Computation of unit groups and class groups I

Michael E. Pohst

Institut für Mathematik
Technische Universität Berlin

June 22, 2013

Units

Let F be an algebraic number field of degree $n = r_1 + 2r_2$. A **unit** of an order R of F is an invertible element ε of R. The group of units of R will be denoted by $U(R)$.

1. $\alpha \in R$ belongs to $U(R)$ precisely if $N(\alpha) \in U(\mathbb{Z}) = \{\pm 1\}$.
2. R contains only a finite number of non–associate elements of bounded norm. (Elements $\alpha, \beta \in R$ are called **associate** if α/β and β/α belong to R.)
3. For any constant $C > 0$ there exist only finitely many elements $\alpha \in R$ such that the absolute values of all conjugates of α are bounded by C.

Units

Let F be an algebraic number field of degree $n = r_1 + 2r_2$. A **unit** of an order R of F is an invertible element ε of R. The group of units of R will be denoted by $U(R)$.

1. $\alpha \in R$ belongs to $U(R)$ precisely if $N(\alpha) \in U(\mathbb{Z}) = \{\pm 1\}$.
2. R contains only a finite number of non–associate elements of bounded norm. (Elements $\alpha, \beta \in R$ are called **associate** if α/β and β/α belong to R.)
3. For any constant $C > 0$ there exist only finitely many elements $\alpha \in R$ such that the absolute values of all conjugates of α are bounded by C.

Roots of unity

An element $\xi \in R$ is a **root of unity** precisely if all conjugates of ξ have absolute value 1.

All roots of unity of R form a finite cyclic subgroup which we denote by $TU(R)$, in case of $R = o_F$ by TU_F.

A generator of the group $TU(R)$ of order w will be denoted by ζ (primitive w–th root of unity).

For imaginary quadratic extensions F $(2 = n = 2r_2)$ we have $U(R) = TU(R)$.

Structure of the unit group

The conjugates of $x \in F$ are denoted by $x^{(1)}, ..., x^{(n)}$. They are ordered in the usual way such that $x^{(j)} \in \mathbb{R}$ for $1 \le j \le r_1$, $x^{(j)} \in \mathbb{C} \setminus \mathbb{R}$ for $r_1 < j \le n$ subject to $x^{(r_1+r_2+j)} = \overline{x^{(r_1+j)}}$ for $1 \le j \le r_2$.

Theorem (Dirichlet) The unit group $U(R)$ of R is a direct product of its torsion subgroup $TU(R)$ with $r = r_1 + r_2 - 1$ infinite cyclic groups:

$$U(R) = TU(R) \times \langle E_1 \rangle \cdots \times \langle E_r \rangle \cong C_w \, \mathbb{Z}^r \, .$$

The generators $E_1, ..., E_r$ form a system of **fundamental units**.

Structure of the unit group

The conjugates of $x \in F$ are denoted by $x^{(1)}, ..., x^{(n)}$. They are ordered in the usual way such that $x^{(j)} \in \mathbb{R}$ for $1 \le j \le r_1$, $x^{(j)} \in \mathbb{C} \setminus \mathbb{R}$ for $r_1 < j \le n$ subject to $x^{(r_1+r_2+j)} = \overline{x^{(r_1+j)}}$ for $1 \le j \le r_2$.

Theorem (Dirichlet) The unit group $U(R)$ of R is a direct product of its torsion subgroup $TU(R)$ with $r = r_1 + r_2 - 1$ infinite cyclic groups:

$$U(R) = TU(R) \times \langle E_1 \rangle \cdots \times \langle E_r \rangle \cong C_w \, \mathbb{Z}^r .$$

The generators $E_1, ..., E_r$ form a system of **fundamental units**.

Regulator

We consider the logarithmic map

$$L : F^{\times} \to \mathbb{R}^r : x \mapsto (c_1 \log|x^{(1)}|, \ldots, c_r \log|x^{(r)}|) ,$$

with constants $c_j = 1$ for $1 \le j \le r_1$ and $c_j = 2$ for $j > r_1$.

The image of the unit group $L(U(R))$ is a lattice of determinant

$$\mathrm{Reg}_R := \left| \det \begin{pmatrix} L(E_1) \\ . \\ . \\ . \\ L(E_r) \end{pmatrix} \right| =: d(L(U(R))) .$$

Reg_R is called the **regulator** of the order R.

In case $R = o_F$ we write Reg_F instead of Reg_R.

Independent units

Units ε_1, ..., ε_k are called **independent**, if a relation

$$\varepsilon_1^{m_1} \cdots \varepsilon_k^{m_k} = 1 \ \ (m_i \in \mathbb{Z})$$

implies $m_1 = \ldots = m_k = 0$. Otherwise they are said to be **dependent**.

Remark ε_1, ..., ε_k are independent if and only if $L(\varepsilon_1)$, ..., $L(\varepsilon_k)$ are $\mathbb{R}$-linearly independent.

The computation of fundamental units is usually done by calculating a maximal system of independent units which generates a subgroup of $U(R)$ of small index. Then this subgroup is gradually enlarged to all of $U(R)$.

Independent units

We choose suitable sets of conjugates
$I = \{i_1, \ldots, i_\mu\} \subset \{1, \ldots, r_1 + r_2\}$.

By $\tilde{I}$ we denote the subset of $\{1, \ldots, n\}$ containing $i_1, \ldots, i_\mu$ and also all $i_\nu + r_2$ in case $i_\nu > r_1$ belongs to I.

We set

$$\#\tilde{I} = \tilde{\mu}, J = \{1, \ldots, r_1 + r_2\} \setminus I, \tilde{J} = \{1, \ldots, n\} \setminus \tilde{I} \ .$$

Independent units

Then we calculate a sequence of elements $\{\beta_{I,k}\}_{k\in\mathbb{Z}^{\geq 0}}$ and modules $M_{I,k}$ with the following properties:

$$\beta_{I,0} = 1,\ M_{I,0} := R$$

$$\beta_{I,k+1} \in M_{I,k},\ M_{I,k+1} := \frac{1}{\beta_{I,k+1}} M_{I,k}$$

$$|\beta_{I,k+1}{}^{(j)}| < 1 \ \ \forall j \in \tilde{I}\,,\ |\beta_{I,k+1}{}^{(j)}| \geq 1 \ \ \forall j \in \tilde{J},$$

$$\prod_{i=0}^{k+1} |N(\beta_{I,i})| \leq \tilde{C}$$

with a fixed constant $\tilde{C} > 0$.

Independent units

Next we compute $\beta_{I,k+1} \in M_{I,k}$.
We choose $d \geq 1$ sufficiently large, for example $d \geq 2^{n(n-1)/2}|d(R)|$. Then we set

$$\lambda_j = d \ \text{ for } j \in \tilde{J},\ \lambda_j = d^{1-n/\tilde{\mu}} \ \text{ for } j \in \tilde{I}.$$

For a $\mathbb{Z}$–Basis $\omega_1, ..., \omega_n$ of $M_{I,k}$ we define a positive definite quadratic form with attached weights:

$$T_{2,\lambda}(\mathbf{x}) = \sum_{j=1}^{n} \lambda_j^{-2} \ \left|\sum_{i=1}^{n} x_i \omega_i^{(j)}\right|^2 .$$

$\beta_{I,k+1}$ is chosen as first basis element of a basis of $M_{I,k}$ which is LLL–reduced with respect to $T_{2,\lambda}$.

Independent units

Upon detecting modules $M_{I,\mu} = M_{I,\nu}$ with indices $\mu > \nu$ we obtain a unit

$$\varepsilon = \prod_{k=\nu+1}^{\mu} \beta_{I,k}.$$

with

$$|\varepsilon^{(j)}| < 1 \ \forall j \in \tilde{I} \text{ and } |\varepsilon^{(j)}| \geq 1 \ \forall j \in \tilde{J} \ .$$

These ideas can be made more efficient by using factor bases and relations, similar to class group computations.

Independent units

A **factor basis** is a set $\mathcal{B}$ of prime ideals of R, say,

$$\mathcal{B} = \{\mathbf{p}_1, \ldots, \mathbf{p}_v\} .$$

By **relations** we denote elements α_i of R (or F) for which the principal ideals $\alpha_i R$ are power products of the elements of $\mathcal{B}$:

$$\alpha_i R = \prod_{j=1}^{w} \mathbf{p}_j^{a_{ij}} .$$

Independent units

Hence, a relation is in $1-1$–correspondence with an exponent vector $\mathbf{a}_i = (a_{i1}, \ldots, a_{iv})$. Having found sufficiently many relations

$$\mathbf{a}_1, \ldots, \mathbf{a}_k \ ,$$

e.g. $k > v$, we obtain non–trivial linear presentations

$$\sum_{\mu=1}^{k} m_\mu \mathbf{a}_\mu \ = \ \mathbf{0} \ \ (\mathbf{m}_\mu \in \mathbb{Z}) \ ,$$

hence, a unit

$$\varepsilon \ = \ \prod_{\mu=1}^{k} \alpha_\mu^{m_\mu}$$

of R.

Independent units

Clearly, we are in need of a method for proving the dependence/independence of the calculated units.

Theorem (Dobrowolsky) An element $\alpha \in o_F$ is either a root of unity or there exists a conjugate $\alpha^{(j)}$ of α subject to

$$|\alpha^{(j)}| > 1 + \frac{1}{6}\frac{\log n}{n^2} \quad .$$

Corollary 1 A unit $\varepsilon \in o_F$ is either a root of unity or its image in logarithmic space satisfies

$$\| L(\varepsilon) \|_2 > \frac{21}{128}\frac{\log n}{n^2} \quad .$$

Calculation of fundamental units

Corollary 2 If F is totally real then $\alpha \in o_F$ is either of the form $\cos q\pi$ ($q \in \mathbb{Q}$) or it has a conjugate $\alpha^{(j)}$ subject to

$$|\alpha^{(j)}| > 2 + \frac{1}{1152} \frac{\log^2 2n}{n^4} \ .$$

At this stage we assume that we know $TU(R)$ as well as r independent units $\varepsilon_1, \dots, \varepsilon_r$ of R. If we know an upper bound for the index of

$$U \ := \ \langle TU(R), \varepsilon_1, \dots, \varepsilon_r \rangle$$

in the full unit group $U(R)$ then there are well known methods for enlarging U to $U(R)$.

That index is easily seen to be

$$(U(R) \,:\, U) \ = \ \frac{d(L(U))}{d(L(U(R)))} \ .$$

Regulator bounds I

Since $d(L(U))$ can be explicitly calculated it suffices to determine a lower bound for the regulator $d(L(U(R))) = \mathrm{Reg}_R$ in order to obtain an upper bound for that index.

$$\begin{aligned} \mathrm{Reg}_F \quad \geq \quad & w\,\tfrac{(1+\gamma)(1+2\gamma)}{2}\Gamma(1+\gamma)^{r_1+r_2} \\ & \times\Gamma(3/2+\gamma)^{r_2}\,2^{-r_1-r_2}\pi^{-r_2/2} \\ & \times\exp\Big((-1-\gamma)\Big((r_1+r_2)\tfrac{\Gamma'}{\Gamma}((1+\gamma)/2) \\ & \qquad + r_2\tfrac{\Gamma'}{\Gamma}(1+\gamma/2) + 2/\gamma + 1/(1+\gamma)\Big)\Big)\ . \end{aligned}$$

This estimate is reasonably good for $n \geq 6$ and for small discriminants. The values for γ lie in the interval $]0, 1[$. (Zimmert 1981)

Regulator bounds I

Since $d(L(U))$ can be explicitly calculated it suffices to determine a lower bound for the regulator $d(L(U(R))) = \mathrm{Reg}_R$ in order to obtain an upper bound for that index.

$$\begin{aligned}\mathrm{Reg}_F \quad \geq \quad & w \, \tfrac{(1+\gamma)(1+2\gamma)}{2} \Gamma(1+\gamma)^{r_1+r_2} \\ & \times \Gamma(3/2+\gamma)^{r_2} \, 2^{-r_1-r_2} \pi^{-r_2/2} \\ & \times \exp\big((-1-\gamma)\big((r_1+r_2)\tfrac{\Gamma'}{\Gamma}((1+\gamma)/2) \\ & \qquad\qquad + r_2 \tfrac{\Gamma'}{\Gamma}(1+\gamma/2) \, + \, 2/\gamma + 1/(1+\gamma)\big)\big) \ .\end{aligned}$$

This estimate is reasonably good for $n \geq 6$ and for small discriminants. The values for γ lie in the interval $]0,1[$.
(Zimmert 1981)

Regulator bounds II

An upper bound:

$$\mathrm{Reg}_F \;<\; w\,2^{2-r_1}(2\pi)^{-r_2}\left(\frac{be\log|d_F|}{n-1}\right)^{n-1}\sqrt{|d_F|}$$

for $b = (1+\log\pi/2 + r_2\log 2/n)^{-1}$.
(Siegel 1969)

Let F be primitive. We put $\kappa = 4^{\lfloor n/2\rfloor}$ in case F is totally real, else $\kappa = n^n$. Then we have:

$$\mathrm{Reg}_R \;\geq \left(\left(\frac{3(\log(|d(R)|/\kappa))^2}{(n-1)n(n+1)-6r_2}\right)^r \frac{2^{r_2}}{n\gamma_r^r}\right)^{1/2} \quad .$$

(P 1977)

Examples of regulators

Already for real-quadratic number fields with discriminants of the same size the corresponding values of the regulators Reg_F can differ substantially:

d_F	$4 \cdot 82$	$4 \cdot 83$	$4 \cdot 86$	$4 \cdot 87$
Reg_F	2.8934	5.0998	9.9431	4.0250

d_F	$4 \cdot 9930$	$4 \cdot 9931$	9933	$4 \cdot 9934$
Reg_F	23.8663	189.0783	5.0074	221.3672

Computing regulator bounds I

We choose a constant $K \geq (1+\sqrt{2})n$ and enumerate the set

$$\begin{aligned} S_K \ := \ & \{\alpha \in R \mid T_2(\alpha) < K\} \\ & \cup \{\alpha \in R \mid \alpha^{-1} \in R, T_2(\alpha^{-1}) < K\} . \end{aligned}$$

Obviously, $TU(R)$ is contained in S_K.

Let us also assume that S_K contains k independent units $(0 \leq k \leq r)$.

Computing regulator bounds II

Next we calculate

$$M_i^* = \begin{cases} \min\{C \mid \exists\, \varepsilon_1, \ldots, \varepsilon_i \in U(R) \cap S_K \\ \qquad\qquad \text{indep. with } \sum_{j=1}^n \log^2 |\varepsilon_i^{(j)}| \le C\} \\ \qquad \text{for } 1 \le i \le k \\ K \qquad \text{for } k+1 \le i \le r \end{cases}$$

and then

$$\tilde{M}_i := \frac{n-j}{4} \operatorname{arcosh}^2\left(\frac{M_i^* - j}{n-j}\right) .$$

The rational integer j is to be chosen in the interval $[0, n-2]$ as small as possible.

Computing regulator bounds III

Lemma A unit $\varepsilon \in U_R$ with $T_2(\varepsilon) \geq M_i^*$ and $T_2(\varepsilon^{-1}) \geq M_i^*$ satisfies

$$\sum_{j=1}^{n} \log^2 |\varepsilon^{(j)}| \geq \tilde{M}_i \ .$$

From this we deduce the following lower regulator bound.

Corollary The regulator Reg_R of the order R of F satisfies

$$\mathrm{Reg}_R \geq (\tilde{M}_1 \cdots \tilde{M}_r 2^{r_2} n^{-1} \gamma_r^{-r})^{1/2} \ .$$

Enlarging subgroups I

For this we need to test units of the form ${\varepsilon_0}^{m_0} \cdots {\varepsilon_r}^{m_r}$ with $\varepsilon_0 = \zeta$, whether they are p-th powers for a prime number p smaller than the index of U in $U(R)$.

At first, the elements ε_i are tested. If ε_i is not a p-th power, then the polynomial $t^p - \varepsilon_i \in F[t]$ is irreducible.

According to the Chebotarev Density Theorem there exists a prime ideal $\mathbf{q}$ in o_F which does not contain the discriminant of F and for which $t^p - \varepsilon_i$ remains irreducible in $o_F/\mathbf{q}[t]$.

Enlarging subgroup II

The prime number p must divide $N(\mathbf{q}) - 1$. (Otherwise, there exists $u \in \mathbb{N}$ with $pu \equiv 1 \bmod (N(\mathbf{q}) - 1)$ implying $({\varepsilon_i}^q)^p = \varepsilon_i$ in $o_F/\mathbf{q}$ in contradiction to our choice of $\mathbf{q}$.) It follows that p divides the order of ε_i in $o_F/\mathbf{q}$.

Hence, for $j = i+1, \ldots, r$ there exist unique exponents $\nu_j \in \{0, 1, \ldots, p-1\}$ such that ${\varepsilon_i}^{\nu_j}\varepsilon_j$ is congruent to a p-th power modulo $\mathbf{q}$.

We therefore replace the generating elements ε_j by ${\varepsilon_i}^{\nu_j}\varepsilon_j$ for $(i+1 \leq j \leq r)$, i.e. we set $\tilde{\varepsilon}_i = \varepsilon_i\,,\ \tilde{\varepsilon}_j = {\varepsilon_i}^{\nu_j}\varepsilon_j$.

Enlarging subgroup III

In any equation $\omega^p = \tilde{\varepsilon}_i^{m_i} \cdots \tilde{\varepsilon}_r^{m_r}$ the product $\tilde{\varepsilon}_{i+1}^{m_{i+1}} \cdots \tilde{\varepsilon}_r^{m_r}$ is congruent to a p-th power modulo $\mathbf{q}$. Then also $\tilde{\varepsilon}_i^{m_i}$ must be a p-th power yielding $m_i = 0$.

As a consequence we need to test only, whether $\tilde{\varepsilon}_{i+1}^{m_{i+1}} \cdots \tilde{\varepsilon}_r^{m_r}$ are p-th powers instead of ${\varepsilon_i}^{m_i} \cdots {\varepsilon_r}^{m_r}$.

Applying this idea for $i = 0, 1, ..., r-1$ (respectively $i = 1, ..., r-1$ in the case that ε_0 is itself a p-th power) we reduce the number of necessary tests for p-th powers from roughly p^r to at most $r+1$.

Example I

We let $F = \mathbb{Q}(\rho)$ with $\rho^{19} + 2 = 0$. The Dedekind test implies $o_F = \mathbb{Z}[\rho]$. We put $\omega_i := \rho^{i-1} \ (1 \le i \le 19)$. The discriminant of F is

$$d_F = -19^{19} 2^{18} = -518630842213417245507316350976 \,.$$

With a suitable factor basis and relations we calculate a system of independent units. The corresponding coefficient vectors are

$$\begin{aligned}
\varepsilon_1 &= [-1, 2, -1, -2, -6, 2, -1, 1, -2, -3, -2, 2, 1, 0, -4, 2, 1, 1] \\
\varepsilon_2 &= [-15, 6, 7, -15, 7, 5, -13, 8, 2, -11, 9, 0, -9, 9, -1, -7, 8, -2, -5] \\
\varepsilon_3 &= [-45, 44, -41, 41, -38, 38, -37, 33, -35, 33, -29, 32, -29, \\
&\quad\ 26, -29, 26, -24, 25, -23] \\
\varepsilon_4 &= [-3, -6, -5, -1, 8, 8, 1, -5, -5, -2, -2, 1, 4, 6, 0, -5, -5, -1, 2] \\
\varepsilon_5 &= [-7, 4, -3, -1, 4, -4, 4, -1, -1, 3, -5, 2, 0, -1, 4, -3, 1, -1, -2] \\
\varepsilon_6 &= [17, -38, 0, 31, -18, -21, 26, 5, -29, 8, 23, -19, -13, 24, \\
&\quad\ 1, -23, 10, 18, -16] \\
\varepsilon_7 &= [9, 2, -2, -2, -2, -2, -5, -5, -5, 1, 4, 6, 3, 1, 1, 2, 1, -3, -5] \\
\varepsilon_8 &= [-19, 15, 9, -10, -3, -4, 15, -2, -13, 5, 3, 7, -10, -6, 13, \\
&\quad\ -1, -4, -4, 2] \\
\varepsilon_9 &= [-91, -147, -84, 21, 44, -32, -109, -91, -2, 58, 28, -45, \\
&\quad\ -67, -9, 60, 67, 11, -34, -15]
\end{aligned}$$

Example II

The regulator of that system of independent units is 36273616083.86579.
Via $K = 2T_2(\omega_n)$ we obtain a lower regulator bound 433281.296, hence an upper bound of 83718 for the index.
The enlarging of the subgroup yields fundamental units

$$\begin{array}{lcl}
E_1 & = & [-1, -1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0] \\
E_2 & = & [-1, 1, 0, 0, 0, 0, 0, 0, 0, 0, -1, 0, 0, 0, 0, 0, 0, 0, 0] \\
E_3 & = & [1, -1, 1, 0, 0, 0, 0, 0, 0, 0, 1, -1, 0, 0, 0, 0, 0, 0, 0] \\
E_4 & = & [1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, -1, 0, 0, 0, -1, 0, 0] \\
E_5 & = & [1, -1, 0, -1, 0, -2, 0, 0, 1, 0, 1, 0, 1, 0, 0, -1, 0, -1, 0] \\
E_6 & = & [-1, 1, -1, 0, 1, -1, 0, 1, -1, 0, 1, -1, 0, 1, -1, 0, 1, -1, 0] \\
E_7 & = & [1, -2, 0, 2, -1, -1, 1, 1, -2, 0, 1, -1, -1, 1, 0, -1, 0, 1 - 1] \\
E_8 & = & [-1, 2, 1, -3, 2, -1, -2, 1, 0, -2, 2, -1, -1, 1, -1, -2, 1, -2, -1] \\
E_9 & = & [1, -3, 2, -1, 1, 0, -2, 1, -1, 1, 0, -1, 0, 0, 0, 1 - 1, 0, 0]
\end{array}$$

with regulator 47980973.65927 and exact index

$$(U_F : \langle -1, \varepsilon_1, \ldots, \varepsilon_9 \rangle) = 756 = 2^2\, 3^3\, 7\ .$$

Example of a norm equation

Let $F = \mathbb{Q}(\sqrt{10})$. Its maximal order is $o_F = \mathbb{Z}[\sqrt{10}]$ with fundamental unit $E = 3 + \sqrt{10}$ of norm -1. The ideal $2o_F$ is the square of the prime ideal $\mathbf{p} = \mathbf{2o_F} + \sqrt{\mathbf{10}}\mathbf{o_F}$. We want to check, whether $\mathbf{p}$ is principal. This is done by computing all $\beta \in o_F$ with absolute norm 2. Hence, we need to solve

$$|x^2 - 10y^2| = 2 \ \ (x, y \in \mathbb{Z}) \ .$$

Multiplying β by a suitable power of E we can assume that

$$1 < x + y\sqrt{10} < E \ .$$

Example of a norm equation (cont.)

Combining this inequality with the condition $(x + y\sqrt{10})(x - y\sqrt{10}) = \pm 2$ we obtain lower and upper bounds for y:

$$1 \mp \frac{2}{E} < 2y\sqrt{10} < E \mp \frac{2}{E} \ .$$

Only $y = 1$ satisfies these inequalities. Hence, there is no solution of that norm equation.