2 x^2 + abxy + \frac{b^2 - d_κ}{2} y^2)
\]

is totally positive and \( \sigma(\lambda a) \). This gives \( N_{K/Q}(\lambda) > 0 \). We conclude that \( q \) is either \( \kappa(e^+(a)) \) or \( \kappa(e^+(\lambda a)) \).

Injective: Suppose that there are fractional ideals \( a, b \) with normalized bases \( a, b \) such that \( q_a \sim q_b \). We may then replace \( b \) by \( bg \) with \( g \in SL_2(\mathbb{Z}) \) to get \( q_a = q_b \). We have to show that there exists \( \lambda \in K^\times \) totally positive such that \( a = \lambda b \). Roots of \( q_a \): \(-a_1/a_2, -a_2^*/a_2^*\), \( b_1/b_2, -b_2^*/b_2^* \). This implies that \( a_1/a_2 = b_1/b_2 \) or \( a_1/a_2 = b_2^*/b_2^* \) and we write \( a_1 = \lambda b_1, a_2 = \lambda b_2 \) in the first case and \( a_1 = \lambda b_1^*, a_2 = \lambda b_2^* \) in the second. In the second case we have

\[
\begin{vmatrix}
a_1 & a_2 \\
a_1^* & a_2^*
\end{vmatrix} = N_{K/Q}(\lambda) \begin{vmatrix}
b_1 & b_2 \\
b_1^* & b_2^*
\end{vmatrix} = -N_{K/Q}(\lambda) \begin{vmatrix}
b_1 & b_2 \\
b_1^* & b_2^*
\end{vmatrix}
\]

and since \( a \) and \( b \) are normalized we find that \( N_{K/Q}(\lambda) < 0 \). Since \( q_a = q_b \) we find that \( N(b^{-1})(b_1 x + b_2 y)(b_1^* x + b_2^* y) = N(a)^{-1}(a_1 x + a_2 y)(a_1^* x + a_2^* y) = N(a)^{-1} N_{K/Q}(\lambda)(b_1 x + b_2 y)(b_1^* x + b_2^* y) \) which implies that \( N_{K/Q}(\lambda) > 0 \), a contradiction. Therefore we are in the first case and then

\[
\sqrt{d_κ} N(a) = \begin{vmatrix}
a_1 & a_2 \\
a_1^* & a_2^*
\end{vmatrix} = N_{K/Q}(\lambda) \begin{vmatrix}
b_1 & b_2 \\
b_1^* & b_2^*
\end{vmatrix} = N_{K/Q}(\lambda) \sqrt{d_κ} N(b).
\]

(remember that \( a, b \) are normalized). This gives \( N_{K/Q}(\lambda) > 0 \). We conclude that \( a = \lambda b \) with some \( \lambda \) such that \( N_{K/Q}(\lambda) > 0 \) which means that \( c^+(a) = c^+(b) \). Indeed, define

\[
\lambda^* = \begin{cases}
\lambda, & \text{if } \lambda > 0, \\
-\lambda, & \text{if } \lambda y < 0.
\end{cases}
\]

Then \( \lambda^* \) is totally positive and

\[
a = \lambda b = \begin{cases}
\lambda b = \lambda^* b, & \lambda > 0, \\
(-\lambda)(-b) = (-\lambda)b = \lambda^* b, & \lambda < 0
\end{cases}
\]

and this gives \( a \sim b \) in the narrow sense. //

Note: A nicer discussion can be found in [3, V, 5.1-5.2]. Look at Prop. 5.1.4, Prop. 5.2.1, Definition 5.2.7, Theorem 5.2.8 and 5.2.9.
14 Representations of integers by binary quadratic forms
(May 14, 2012)

In this final lecture we shall determine which numbers \( n \) can be represented by some fixed primitive binary quadratic form \( q(x, y) \). It turns out that the answer depends only on the proper equivalence class \([q]\) of the form. Furthermore it can be shown that the answer depends only on the residue of \( n \) modulo the discriminant \( d \) of the form. We introduce therefore in the group \( U_d = (\mathbb{Z}/d\mathbb{Z})^\times \) of units of the residue class ring \( \mathbb{Z}/d\mathbb{Z} \) modulo \( d \) a subgroup \( \mathcal{H}_d \) and define for each \([q]\) as above an element \( \omega_d([q]) \) in \( U_d/\mathcal{H}_d \) as follows:

Let \( n \) be an integer co-prime with \( d \) that is represented by some form \( q \in [q] \) and let \( \overline{n} \) be its image in \( U_d/\mathcal{H}_d \). We put \( \omega_d([q]) = \overline{n} \). This defines a map \( \omega_d : \mathbb{Q}_d \longrightarrow U_d/\mathcal{H}_d \).

and one shows that \( \omega_d \) is a homomorphism. For this one has to verify that the map is well-defined. This amounts to showing that if \( m \) is another integer represented by \( q \) then \( \overline{n} = \overline{m} \) and that if \( q' \sim q \) then the set of integers represented by \( q \) coincides with the set represented by \( q' \).

The definition of the subgroup \( \mathcal{H}_d \) needs characters of the group \( \mathbb{Z}/d\mathbb{Z} \).

**Definition 14.1.** A character of a finite abelian group \( G \) is a homomorphism \( \chi : G \longrightarrow \mathbb{Q}^\times \).

The characters of the group \( G \) form a group \( X(G) \) which isomorphic to the group \( G \). If \( G = G' \times G'' \) then \( X(G) = X(G') \times X(G'') \) and this shows by virtue of the Chinese Remainder Theorem that if \( d = 2^e \prod p \) with \( e \) zero or 3 depending on whether the discriminant is even or odd and the product taken over all odd prime divisors of \( d \) then

\[
X(U_d) = X(U_{2^e}) \prod X(U_p).
\]

We denote for \( p \) odd by \( \chi_p \) the character given by the Jacobi symbol \((\frac{n}{p})\). We also have to introduce the character \( \chi_{2^e} \) belonging to the group \( X(U_{2^e}) \). The order of \( U_8 \) is 4 and therefore there are 4 characters in the group. They are given by

\[
1, (-1)^{\frac{n-1}{2}}, (-1)^{\frac{n^2-1}{8}}, (-1)^{\frac{n-1}{2} + \frac{n^2-1}{8}}
\]

and we take their product as \( \chi_8 \). It can be expressed as

\[
\chi_{2^e} = (-1)^{\frac{n^2-1}{8} + \frac{\delta-1}{2} \frac{n-1}{2}}
\]

if \( d = 2^e \delta \) with \( \delta \) odd.
References


Index

$\mathcal{O}$-module, 16
$\mathbb{Z}$-module, 11

Cassel’s Lemma, 18
class number, 16
Conway-Schneeberger Fifteen Theorem, 4
decomposition group, 15
discriminant, 2
equivalence of forms, 2
euclidean algorithm, 9
euclidean ring, 8
Euler’s identity, 5
factorial ring, 8
factorization, 7
Gaussian number rings, 9
ideal
  fractional, 2
  irreducible, 13
  maximal, 13
  prime, 7
  principal fractional, 16
  product of, 11
ideal class group, 16
inertia group, 15
integral, 6
irreducible, 8

narrow class group, 16
normalized basis, 24
number rings, 6
Pell’s equation, 7
prime, 8
  inert, 3
  ramified, 3
  split, 3
principal ideal domain (PID), 8
proper equivalence of quadratic forms, 21
quadratic
  binary quadratic form, 1
  imaginary, 6
  indefinite form, 21
  negative definite form, 21
  positive definite form, 21
  primitive binary forms, 19
  quadratic number field, 2
  real, 6
  reducible form, 21
quadratic reciprocity law, 5
residue field, 15

Theorem
  Dirichlet’s unit, 7
  Four squares, 4, 19
  Three squares, 18
  Two squares, 5
  Wilson’s, 5
totally positive element, 17
unique factorization domain (UFD), 8