Computation of unit and class groups II

Michael E. Pohst

Institut für Mathematik
Technische Universität Berlin

May 23, 2013

Fractional ideals I

Let R be an integral domain with quotient field F. For example, R is an order in an algebraic number field F.

Definition Any non–zero R-module $\mathbf{A}$ in F for which a non–zero element $a \in R$ exists such that $a\mathbf{A}$ is an ideal $\mathbf{a}$ of R is called a **fractional ideal** of R.

We denote the set of all fractional ideals of R by I_R or just I.

Fractional Ideals II

The usual non–zero ideals of R are also fractional ideals (with denominator 1). They are called **integral ideals**. We list several useful properties of fractional ideals.

- the product, the sum, and the intersection of fractional ideals belong to I.
- More important is the so-called **ring of multipliers** for an ideal $\mathbf{A} \in \mathbf{I}$:

  $$[R/\mathbf{A}] := \{\mathbf{x} \in \mathbf{F} \mid \mathbf{xA} \subseteq \mathbf{R}\} \ .$$

  We remark that $[R/\mathbf{A}]$ is again a fractional ideal which equals $\mathbf{A}^{-1}$ in case $\mathbf{A}$ is invertible.
- Invertible ideals $\mathbf{A}$ satisfy $[\mathbf{A}/\mathbf{A}] = \mathbf{R}$.

Fractional Ideals III

Lemma If an ideal $\mathbf{a}$ of R is contained in an integral invertible ideal $\mathbf{m}$ then $\mathbf{a}$ is a multiple of $\mathbf{m}$ with an ideal of R, namely

$$\mathbf{a} = (\mathbf{a}\mathbf{m}^{-1})\mathbf{m} \ .$$

Conversely, if the ideal $\mathbf{a}$ is a multiple of an ideal $\mathbf{m}$ of R, i.e. $\mathbf{a} = \mathbf{m}\mathbf{b}$ for an integral ideal $\mathbf{b}$, then $\mathbf{a}$ is contained in $\mathbf{m}$.

Proof For $\mathbf{a} \subseteq \mathbf{m} \subseteq \mathbf{R}$ we get $\mathbf{a}\mathbf{m}^{-1} \subseteq \mathbf{m}\mathbf{m}^{-1} = \mathbf{R} \subseteq \mathbf{m}^{-1}$.
(The same applies in case of proper containment.)
For the second statement, we conclude via $\mathbf{a} = \mathbf{m}\mathbf{b} \subseteq \mathbf{m}\mathbf{R} = \mathbf{m}$.

Fractional ideals IV

Corollary Integral ideals $\mathbf{a}$ which are properly contained in an invertible maximal ideal $\mathbf{m}$ satisfy

$$\mathbf{a} = (\mathbf{a}\mathbf{m}^{-1})\mathbf{m} ,$$

and $\mathbf{a}\mathbf{m}^{-1}$ is an ideal of R properly containing $\mathbf{a}$.

If every non–zero ideal of R is invertible then every non–zero prime ideal of R is maximal.

It is not difficult to show that R is also Noetherian and integrally closed in that case.

Dedekind rings I

Definition An integral domain R is called a **Dedekind ring** if it has the properties

1. R is noetherian,
2. R is integrally closed,
3. in R every non–zero prime ideal is maximal.

Theorem For integral domains R the following conditions are equivalent:

1. R is a Dedekind ring.
2. The fractional ideals of R form a group.
3. Every non–zero ideal $\mathbf{a}$ of R is a product of non–zero prime ideals. (This presentation is unique up to the ordering of the factors.)

Dedekind rings I

Definition An integral domain R is called a **Dedekind ring** if it has the properties

1. R is noetherian,
2. R is integrally closed,
3. in R every non–zero prime ideal is maximal.

Theorem For integral domains R the following conditions are equivalent:

1. R is a Dedekind ring.
2. The fractional ideals of R form a group.
3. Every non–zero ideal $\mathbf{a}$ of R is a product of non–zero prime ideals. (This presentation is unique up to the ordering of the factors.)

Ideals in O_F

Any non-zero ideal of O_F (and therefore every fractional ideal) has a $\mathbb{Z}$–basis of n elements. Hence, there exists a transformation matrix $T \in \mathbb{Z}^{n\times n}$ from a basis of O_F to a basis of $\mathbf{a}$. We call $|\det T|$ the **norm** $N(\mathbf{a})$ of $\mathbf{a}$. $N(\mathbf{a})$ coincides with the $\mathbb{Z}$-module index of $\mathbf{a}$ in O_F.

Lemma Let $\mathbf{a}$ be an integral ideal of O_F and $0 \neq a \in \mathbf{a}$. Then there exists $\alpha \in \mathbf{a}$ such that $\mathbf{a}$ is the greatest common divisor of two principal ideals:

$$\mathbf{a} = \mathbf{aO_F} + \alpha\mathbf{O_F} \quad .$$

The 2-element presentation can be normalized such that $(a, \alpha)(b, \beta) = (ab, \alpha\beta)$.

Ideals in O_F

Lemma Any two integral ideals $\mathbf{a}, \mathbf{b}$ of O_F satisfy $N(\mathbf{ab}) = \mathbf{N}(\mathbf{a})\mathbf{N}(\mathbf{b})$, i.e. the ideal norm is multiplicative.

Proof Since the considered ideals are power products of prime ideals it suffices to show that

$$N\left(\prod_{i=1}^{k} \mathbf{p_i^{m_i}}\right) = \prod_{i=1}^{k} N(\mathbf{p_i})^{\mathbf{m_i}}$$

for pairwise different non-zero prime ideals $\mathbf{p_i}$ of O_F and positive exponents m_i. We will do this in two steps.

Ideals in O_F

Step 1

$$N\left(\prod_{i=1}^{k}\mathbf{p_i^{m_i}}\right) = \prod_{i=1}^{k} N(\mathbf{p_i^{m_i}})$$

is just a consequence of the Chinese Remainder Theorem stating that

$$O_E/\prod_{i=1}^{k}\mathbf{p_i^{m_i}}$$

is isomorphic to the direct product

$$\prod_{i=1}^{k} O_E/\mathbf{p_i^{m_i}} \quad .$$

Ideals of O_F

Step 2

In order to prove that $N(\mathbf{p^m}) = \mathbf{N}(\mathbf{p})^\mathbf{m}$ holds for prime ideals it suffices to show that the $\mathbb{Z}$-modules $O_E/\mathbf{p}$ and $\mathbf{p^{m-1}}/\mathbf{p^m}$ are isomorphic for $m \geq 2$. We choose an element $\pi \in \mathbf{p} \setminus \mathbf{p^2}$ and introduce the $\mathbb{Z}$–module homomorphism

$$\varphi \ : \ O_E \to \mathbf{p^{m-1}}/\mathbf{p^m} \ : \ \mathbf{x} \mapsto \mathbf{x}\pi^{\mathbf{m-1}} + \mathbf{p^m} \ \ .$$

The kernel of φ equals $\mathbf{p}$. It remains to show that φ is also surjective. For this we let $y \in \mathbf{p^{m-1}}$. Because of $\pi^{m-1}O_E + \mathbf{p^m} = \mathbf{p^{m-1}}$ there exists an element $z \in O_E$ such that the residue classes $\pi^{m-1}z + \mathbf{p^m}$ and $y + \mathbf{p^m}$ coincide, hence $y = \varphi(z)$.

Finiteness of the class group

We fix some notation. By I_F we denote the (abelian multiplicative) group of fractional ideals of O_F. It contains a subgroup P_F of principal fractional ideals. The factor group $Cl_F := I_F/P_F$ is called the **class group** of O_F, respectively F. Its order h_F is said to be the **class number** of F.

Lemma Every ideal class of F contains an integral ideal $\mathbf{a}$ satisfying

$$N(\mathbf{a}) \leq \frac{\mathbf{2^{n(n-1)/4}}}{\mathbf{n^{n/2}}}\sqrt{|\mathbf{d_F}|} =: \mathbf{B_F} \ .$$

Proof

Let $\mathbf{m}$ be an ideal and $\mathbf{mP_F}$ its corresponding ideal class. We choose an integral ideal $\mathbf{b}$ in $(\mathbf{mP_F})^{-1}$. Then $\mathbf{b}$ has a $\mathbb{Z}$-basis which we assume to be reduced by the *LLL*-algorithm. Let β_1 be the first basis element of that reduced basis. By the *LLL* property we have

$$T_2(\beta_1) \leq 2^{(n-1)/2}(N(\mathbf{b})\sqrt{|\mathbf{d_F}|})^{\mathbf{2/n}} \ .$$

On the other hand, the principal ideal $\beta_1 o_F$ is the product of $\mathbf{b}$ and another integral ideal, say $\mathbf{a}$, which belongs to $(\mathbf{bP_F})^{-1} = \mathbf{mP_F}$. We obtain

$$\begin{aligned} N(\mathbf{a}) &= \frac{N(\beta_1 o_F)}{N(\mathbf{b})} = \frac{|N(\beta_1)|}{N(\mathbf{b})} \leq \left(\frac{T_2(\beta_1)}{n}\right)^{n/2} N(\mathbf{b})^{-1} \\ &\leq \frac{2^{n(n-1)/4}}{n^{n/2}} \sqrt{|d_F|} \ . \end{aligned}$$

Remark In practice we rather use Minkowski's bound $M_F := \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|d_F|}$.

Class group computation I

With those last results it is now easy to develop a concept for an algorithm for computing the class group of F. We recall the following facts on integral ideals:

- the ideal norm is multiplicative;
- every ideal is a product of prime ideals;
- every prime ideal $\mathbf{p}$ contains exactly one prime number p;
- the norm of $\mathbf{p}$ is a power p^f with $1 \leq f \leq n$.

From the last lemma we know that every ideal class has an integral representative, say $\mathbf{a}$, subject to $N(\mathbf{a}) \leq \mathbf{B_F}$. Clearly, $\mathbf{a}$ is a product of prime ideals $\mathbf{p}$ with $N(\mathbf{p}) \leq \mathbf{B_F}$. Hence, we proceed as follows.

Class group computation II

We generate a list L_1 of prime numbers $p \leq B_F$. For each $p \in L_1$ we decompose pO_F into prime ideals. Then we obtain a list L_2 of all non–zero prime ideals of norm $\leq B_F$.

Theorem (Kummer) Let $F = \mathbb{Q}(\rho)$ be an algebraic number field of degree n. Let $f(t) \in \mathbb{Z}[t]$ be the minimal polynomial of ρ. Let p be a prime number not dividing the index $(O_F : \mathbb{Z}[\rho])$. Let $f_i(t) \in \mathbb{Z}[t]$ $(1 \leq i \leq g)$ be monic such that

$$f(t) \equiv \prod_{i=1}^{g} f_i(t)^{\hat{e}_i} \bmod p\mathbb{Z}[t]$$

corresponds to a factorization of $f(t)$ into prime polynomials in $\mathbb{Z}/p\mathbb{Z}[t]$.

Class group computation III

Then pO_F is decomposed into prime ideals as follows:

$$pO_F = \prod_{i=1}^{g} \mathbf{p_i}^{\mathbf{e(p_i|pO_F)}}$$

subject to

$$\mathbf{p_i} = \mathbf{pO_F} + \mathbf{f_i}(\rho)\mathbf{O_F},\ \mathbf{e}(\mathbf{p_i}\,|\,\mathbf{pO_F}) = \hat{\mathbf{e}}_\mathbf{i},\ \mathbf{f}(\mathbf{p_i}\,|\,\mathbf{pO_F}) = \deg(\mathbf{f_i})\ (\mathbf{1} \leq \mathbf{i} \leq \mathbf{g})\ .$$

We note that the calculation of the prime ideal decomposition of prime numbers dividing the index $(O_F : \mathbb{Z}[\rho])$ is a lot more difficult.

Class group computation IV

We assume that $L_2 = \{\mathbf{p_1}, \ldots, \mathbf{p_v}\}$. L_2 is usually called **factor basis**. Then we need to generate sufficiently many **relations** between the elements of L_2. These are principal ideals $\gamma_j O_F$ which are power products of the elements of L_2, $j = 1, 2, \ldots, k$. We then obtain a so-called **class group matrix** $M = (m_{ij}) \in \mathbb{Z}^{v \times k}$ whose columns are just the exponent vectors of the relations $\gamma_j o_F = \prod_{i=1}^{v} \mathbf{p_1}^{\mathbf{m_{ij}}}$.

We remark that we get a few relations for free by decomposing pO_F with $p \in L_1$ into prime ideals, for example, with Kummer's theorem. The number k of relations is sufficient when M is of full rank v. Usually, we try to exhibit new relations via the basis elements of a LLL–reduced bases of one of the prime ideals of L_2, respectively of small products of those. In this way we can also increase the rank of M systematically.

Example I

Let $F = \mathbb{Q}(\sqrt{-814})$. Then L_1 consists of all prime numbers less than $40 = \lfloor B_F \rfloor$. By factoring $t^2 + 814 \bmod p$ for all $p \in L_1$ we find

$$L_2 = \{\mathbf{p_2},\, \mathbf{p_{5,1}},\, \mathbf{p_{5,2}},\, \mathbf{p_{11}},\, \mathbf{p_{17,1}},\, \mathbf{p_{17,2}},\, \mathbf{p_{37}}\}\,.$$

We note that 2, 11, 37 are ramified and 5 and 17 are the only prime numbers $p \in L_1$ for which pO_F decomposes into two prime ideals. From Kummer's Theorem we obtain

$$\begin{array}{lclcl}
\mathbf{p_2} & = & 2\,O_F & + & \sqrt{-814}\,O_F\,, \\
\mathbf{p_{5,1}} & = & 5\,O_F & + & (1+\sqrt{-814})\,O_F\,, \\
\mathbf{p_{5,2}} & = & 5\,O_F & + & (-1+\sqrt{-814})\,O_F\,, \\
\mathbf{p_{11}} & = & 11\,O_F & + & \sqrt{-814}\,O_F\,, \\
\mathbf{p_{17,1}} & = & 17\,O_F & + & (6+\sqrt{-814})\,O_F\,, \\
\mathbf{p_{17,2}} & = & 17\,O_F & + & (-6+\sqrt{-814})\,O_F\,, \\
\mathbf{p_{37}} & = & 37\,O_F & + & \sqrt{-814}\,O_F
\end{array}\,.$$

Example II

The following class group matrix is immediate.

	2	5	11	17	37
$\mathfrak{p}_2$	2	0	0	0	0
$\mathfrak{p}_{5,1}$	0	1	0	0	0
$\mathfrak{p}_{5,2}$	0	1	0	0	0
$\mathfrak{p}_{11}$	0	0	2	0	0
$\mathfrak{p}_{17,1}$	0	0	0	1	0
$\mathfrak{p}_{17,2}$	0	0	0	1	0
$\mathfrak{p}_{37}$	0	0	0	0	2

.

Since we have 7 different prime ideals we need at least two more relations.

Example III

We try elements of the form $m + \sqrt{-814}$ and easily find

$$\begin{array}{rclcrcl} \gamma_1 & = & 6 + \sqrt{-814} & \text{of norm} & 850 & = & 2 \cdot 5^2 \cdot 17\,, \\ \gamma_2 & = & -11 + \sqrt{-814} & \text{of norm} & 935 & = & 5 \cdot 11 \cdot 17 \end{array} .$$

We observe that $\gamma_1 O_F = \mathbf{p_2 p_{5,1}^2 p_{17}}$, and $\gamma_2 O_F = \mathbf{p_{5,2} p_{11} p_{17}}$. Hence, we get two additional columns for the class group matrix M: $(1, 2, 0, 0, 1, 0, 0)^{\text{tr}}$ and $(0, 0, 1, 1, 1, 0, 0)^{\text{tr}}$.

Class group computation V

Once the class group matrix is of rank v we apply Hermite column reduction in order to transform it into an upper triangular matrix. We call the result again M. That reduction procedure produces new relations, but we are only interested in the corresponding exponent vectors.

Next we can remove all rows and columns with a 1 on the diagonal. Namely, an entry $m_{ii} = 1$ either means $\mathbf{p_i}$ is principal in case $m_{\mu i} = 0 \ (1 \leq \mu < i$ or – if there are non–zero entries $m_{\mu i}$ with $1 \leq \mu < i$ – then $\mathbf{p_i}\,\mathbf{P_F}$ is represented by $\left(\prod_{\mu=1}^{i-1} \mathbf{p}_\mu^{\mathbf{m}_{\mu\mathbf{i}}}\,\mathbf{P_F}\right)^{-1})$.

This yields a **reduced class group matrix** of much smaller size.

Example IV

We start by permuting the columns of M: The new order will be (1 3 2 7 6 4 5):

$$M = \begin{pmatrix} 2 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix} .$$

Example V

We subtract columns 3 and 5 from column 4, yielding a new 4th column $(0\,0\,0\,1\,0\,-3\,-1)^{\text{tr}}$.
Then we subtract $2\times$ the new column 4 and column 1 from column 2:

$$M = \begin{pmatrix} 2 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 6 & 1 & -3 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix} .$$

Example VI

Removing all ones on the diagonal we end up with only three prime ideals $\mathbf{p_2}, \mathbf{p_{5,1}}, \mathbf{p_{37}}$ and a reduced class group matrix

$$M = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 2 \end{pmatrix} .$$

Class group computation VI

At this stage we know prime ideals $\{\mathbf{p_1}, \ldots, \mathbf{p_u}\}$ with $u \leq v$ and relations $\gamma_j\, O_F = \prod_{i=1}^{u} \mathbf{p_i}^{\mathbf{m_{ij}}}$.

Especially, we know that

- $\mathbf{p_1}^{\mathbf{m_{11}}}$ is a principal ideal,
- $\#\langle \mathbf{p_1}\, \mathbf{P_F}, \ldots, \mathbf{p_i}\, \mathbf{P_F} \rangle \mid (\mathbf{m_{11}} \cdot \ldots \cdot \mathbf{m_{ii}})$,
- $h_F \mid \prod_{i=1}^{u} m_{ii}$.

Class group computation VII

For determining the order of $\mathbf{p_1}\,\mathbf{P_F}$ we need to test whether $\mathbf{p_1}^{\mathbf{m}_{11}/\mathbf{q}}$ is principal for all prime numbers q dividing m_{11}.

We note that an integral ideal $\mathbf{a}$ is principal precisely if $\mathbf{a} \ni \alpha$ subject to $\mathbf{a} = \alpha\,\mathbf{O_F}$. A necessary condition for the existence of such an element is the existence of $\alpha \in O_F$ with $|N(\alpha)| = N(\mathbf{a})$.

This idea can usually only be used if the unit rank of F is small.

Example VII

We know that $\mathbf{p_2^2}$, $\mathbf{p_{5,1}^6}$, $\mathbf{p_{37}^2} \in \mathbf{P_F}$.

We have $N(\mathbf{p_2}) = \mathbf{2}$, $\mathbf{N(p_{5,1}) = 5}$, $\mathbf{N(p_{37}) = 37}$.

An element $\alpha = a + b\sqrt{-814} \in o_F$ has norm $|N(\alpha)| = N(\alpha) = a^2 + 814\, b^2$. This excludes norms 2, 125, 37, 50, 250.

We can obtain $N(\alpha) = 25$ only for $\alpha = 5$, but $5\, o_F = \mathbf{p_{5,1}\, p_{5,2}} \neq \mathbf{p_{5,1}^1}$. Therefore we get $\#\langle \mathbf{p_2\, P_F},\, \mathbf{p_{5,1}\, P_F} \rangle = \mathbf{12}$.

Example VIII

If the subgroup $\langle \mathbf{p_2}\,\mathbf{H_F}\rangle \times \langle \mathbf{p_{5,1}}\,\mathbf{H_F}\rangle$ of the class group also contains $\mathbf{p_{37}}\,\mathbf{H_F}$ then we must have an element with norm in $\{37,\, 2\cdot 37,\, 5^3\cdot 37\}$.

The first two values are clearly impossible. But the element $\alpha = 37 + 2\sqrt{-814}$ has norm $5^3 \cdot 37$. We have $\alpha \in \mathbf{p_{37}}$ and $\alpha \in \mathbf{p_{5,1}}$, hence $\alpha \in \mathbf{p_{5,1}^3}$. Therefore $\alpha\, o_F \subseteq \mathbf{p_{37}}\mathbf{p_{5,1}^3} = \mathbf{p_{37}}\mathbf{p_{5,1}^3}$ and because of $N(\alpha) = 5^3 \cdot 37$ we must have equality. This tells us that $\mathbf{p_{37}}\,\mathbf{P_F} = \mathbf{p_{5,1}^3}\,\mathbf{P_F}$.

We obtain $h_F = 12$ and $Cl_F \cong C_2 \times C_6$.

Class and unit group computations

Computing class and unit groups jointly.
Let F be an algebraic number field with unit rank r. As usual, we choose a factor basis $L = \{\mathbf{p_1}, \dots, \mathbf{p_v}\}$. We now consider

$$\Phi : F^{\times} \to \mathbb{Z}^v \times \mathbb{R}^r$$

which maps

$$0 \neq \alpha_j \in F \text{ with } \alpha O_F = \prod_{i=1}^{v} \mathbf{p_i}^{\mathbf{a_{ij}}}$$

onto the vector $(a_{1j}, ..., a_{vj}, c_1 \log(|\alpha^{(1)}|), ..., c_r \log(|\alpha^{(r)}|))^{\mathrm{tr}}$ with constants $c_i = 1$ for $1 \leq i \leq r_1$ and $c_i = 2$ for $i > r_1$. The upper parts of those vectors correspond to the class group matrix introduced before. If a $\mathbb{Z}$–linear combination of those vectors has all first v coordinates 0 then the corresponding power product of the relations represents a unit.

Class and unit group computations

Hence, having computed sufficiently many relations we may assume that the Hermite normal form of the matrix of the corresponding Φ–values is of the form

$$\left(\begin{array}{c|c} A & \mathbf{0} \\ \hline C & B \end{array}\right)$$

with matrices of full rank $A \in \mathbb{Z}^{v \times v}$ and $B \in \mathbb{R}^{r \times r}$. We easily see that $\det(A)$ is an integral multiple of the class number h_F and that $\det(B)$ is an integral multiple of Reg_F.

If we can approximate $h_F \mathrm{Reg}_F$ sufficiently well we see when we have calculated sufficiently many relations and know both h_F and Reg_F, also yielding generating elements of the class group and of the unit group of F.

Analytic methods

Lemma (Bach) Assuming GRH to be true the class group of F is generated by prime ideals $\mathbf{p}$ whose norms are bounded by $B = 12(\log(|d_F|))^2$.

Theorem $h_F \mathrm{Reg}_F = 2^{-r_1}(2\pi)^{-r_2} w \sqrt{|d_F|} \prod_{p \in \mathbb{P}} \frac{1-1/p}{\prod_{\mathbf{p} \ni p} 1-1/N(\mathbf{p})}$.

Principal ideal test

Given an (integral) ideal **a** decide whether it is principal. If **a** is indeed principal construct a generating element α with $\mathbf{a} = \alpha\mathbf{O_F}$.

1. Method: Solve a norm equation $|N(x)| = N(\mathbf{a})$ for $x \in O_F$.

2. Method: Search for elements $0 \neq \beta$ of small T_2–norm in *IDa* and try to factorize $\beta O_F/\mathbf{a}$ over the factor basis.

We note that the quotient of $\min\{N(\beta O_F/\mathbf{a}) | \mathbf{0} \neq \beta \in \mathbf{a}\}$ and Minkowski's upper bound M_F for norms of integral ideals in each ideal class tends to 0 for $n \to \infty$.