ECC summer school, Izmir, 2 September 2016

Class and unit group computations

Razvan Barbulescu
CNRS and IMJ-PRG

Notations

- f in $\mathbb{Z}[x]$ irreducible and monic
- K = the number field of f
- α = a root of f in its number field
- $\mathfrak{q}$ = a prime ideal of K
- h = the class number of K
- R = the regulator of K

Theoretical prerequisites

Theorem (Dirichlet) (10-9)

$\mathcal{O}_K^* \simeq \mu(K) \times \mathbb{Z}^{r+s-1}$ where

- $\mu(K)$ is the group of roots of unity;
- r=number of real embeddingd and s half of the number of complex ones;

Minkowski bound (10-4)

$$h \leq (\frac{\pi}{4})^s \frac{n!}{n^n} |\operatorname{Disc}(K)|^{\frac{1}{2}},$$

where $n = \deg(K)$.

Analytic class number formula (11-5)

$$hR = \#\mu(K) 2^{-r} (2\pi)^{-s} |\operatorname{Disc}(K)|^{\frac{1}{2}} \Pi_p \frac{1 - p^{-1}}{\Pi_{\mathfrak{p}|p}(1 - p^{-f(\mathfrak{p}/p)})}.$$

One can compute an approximation of hR in polynomial time.

Important notions of the algorithm

B-smoothness

Given an integer B and a number field $K = \mathbb{Q}(\alpha)$, the factor base of K with respect to B is

$$\mathcal{F}(B) = \{\mathfrak{q} \text{ prime ideal} \mid \mathrm{N}\,\mathfrak{q} \leq B\}.$$

An element $\phi(\alpha)$ of K is B-smooth if the principal ideal of $\phi(\alpha)$ contains only elements of $\mathcal{F}(B)$.

Exponents group of a parameter B

$$W(B) = \mathrm{Span}\{(\mathrm{val}_{\mathfrak{q}}\, x : \mathfrak{q} \in \mathcal{F}(B)) \mid x \in K^*\}$$

Theorem: For all $B \geq B_0$, $\mathrm{Cl}(K) \simeq \mathbb{Z}^{\#\mathcal{F}(B)}/W(B)$ where

- Minkowski: $B_0 = O(1)|\operatorname{Disc}(K)|^{\frac{1}{2}}$;
- Bach (under GRH): $B_0 = 12(\log \operatorname{Disc}(K))^2$.

Outline of Buchmann's algorithm

Polynomial selection

Given a polynomial in $\mathbb{Q}(x)$, select an other polynomial, f, which defines the same number field (hence of same degree) having the smallest possible norm.

Relation collection (sieve)

Enumerate polynomials $\phi \in \mathbb{Z}[x]$ of degree less than $\deg f$ with $\|\phi\| \leq E$ for a parameter E and collect those such that $\mathrm{Res}(\phi, f)$ is B-smooth for a parameter B.

Linear algebra

- For each relation $\phi(x)$ write

$$\phi(\alpha)\mathcal{O}_K = \prod_{\mathfrak{q} \in \mathcal{F}(B)} \mathfrak{q}^{\mathrm{val}_{\mathfrak{q}} \phi(\alpha)},$$

- Compute the structure of $\mathbb{Z}^{\#\mathcal{F}(B)}/W(B)$ by computing the Smith normal form of its matrix.
- Multiply several ϕ's together to obtain units, and therefore the regulator.

Post-computation

Compute an approximation of hR using analytc methods and hence certify the results.

Polynomial selection : algorithm

- use $\{\omega_i = \alpha^i\}$ or compute a basis $(\omega_i)_{i=1,n}$ of $\mathcal{O}_K$;
- compute the matrix

$$\begin{pmatrix} \sigma_1(\omega_1) & \cdots & \sigma_{r_1}(\omega_1) & \mathrm{Re}(\sigma_{r_1+1}(\omega_1)) & \mathrm{Im}(\sigma_{r_1+1}(\omega_1)) & \cdots & \mathrm{Im}(\sigma_{r_1+r_2}(\omega_1)) \\ \ddots & & & & & & \ddots \\ \sigma_1(\omega_n) & \cdots & \sigma_{r_1}(\omega_n) & \mathrm{Re}(\sigma_{r_1+1}(\omega_n)) & \mathrm{Im}(\sigma_{r_1+1}(\omega_n)) & \cdots & \mathrm{Im}(\sigma_{r_1+r_2}(\omega_n)) \end{pmatrix};$$

- compute several $\mathbb{Z}$-liner combinations of the rows of small L_2-norm;
- for each such linear combination $\lambda_1, \ldots, \lambda_n$ compute

$$\beta = \lambda_1\omega_1 + \cdots + \lambda_n\omega_n$$

and output the minimal polynomial of β.

Polynomial selection : Example (12-1)

Input: $x^3 - 3000x^2 + 3000000x - 999999956$

- $\omega_1 = 1/3\alpha^2 + 2/3\alpha + 1/3$, $\omega_2 = \alpha$, $\omega_3 = 1/2\alpha^2$
- embeddings matrix:

$$\begin{pmatrix} 331648.568664015 & 335176.215667992 & -2043.88367123866 \\ 996.469651664674 & 1001.76517416766 & -3.0573713426004 7 \\ 496475.883344358 & 501762.058327821 & -3062.76813551539 \end{pmatrix}$$

- among the shortest vectors:

$$(-3.53, 1.76, -3.05) = (-3000)L_1 + 2001L_2 + 2000L_3;$$

- $\beta = (-3000)\omega_1 + 2001\omega_2 + 2000\omega_3$ whose minimum polynomial is $x^3 + 44$. Another short vector corresponds to an element δ whose minimal polynomial is $g = x^3 + x^2 - 7x - 13$.

Relation collection : algorithm

Method 1: enumeration

For each polynomial ϕ of degree less than $\deg K$ such that $\|\phi\| \leq E$ compute $\mathrm{Res}(\phi, f)$ and test if it is B-smooth with ECM, whose complexity is sub-exponentially in B and polynomially in the size of input.

Method 2: sieve

For each ideal $\mathfrak{q}$ in $\mathcal{F}(B)$

- compute a basis of elements of K: $(\phi_1(\alpha), \dots, \phi_n(\alpha))$.
- for each linear combination with integer coefficients $(\lambda_1, \dots, \lambda_n)$ such that for all i, $|\lambda_i| \leq E / \mathrm{N}\, q^{\frac{1}{n}}$ mark that $\phi = \lambda_1\phi_1 + \cdots + \lambda_n\phi_n$ is divisible by $\mathfrak{q}$.

Method 3: special-Q sieve

For a few large ideals $\mathfrak{r}$ do the sieve by replacing $\mathfrak{q}$ with $\mathfrak{q}\mathfrak{r}$.

Relation collection : example (12-1) w.r.t. g and $B = 7$

Factor base $\mathcal{F}(7)$

- $\mathfrak{p}_2 = \langle \delta - 3 \rangle$
- $\mathfrak{q}_3 = \langle \delta + 2 \rangle$
- $\mathfrak{p}_3 = \langle -2\delta^2 - 8\delta - 9 \rangle$
- $\mathfrak{p}_5 = \langle -3\delta^2 - 12\delta - 14 \rangle$
- $\mathfrak{q}_5 = \langle 3\delta^2 - 6\delta - 8 \rangle$

For each rational prime less than B we get a so called free relation:

$$\langle 2 \rangle = \mathfrak{p}_2^3 \qquad \langle 3 \rangle = \mathfrak{p}_3^2 \mathfrak{q}_3 \qquad \langle 5 \rangle = \mathfrak{p}_5 \mathfrak{q}_5.$$

Enumeration

We try $\phi(x) = x - k$ for $k = -3, -2, -1, 0, 1, 2, 3$. Classical result: $\mathrm{Res}(x - k, g) = g(k)$.

For example, when $k = -3$ so that $\phi(x) = x + 3$, $\mathrm{Res}(\phi, g) = g(-3) = -10 = -2 \cdot 5$ which is 7-smooth. Then we compute $\langle \delta + 3 \rangle = \mathfrak{p}_2 \mathfrak{p}_5$ wnd deduce a vector of $W(7)$:

$$(\mathrm{val}_{\mathfrak{p}_2}, \mathrm{val}_{\mathfrak{p}_3}, \mathrm{val}_{\mathfrak{q}_3}, \mathrm{val}_{\mathfrak{p}_5}, \mathrm{val}_{\mathfrak{q}_5})(\delta + 3) = (1, 0, 0, 1, 0).$$

Other relations are $\langle \delta + 2 \rangle = \mathfrak{p}_3$, $\langle \delta + 1 \rangle = \mathfrak{p}_2 \mathfrak{p}_3$, $\langle \delta - 1 \rangle = \mathfrak{p}_2 \mathfrak{q}_3^2$, $\langle \delta - 2 \rangle = \mathfrak{p}_3 \mathfrak{p}_5$ and $\langle \delta - 3 \rangle = \mathfrak{p}_2$.

Linear algebra – class group : algorithm

Definition-Theorem: Smith normal form (SNF)

A matrix $A \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ is in Smith normal form if all its entries are 0 except for $d_i = a_{i,i}$ for $i \in \{1, \ldots, \mathrm{rank}(A)\}$ and for each pair $i_1 < i_2$, d_{i_1} divides d_{i_2}. For any matrix A there exists a matrix SNF(A) which is in Smith normal form and two matrices $U \in \mathrm{GL}_m(\mathbb{Z})$ and $V \in \mathrm{GL}_n(\mathbb{Z})$ so that

$$\mathrm{SNF}(A) = UAV.$$

SNF reduction

- find pivot: do gcd's between the entries in the first row to obtain r_1 in the first column, compute its gcd with the entry $a_{2,1}$ and put it in position $(2,1)$; do gcd's in the second row and obtain gcd in position $(2,1)$, compute gcd with $a_{3,1}$ and put it in position $(3,1)$; and repeat with next rows.
- permute rows and columns so that the gcd of the coeffs of the matrix is in position $(1,1)$. Use it to make 0s at all the entries of row 1 and column 1 except $(1,1)$.
- start over with the sublatice of indices $\{2, \ldots, m\} \times \{2, \ldots, n\}$.

Theorem

$\mathbb{Z}^n/\mathrm{Span}(\mathrm{Rows}(A)) \simeq \mathbb{Z}^n/\mathrm{Rows}(\mathrm{SNF}(A)) \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_{\mathrm{rank}(A)}\mathbb{Z}$.

proof: U acts by row combinations and hence keeps $\mathrm{Span}(\mathrm{Rows}(A))$ unchanged. V acts by column combinations on the columns which defines a morphism φ from $\mathbb{Z}^n/\mathrm{Span}(A)$ to $\mathbb{Z}^n/\mathrm{Span}(\mathrm{SNF}(A))$, and U^{-1} defines φ^{-1}.

Linear algebra – class group: ex (12-1)

Input data: relations

$\langle 2\rangle = \mathfrak{p}_2^3$, $\langle 3\rangle = \mathfrak{p}_3^2\mathfrak{q}_3$, $\langle 5\rangle = \mathfrak{p}_5\mathfrak{q}_5$, $\langle \delta+3\rangle = \mathfrak{p}_2\mathfrak{p}_5$, $\langle \delta+2\rangle = \mathfrak{q}_3$, $\langle \delta+1\rangle = \mathfrak{p}_2\mathfrak{p}_3$, $\langle \delta-1\rangle = \mathfrak{p}_2\mathfrak{q}_3^2$, $\langle \delta-2\rangle = \mathfrak{p}_3\mathfrak{p}_5$ and $\langle \delta-3\rangle = \mathfrak{p}_2$.

SNF reducing the matrix

$$\begin{pmatrix} 3 & 0 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Compute the matrix from the exponents, each column corresponds to an ideal: $\mathfrak{p}_2$,$\mathfrak{p}_3$,$\mathfrak{q}_3$,$\mathfrak{p}_5$,$\mathfrak{q}_5$

Linear algebra – class group: ex (12-1)

Input data: relations

$\langle 2\rangle = \mathfrak{p}_2^3$, $\langle 3\rangle = \mathfrak{p}_3^2\mathfrak{q}_3$, $\langle 5\rangle = \mathfrak{p}_5\mathfrak{q}_5$, $\langle \delta+3\rangle = \mathfrak{p}_2\mathfrak{p}_5$, $\langle \delta+2\rangle = \mathfrak{q}_3$, $\langle \delta+1\rangle = \mathfrak{p}_2\mathfrak{p}_3$, $\langle \delta-1\rangle = \mathfrak{p}_2\mathfrak{q}_3^2$, $\langle \delta-2\rangle = \mathfrak{p}_3\mathfrak{p}_5$ and $\langle \delta-3\rangle = \mathfrak{p}_2$.

SNF reducing the matrix

$$\begin{pmatrix} 3 & 0 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 2 & 0 & 0 \\ \boxed{1} & 0 & 0 & 0 & 0 \end{pmatrix}$$

Find an element equal to the gcd of all coeffs: (8,1).

Linear algebra – class group: ex (12-1)

Input data: relations

$\langle 2\rangle = \mathfrak{p}_2^3$, $\langle 3\rangle = \mathfrak{p}_3^2\mathfrak{q}_3$, $\langle 5\rangle = \mathfrak{p}_5\mathfrak{q}_5$, $\langle \delta+3\rangle = \mathfrak{p}_2\mathfrak{p}_5$, $\langle \delta+2\rangle = \mathfrak{q}_3$, $\langle \delta+1\rangle = \mathfrak{p}_2\mathfrak{p}_3$, $\langle \delta-1\rangle = \mathfrak{p}_2\mathfrak{q}_3^2$, $\langle \delta-2\rangle = \mathfrak{p}_3\mathfrak{p}_5$ and $\langle \delta-3\rangle = \mathfrak{p}_2$.

SNF reducing the matrix

$$\begin{pmatrix} \boxed{1} & 0 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Put it in position (1,1) and use it to erase the first row and column.

Linear algebra – class group: ex (12-1)

Input data: relations

$\langle 2\rangle = \mathfrak{p}_2^3$, $\langle 3\rangle = \mathfrak{p}_3^2\mathfrak{q}_3$, $\langle 5\rangle = \mathfrak{p}_5\mathfrak{q}_5$, $\langle \delta+3\rangle = \mathfrak{p}_2\mathfrak{p}_5$, $\langle \delta+2\rangle = \mathfrak{q}_3$, $\langle \delta+1\rangle = \mathfrak{p}_2\mathfrak{p}_3$, $\langle \delta-1\rangle = \mathfrak{p}_2\mathfrak{q}_3^2$, $\langle \delta-2\rangle = \mathfrak{p}_3\mathfrak{p}_5$ and $\langle \delta-3\rangle = \mathfrak{p}_2$.

SNF reducing the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & \boxed{1} & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Find an element equal to the gcd of the elements other than in row 1 and column 1.

Linear algebra – class group: ex (12-1)

Input data: relations

$\langle 2\rangle=\mathfrak{p}_2^3$, $\langle 3\rangle=\mathfrak{p}_3^2\mathfrak{q}_3$, $\langle 5\rangle=\mathfrak{p}_5\mathfrak{q}_5$, $\langle\delta+3\rangle=\mathfrak{p}_2\mathfrak{p}_5$, $\langle\delta+2\rangle=\mathfrak{q}_3$, $\langle\delta+1\rangle=\mathfrak{p}_2\mathfrak{p}_3$, $\langle\delta-1\rangle=\mathfrak{p}_2\mathfrak{q}_3^2$, $\langle\delta-2\rangle=\mathfrak{p}_3\mathfrak{p}_5$ and $\langle\delta-3\rangle=\mathfrak{p}_2$.

SNF reducing the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \boxed{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Put it in position (2,2) and use it to erase row 2 and column 2.

Linear algebra – class group: ex (12-1)

Input data: relations

$\langle 2\rangle = \mathfrak{p}_2^3$, $\langle 3\rangle = \mathfrak{p}_3^2\mathfrak{q}_3$, $\langle 5\rangle = \mathfrak{p}_5\mathfrak{q}_5$, $\langle \delta+3\rangle = \mathfrak{p}_2\mathfrak{p}_5$, $\langle \delta+2\rangle = \mathfrak{q}_3$, $\langle \delta+1\rangle = \mathfrak{p}_2\mathfrak{p}_3$, $\langle \delta-1\rangle = \mathfrak{p}_2\mathfrak{q}_3^2$, $\langle \delta-2\rangle = \mathfrak{p}_3\mathfrak{p}_5$ and $\langle \delta-3\rangle = \mathfrak{p}_2$.

SNF reducing the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \boxed{1} & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Find an element equal to the gcd of the elements in rows ≥ 3 and columns ≥ 3.

Linear algebra – class group: ex (12-1)

Input data: relations

$\langle 2\rangle = \mathfrak{p}_2^3$, $\langle 3\rangle = \mathfrak{p}_3^2\mathfrak{q}_3$, $\langle 5\rangle = \mathfrak{p}_5\mathfrak{q}_5$, $\langle \delta+3\rangle = \mathfrak{p}_2\mathfrak{p}_5$, $\langle \delta+2\rangle = \mathfrak{q}_3$, $\langle \delta+1\rangle = \mathfrak{p}_2\mathfrak{p}_3$,
$\langle \delta-1\rangle = \mathfrak{p}_2\mathfrak{q}_3^2$, $\langle \delta-2\rangle = \mathfrak{p}_3\mathfrak{p}_5$ and $\langle \delta-3\rangle = \mathfrak{p}_2$.

SNF reducing the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & \boxed{1} & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Put it in position (3,3) and use it to erase row 3 and column 3.

Linear algebra – class group: ex (12-1)

Input data: relations

$\langle 2\rangle = \mathfrak{p}_2^3$, $\langle 3\rangle = \mathfrak{p}_3^2\mathfrak{q}_3$, $\langle 5\rangle = \mathfrak{p}_5\mathfrak{q}_5$, $\langle \delta+3\rangle = \mathfrak{p}_2\mathfrak{p}_5$, $\langle \delta+2\rangle = \mathfrak{q}_3$, $\langle \delta+1\rangle = \mathfrak{p}_2\mathfrak{p}_3$, $\langle \delta-1\rangle = \mathfrak{p}_2\mathfrak{q}_3^2$, $\langle \delta-2\rangle = \mathfrak{p}_3\mathfrak{p}_5$ and $\langle \delta-3\rangle = \mathfrak{p}_2$.

SNF reducing the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \boxed{1} & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Find an element equal to the gcd of the elements in rows ≥ 4 and columns ≥ 3.

Linear algebra – class group: ex (12-1)

Input data: relations

$\langle 2\rangle = \mathfrak{p}_2^3$, $\langle 3\rangle = \mathfrak{p}_3^2\mathfrak{q}_3$, $\langle 5\rangle = \mathfrak{p}_5\mathfrak{q}_5$, $\langle \delta+3\rangle = \mathfrak{p}_2\mathfrak{p}_5$, $\langle \delta+2\rangle = \mathfrak{q}_3$, $\langle \delta+1\rangle = \mathfrak{p}_2\mathfrak{p}_3$, $\langle \delta-1\rangle = \mathfrak{p}_2\mathfrak{q}_3^2$, $\langle \delta-2\rangle = \mathfrak{p}_3\mathfrak{p}_5$ and $\langle \delta-3\rangle = \mathfrak{p}_2$.

SNF reducing the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \boxed{1} & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Put it in position (4,4) and use it to erase row 4 and column 4.

Linear algebra – class group: ex (12-1)

Input data: relations

$\langle 2\rangle = \mathfrak{p}_2^3$, $\langle 3\rangle = \mathfrak{p}_3^2\mathfrak{q}_3$, $\langle 5\rangle = \mathfrak{p}_5\mathfrak{q}_5$, $\langle \delta+3\rangle = \mathfrak{p}_2\mathfrak{p}_5$, $\langle \delta+2\rangle = \mathfrak{q}_3$, $\langle \delta+1\rangle = \mathfrak{p}_2\mathfrak{p}_3$, $\langle \delta-1\rangle = \mathfrak{p}_2\mathfrak{q}_3^2$, $\langle \delta-2\rangle = \mathfrak{p}_3\mathfrak{p}_5$ and $\langle \delta-3\rangle = \mathfrak{p}_2$.

SNF reducing the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \boxed{1} \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Find an element equal to the gcd of the elements in rows ≥ 5 and columns ≥ 5.

Linear algebra – class group: ex (12-1)

Input data: relations

$\langle 2\rangle = \mathfrak{p}_2^3$, $\langle 3\rangle = \mathfrak{p}_3^2\mathfrak{q}_3$, $\langle 5\rangle = \mathfrak{p}_5\mathfrak{q}_5$, $\langle \delta+3\rangle = \mathfrak{p}_2\mathfrak{p}_5$, $\langle \delta+2\rangle = \mathfrak{q}_3$, $\langle \delta+1\rangle = \mathfrak{p}_2\mathfrak{p}_3$, $\langle \delta-1\rangle = \mathfrak{p}_2\mathfrak{q}_3^2$, $\langle \delta-2\rangle = \mathfrak{p}_3\mathfrak{p}_5$ and $\langle \delta-3\rangle = \mathfrak{p}_2$.

SNF reducing the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & \boxed{1} \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Put it in position (5,5) and multiply row 5 by (-1).

Linear algebra – class group: ex (12-1)

Input data: relations

$\langle 2\rangle = \mathfrak{p}_2^3$, $\langle 3\rangle = \mathfrak{p}_3^2\mathfrak{q}_3$, $\langle 5\rangle = \mathfrak{p}_5\mathfrak{q}_5$, $\langle \delta+3\rangle = \mathfrak{p}_2\mathfrak{p}_5$, $\langle \delta+2\rangle = \mathfrak{q}_3$, $\langle \delta+1\rangle = \mathfrak{p}_2\mathfrak{p}_3$, $\langle \delta-1\rangle = \mathfrak{p}_2\mathfrak{q}_3^2$, $\langle \delta-2\rangle = \mathfrak{p}_3\mathfrak{p}_5$ and $\langle \delta-3\rangle = \mathfrak{p}_2$.

SNF reducing the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

The **class group** is isomorphic to $\mathbb{Z}/1 \times \mathbb{Z}/1 \times \mathbb{Z}/1 \times \mathbb{Z}/1 \times \mathbb{Z}/1$ which is the trivial group.

Linear algebra – units: algorithm (part 1/2)

Definition-Theorem: (Hermit normal form)

A matrix $A \in \mathrm{Mat}(m, n, \mathbb{Z})$ is in Hermite normal form (HNF) if there exist $r \leq n$ and a strictly increasing map $f : \{r+1, \ldots, n\} \to \{1, 2, \ldots, m\}$ such that the first r columns are zero for all pairs (i, j):

- $a_{f(j)i, f(i)} > 0$;
- $a_{i,j} = 0$ if $i < f(j)$;
- $a_{i,j} \in [0, a_{f(j),j} - 1]$ if $j > i$.

Every matrix A admits a unique matrix HNF(A) which is in HNF so that there exists $U \in \mathrm{GL}_n(\mathbb{Z})$ and HNF(A)=UA.
The $\mathbb{Z}$-module of vectors v in $\mathbb{Z}^m$ so that $vA = 0$ is generated by the first r columns of U.

Algorithm: HNF reduction

1. - we can assume the last row non-zero because otherwise we can forget about it; do elementary transformations on the columns so that the gcd of the elements in the last row is contained at position (m, n);
   - use the element in position (m, n) to erase row m
   - start ober with the sub-matrix in positions of indices $i \leq m-1$ and $j \leq n-1$.
2. for each row use the left-most non-zero element to reduce the elements at its right.

Linear algebra – units (part 1/2): ex (12-1)

HNF reducing the matrix

$$\begin{pmatrix} 3 & 0 & 0 & 1 & 0 & 1 \\ 0 & 2 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ \hline 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

We transpose the matrix so that we can compute a left kernel. In order to determine U we write identity under the matrix.

Linear algebra – units (part 1/2): ex (12-1)

HNF reducing the matrix

$$\begin{pmatrix} 3 & 0 & 0 & 1 & 0 & 1 \\ 0 & 2 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & \boxed{1} & 0 & 0 & 0 \\ \hline 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Find a gcd of the row 5.

Linear algebra – units (part 1/2): ex (12-1)

HNF reducing the matrix

$$\begin{pmatrix} 3 & 0 & 1 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & \boxed{1} \\ \hline 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Put it in the left-down corner and erase entries at its left side.

Linear algebra – units (part 1/2): ex (12-1)

HNF reducing the matrix

$$\begin{pmatrix} 3 & 0 & 1 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \boxed{1} & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Find a gcd of the row 4.

Linear algebra – units (part 1/2): ex (12-1)

HNF reducing the matrix

$$\begin{pmatrix} 3 & 0 & 1 & 0 & 1 & 0 \\ 0 & 2 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \boxed{1} & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Put it in position (4,5) and erase entries at its left side.

Linear algebra – units (part 1/2): ex (12-1)

HNF reducing the matrix

$$\begin{pmatrix} 3 & 0 & 1 & 0 & 1 & 0 \\ 0 & 2 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & \boxed{1} & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Find a gcd of the row 3.

Linear algebra – units (part 1/2): ex (12-1)

HNF reducing the matrix

$$\begin{pmatrix} 3 & 0 & 1 & 0 & 1 & 0 \\ 0 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & \boxed{1} & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Put it in position (3,4) and erase entries at its left side.

Linear algebra – units (part 1/2): ex (12-1)

HNF reducing the matrix

$$\begin{pmatrix} 3 & 0 & 1 & 0 & 1 & 0 \\ 0 & 2 & \boxed{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Find a gcd of the row 2.

Linear algebra – units (part 1/2): ex (12-1)

HNF reducing the matrix

$$\begin{pmatrix} 3 & -2 & 1 & 0 & 1 & 0 \\ 0 & 0 & \boxed{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 & 0 & 0 \\ 0 & -2 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Put it in position (2,3) and erase entries at its left side.

Linear algebra – units (part 1/2): ex (12-1)

HNF reducing the matrix

$$\left(\begin{array}{cccccc} 3 & \boxed{1} & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ \hline 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 & 0 & 0 \\ 0 & -2 & 1 & 0 & 0 & 0 \end{array}\right)$$

Find a gcd of the row 1.

Linear algebra – units (part 1/2): ex (12-1)

HNF reducing the matrix

$$\left(\begin{array}{cccccc} 0 & \boxed{1} & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ \hline -2 & 1 & 0 & 0 & 0 & 0 \\ -3 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 3 & -1 & 0 & 1 & 0 & 0 \\ 6 & -2 & 1 & 0 & 0 & 0 \end{array}\right)$$

Put it in position (1,2) and erase entries at its left side.

Linear algebra – units (part 1/2): ex (12-1)

HNF reducing the matrix

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ \hline -2 & 1 & -1 & 0 & -1 & 1 \\ -3 & 1 & -1 & 0 & -1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & -1 \\ 3 & -1 & 1 & 1 & 1 & -1 \\ 6 & -2 & 2 & 0 & 2 & -2 \end{pmatrix}$$

Use left-most entry of each row to reduce the entries on its right side.

Linear algebra – units (part 1/2): ex (12-1)

HNF reducing the matrix

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ \hline -2 & 1 & -1 & 0 & -1 & 1 \\ -3 & 1 & -1 & 0 & -1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & -1 \\ 3 & -1 & 1 & 1 & 1 & -1 \\ 6 & -2 & 2 & 0 & 2 & -2 \end{pmatrix}$$

The first column of the transformation matrix generates the left kernel.

Linear algebra – units (part 2/2): algorithm

System of generators

Using the left kernal obtain a set of units. One can estimate the number of relations required before this set of units is a system of generators of $\mathcal{O}_K^*$: $\varepsilon_1, \ldots, \varepsilon_k$.

Remark One cannot always extract a basis from a system of generators of a $\mathbb{Z}$-module, e.g. $\{2, 3\}$ generate $\mathbb{Z}$.

Log-unit matrix

Using the embeddings σ_i into $\mathbb{C}$, compute the matrix

$$L = \begin{pmatrix} \log(\sigma_1(\varepsilon_1)) & \cdots & \log(\sigma_1(\varepsilon_k)) \\ \vdots & & \vdots \\ \log(\sigma_n(\varepsilon_1)) & \cdots & \log(\sigma_n(\varepsilon_k)) \end{pmatrix}$$

at a precision which is large enough, depending on an approximative lower bound R found from the Minkowski bound and the analytic formula.

HNF reduction

One modifies the HNF algorithm so that the relation "a is divisible by b" is replaed by "the fractional part of a/b is upper bounded by a threshold". The modified HNF on L computes a system of fundamental units. Their minor in HNF(L) is the **regulator**.

Linear algebra – units (part 2/2): ex (12-1)

System of generators

Recall the relations: $\langle 2\rangle = \mathfrak{p}_2^3$, $\langle 3\rangle = \mathfrak{p}_3^2\mathfrak{q}_3$, $\langle 5\rangle = \mathfrak{p}_5\mathfrak{q}_5$, $\langle \delta+3\rangle = \mathfrak{p}_2\mathfrak{p}_5$, $\langle \delta+2\rangle = \mathfrak{q}_3$, $\langle \delta+1\rangle = \mathfrak{p}_2\mathfrak{p}_3$. Recall the generator of the left kernel: $(-2,-3,0,3,6)$. Then we obtain the unit

$$\varepsilon = 2^{-2}3^{-3}(\delta+2)^3(\delta+1)^6.$$

Log-unit matrix

$$\begin{pmatrix}\log|\sigma_1(\varepsilon)|\\ \log|\sigma_2(\varepsilon)|\end{pmatrix} = \begin{pmatrix}8.29\\ -8.29\end{pmatrix}$$

Hence the probable regulator is 8.29.

Certify

Algorithm

Compute hR using the analytic formula and compare with the probable value.

Example (12-1)

$hR \approx 8.29$. We computed $h = 1$ an the probable regulator 8.29. Since we have equality, ϵ is a fundamental unit so that $\mathcal{O}_K^* = \langle -1 \rangle \langle \varepsilon \rangle$.