Algebraic number theory **LTCC 2008**

Solutions to Problem Sheet 1

(1) If α is algebraic over $\mathbb{Q}$ then α satisfies an equation of the form

$$\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = 0$$

where $c_0, c_1, \ldots, c_{n-1} \in \mathbb{Q}$. Since $\alpha \neq 0$, we can assume that $c_0 \neq 0$. Multiplying the equation by $c_0^{-1}\alpha^{-n}$ gives

$$c_0^{-1} + c_0^{-1}c_{n-1}\alpha^{-1} + \cdots + c_0^{-1}c_1(\alpha^{-1})^{n-1} + (\alpha^{-1})^n = 0,$$

which shows that α^{-1} is algebraic over $\mathbb{Q}$.

(2) Since $\alpha \in K$ and K is an algebraic number field, it follows that α is algebraic over $\mathbb{Q}$ and therefore satisfies an equation of the form

$$\alpha^d + c_{d-1}\alpha^{d-1} + \cdots + c_1\alpha + c_0 = 0$$

where $c_0, c_1, \ldots, c_{d-1} \in \mathbb{Q}$. Let $n \in \mathbb{N}$ be a common denominator of the c_i, i.e. $nc_0, nc_1, \ldots, nc_{d-1} \in \mathbb{Z}$. Multiplying the equation by n^d gives

$$(n\alpha)^d + c_{d-1}n(n\alpha)^{d-1} + \cdots + c_1n^{d-1}(n\alpha) + c_0n^d = 0.$$

Since $c_{d-1}n, \ldots, c_1n^{d-1}, c_0n^d \in \mathbb{Z}$, this shows that $n\alpha$ is integral over $\mathbb{Z}$, i.e. $n\alpha \in R_K$.

(3) We assume that $m \neq 1$ is a square-free integer such that $m \equiv 1 \pmod 4$. Let $K = \mathbb{Q}(\sqrt{m})$ and R_K the ring of integers of K.

If $\alpha \in \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{m}}{2}$ then $\alpha = a + b\frac{1+\sqrt{m}}{2}$ with $a, b \in \mathbb{Z}$. One easily checks that α is a root of the monic polynomial

$$X^2 - (2a+b)X + \left(a^2 + ab + b^2\frac{1-m}{4}\right),$$

and the assumption $m \equiv 1 \pmod 4$ implies that the coefficients of this polynomial are in $\mathbb{Z}$. This shows that $\alpha \in R_K$.

Conversely assume that $\alpha \in R_K$. Write $\alpha = a + b\sqrt{m}$ with $a, b \in \mathbb{Q}$. Then as in the case $m \not\equiv 1 \pmod 4$ it follows that $2a = \alpha + \tau(\alpha) \in R_K \cap \mathbb{Q} = \mathbb{Z}$ and $a^2 - mb^2 = \alpha\tau(\alpha) \in R_K \cap \mathbb{Q} = \mathbb{Z}$.

If $a \in \mathbb{Z}$ then $mb^2 \in \mathbb{Z}$ which implies $b \in \mathbb{Z}$ because m is square-free, so $\alpha = a + b\sqrt{m} = (a-b) + 2b\frac{1+\sqrt{m}}{2} \in \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{m}}{2}$.

If $a \notin \mathbb{Z}$ then $a = c/2$ with $c \in \mathbb{Z}$ odd, so $c^2 \equiv 1 \pmod 4$. From $(c/2)^2 - mb^2 \in \mathbb{Z}$ it follows that $c^2 - m(2b)^2 \in \mathbb{Z}$ and moreover $c^2 - m(2b)^2 \equiv 0 \pmod 4$. Now $m(2b)^2 \in \mathbb{Z}$ implies $2b \in \mathbb{Z}$ because m is square-free. The congruences $c^2 - m(2b)^2 \equiv 0 \pmod 4$, $c^2 \equiv 1 \pmod 4$ and $m \equiv 1 \pmod 4$ imply that $(2b)^2 \equiv 1 \pmod 4$, so $2b$ is odd. Since c and $2b$ are odd, it follows that $a - b = \frac{c-2b}{2}$ is an integer. Therefore $\alpha = a + b\sqrt{m} = (a-b) + 2b\frac{1+\sqrt{m}}{2} \in \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{m}}{2}$.

(4) Suppose that A is a prime ideal and that I, J are ideals such that $IJ \subseteq A$. If $I \subseteq A$ we are finished. So suppose that $I \not\subseteq A$, i.e. there exits $\alpha \in I \setminus A$. Now if $\beta \in J$ then $\alpha\beta \in IJ \subseteq A$, hence $\alpha \in A$ or $\beta \in A$ since A is prime. Since $\alpha \notin A$, it follows that $\beta \in A$. Hence $J \subseteq A$.

Conversely assume that A is an ideal that has the property that $IJ \subseteq A$ implies $I \subseteq A$ or $J \subseteq A$. Let $\alpha, \beta \in R$ be such that $\alpha\beta \in A$. Then $(\alpha\beta) \subseteq A$. But $(\alpha\beta) = (\alpha)(\beta)$, so $(\alpha) \subseteq A$ or $(\beta) \subseteq A$. Hence $\alpha \in A$ or $\beta \in A$. This shows that A is a prime ideal.

(5) Step 1: $A^2 = (9, 7+\sqrt{-14})$.

We have

$$\begin{aligned} A^2 &= \big(3\cdot 3, 3\cdot(1+\sqrt{-14}), (1+\sqrt{-14})\cdot(1+\sqrt{-14})\big) \\ &= (9, 3+3\sqrt{-14}, -13+2\sqrt{-14}). \end{aligned}$$

From this we see that

$$\begin{aligned} 9 &= 1\cdot 9 + 0\cdot(3+3\sqrt{-14}) + 0\cdot(-13+2\sqrt{-14}) \in A^2, \\ 7+\sqrt{-14} &= (-1)\cdot 9 + 1\cdot(3+3\sqrt{-14}) + (-1)\cdot(-13+2\sqrt{-14}) \in A^2, \end{aligned}$$

hence $(9, 7+\sqrt{-14}) \subseteq A^2$. Conversely, we have

$$\begin{aligned} 9 &= 1\cdot 9 + 0\cdot(7+\sqrt{-14}) \in (9, 7+\sqrt{-14}), \\ 3+3\sqrt{-14} &= (-2)\cdot 9 + 3\cdot(7+\sqrt{-14}) \in (9, 7+\sqrt{-14}), \\ -13+2\sqrt{-14} &= (-3)\cdot 9 + 2\cdot(7+\sqrt{-14}) \in (9, 7+\sqrt{-14}), \end{aligned}$$

hence $A^2 \subseteq (9, 7+\sqrt{-14})$.

Step 2: $A^4 = (5+2\sqrt{-14})$.

We have

$$\begin{aligned} A^4 &= \big(9\cdot 9, 9\cdot(7+\sqrt{-14}), (7+\sqrt{-14})\cdot(7+\sqrt{-14})\big) \\ &= (81, 63+9\sqrt{-14}, 35+14\sqrt{-14}). \end{aligned}$$

From this we see that

$$5+2\sqrt{-14} = 3\cdot 81 + (-6)\cdot(63+9\sqrt{-14}) + 4\cdot(35+14\sqrt{-14}) \in A^4,$$

hence $(5+2\sqrt{-14}) \subseteq A^4$. Conversely, we have

$$\begin{aligned} 81 &= (5-2\sqrt{-14})\cdot(5+2\sqrt{-14}) \in (5+2\sqrt{-14}), \\ 63+9\sqrt{-14} &= (7-\sqrt{-14})\cdot(5+2\sqrt{-14}) \in (5+2\sqrt{-14}), \\ 35+14\sqrt{-14} &= 7\cdot(5+2\sqrt{-14}) \in (5+2\sqrt{-14}), \end{aligned}$$

hence $A^4 \subseteq (5+2\sqrt{-14})$.

Step 3: A^2 is not principal.

We define the norm of $\alpha = a+b\sqrt{-14}$ (with $a, b \in \mathbb{Q}$) by $N\alpha = a^2+14b^2$. Then $N(\alpha\beta) = N\alpha \cdot N\beta$ (easy computation), and $N\alpha \in \mathbb{N}$ if $\alpha \in R_K \setminus \{0\}$.

Now suppose that $A^2 = (\alpha)$ with $\alpha \in R_K = \mathbb{Z}+\mathbb{Z}\sqrt{-14}$. Then $9 \in (\alpha)$ implies that $9 = \lambda\alpha$ for some $\lambda \in R_K$, hence $81 = N(9) = N\lambda \cdot N\alpha$ which shows that $N\alpha \mid 81$. Similarly $7+\sqrt{-14} \in (\alpha)$ implies $N\alpha \mid N(7+\sqrt{-14}) = 63$. This shows that $N\alpha = 1, 3$ or 9. Write $\alpha = a+b\sqrt{-14}$ with $a, b \in \mathbb{Z}$. Then $N\alpha = a^2+14b^2$, so clearly $N\alpha = 3$ is impossible. If $N\alpha = 9$ then $\alpha = \pm 3$. But clearly $7+\sqrt{-14} \notin (\pm 3)$, so $N\alpha = 9$ is impossible. Finally if $N\alpha = 1$ then $\alpha = \pm 1$ and therefore $1 \in (\pm 1) = A^2 = (9, 7+\sqrt{-14})$. So there exist $v, w, x, y \in \mathbb{Z}$ such that

$$\begin{aligned} 1 &= (v+w\sqrt{-14})\cdot 9 + (x+y\sqrt{-14})\cdot(7+\sqrt{-14}) \\ &= (9v+7x-14y) + (9w+x+7y)\sqrt{-14}. \end{aligned}$$

Now $9v+7x-14y = 1$ and $9w+x+7y = 0$ imply $1 = (9v+7x-14y)+2\cdot(9w+x+7y) = 9\cdot(v+2w+x)$ which is impossible. Hence the case $N\alpha = 1$ is impossible. This completes the proof that there is no $\alpha \in R_K$ such that $A^2 = (\alpha)$.

Step 4: h_K is divisible by 4.

Let $[A]$ denote the class of the (fractional) ideal A in the class group $\mathrm{Cl}(K)$. By Step 2 the ideal A^4 is principal, thus $[A]^4 = [A^4]$ is the identity element in $\mathrm{Cl}(K)$. It follows that the order of $[A]$ in $\mathrm{Cl}(K)$ divides 4. But Step 2 shows that the ideal A^2 is not principal which implies that $[A]$ and $[A]^2 = [A^2]$ are not the identity element in $\mathrm{Cl}(K)$. Hence $[A]$ has order 4 in $\mathrm{Cl}(K)$, and this implies that $h_K = |\mathrm{Cl}(K)|$ is divisible by 4.

(6) Clearly $\{1, -1, \sqrt{-1}, -\sqrt{-1}\} \subseteq \mu_{\mathbb{Q}(\sqrt{-1})}$.

Conversely assume that $\zeta \in \mu_{\mathbb{Q}(\sqrt{-1})}$. Then $\zeta \in R_{\mathbb{Q}(\sqrt{-1})}$ since ζ satisfies a polynomial equation of the form $X^e - 1 = 0$. So we can write $\zeta = a + b\sqrt{-1}$ with $a, b \in \mathbb{Z}$. Now $\zeta^e = 1$ implies $|\zeta|^e = 1$ where $|\zeta| = \sqrt{a^2 + b^2}$ is the usual absolute value of the complex number ζ, therefore $|\zeta| = 1$. So $a^2 + b^2 = 1$ and hence either $a = \pm 1$ and $b = 0$ which gives $\zeta = \pm 1$, or $a = 0$ and $b = \pm 1$ which gives $\zeta = \pm\sqrt{-1}$. This shows $\mu_{\mathbb{Q}(\sqrt{-1})} \subseteq \{1, -1, \sqrt{-1}, -\sqrt{-1}\}$.

(7) If $K = \mathbb{Q}(\sqrt{m})$ for a square-free integer $m > 1$, then K is a real quadratic field, so K has two real embeddings and no complex embeddings, and $\mu_K = \{\pm 1\}$. Therefore by Dirichlet's unit theorem $R_K^\times \cong \{\pm 1\} \times \mathbb{Z}$. A unit $\varepsilon \in R_K^\times$ is a fundamental unit if and only if it is mapped to a generator of the torsion free quotient $R_K^\times / \mu_K \cong (\{\pm 1\} \times \mathbb{Z})/\{\pm 1\} \cong \mathbb{Z}$. It follows that there exist precisely four fundamental units: if ε is one fundamental unit, then the other three fundamental units are $-\varepsilon$, ε^{-1} and $-\varepsilon^{-1}$.

Now let $\varepsilon = x + y\sqrt{m}$ with $x, y \in \mathbb{Q}$ be a fundamental unit of $R_K^\times$. Clearly we must have $x \neq 0$ and $y \neq 0$. By Lemma 6.9 we know that $N(\varepsilon) = (x + y\sqrt{m})(x - y\sqrt{m}) = \pm 1$, so $\varepsilon^{-1} = (x + y\sqrt{m})^{-1} = (\pm x) + (\mp y)\sqrt{m}$. But it is clear that of the four fundamental unit $\varepsilon = x + y\sqrt{m}$, $-\varepsilon = (-x) + (-y)\sqrt{m}$, $\varepsilon^{-1} = (\pm x) + (\mp y)\sqrt{m}$ and $-\varepsilon^{-1} = (\mp x) + (\pm y)\sqrt{m}$ precisely one is of the form $a + b\sqrt{m}$ with $a > 0$ and $b > 0$.

If $\varepsilon = a + b\sqrt{m}$ is a fundamental unit with $a, b > 0$ and $\varepsilon^i = x + y\sqrt{m}$ with $i \geq 2$, then obviously $x > a$ and $y > b$. Hence the fundamental unit ε can be characterised as the element with minimal a among all units $a + b\sqrt{m}$ for which a and b are positive. Therefore we can find ε by systematically trying $a = 1, 2, 3, \ldots$ (if $m \not\equiv 1 \pmod 4$) or $a = \frac{1}{2}, \frac{2}{2}, \frac{3}{2}, \ldots$ (if $m \equiv 1 \pmod 4$) until we find an a for which there exists an b such that $a + b\sqrt{m} \in R_{\mathbb{Q}(\sqrt{m})}^\times$. Note that $a + b\sqrt{m} \in R_{\mathbb{Q}(\sqrt{m})}^\times$ implies $N(a + b\sqrt{m}) = a^2 - mb^2 = \pm 1$, so it is easy to test whether such a b exists.

In the case $m = 7 \not\equiv 1 \pmod 4$ we have $R_{\mathbb{Q}(\sqrt{7})} = \mathbb{Z} + \mathbb{Z}\sqrt{7}$. We try $a = 1, 2, 3, \ldots$, and for each a we then test whether $a^2 - 7b^2 = \pm 1$ has a solution $b \in \mathbb{N}$, i.e. whether $(a^2 \mp 1)/7$ is a square of a positive integer. The first time this is the case is for $a = 8$ where we find $(8^2 - 1)/7 = 3^2$. Hence $\varepsilon = 8 + 3\sqrt{7}$ is a fundamental unit of $\mathbb{Q}(\sqrt{7})$.

Remark: There exists a much more efficient algorithm to find fundamental units of real quadratic fields by using continued fractions. For details see for example §5.7 in H. Cohen: *A course in computational algebraic number theory*, Springer, 1993.

(8) Choice of $(r + s - 1) \times (r + s - 1)$-minor:

Let $v_1, \ldots, v_{r+s}$ denote the rows of the matrix in Definition 6.12. We must show that the absolute value of the determinant of the matrix which is obtained by omitting the i-th row is independent of i. Recall from the proof of Lemma 6.10 that for every unit α we have

$$\log|\sigma_1(\alpha)| + \cdots + \log|\sigma_r(\alpha)| + 2\log|\sigma_{r+1}(\alpha)| + \cdots + 2\log|\sigma_{r+s}(\alpha)| = 0.$$

Hence $v_1 + \cdots + v_{r+s} = (0, \ldots, 0)$. Therefore for every $i = 1, \ldots, r+s-1$ we have

$$\begin{aligned}
\det \begin{pmatrix} v_1 \\ \vdots \\ v_{i-1} \\ v_{i+1} \\ \vdots \\ v_{r+s-1} \\ v_{r+s} \end{pmatrix} &= \det \begin{pmatrix} v_1 \\ \vdots \\ v_{i-1} \\ v_{i+1} \\ \vdots \\ v_{r+s-1} \\ -v_1 - \cdots - v_{r+s-1} \end{pmatrix} \\
&= \det \begin{pmatrix} v_1 \\ \vdots \\ v_{i-1} \\ v_{i+1} \\ \vdots \\ v_{r+s-1} \\ -v_i \end{pmatrix} \\
&= \pm \det \begin{pmatrix} v_1 \\ \vdots \\ v_{r+s-1} \end{pmatrix}.
\end{aligned}$$

This shows that the absolute value of this determinant is independent of i. Hence the definition of the regulator does not depend on the choice of $(r+s-1) \times (r+s-1)$-minor.

Choice of order of the embeddings:
Changing the order of the embeddings only permutes the rows of the matrix, therefore the absolute value of the determinant of an $(r+s-1) \times (r+s-1)$-submatrix does not change.

Choice (and order) of fundamental units:
Suppose that $\beta_1, \ldots, \beta_{r+s-1}$ is another system of fundamental units for $R_K^\times$. Then $\lambda(\alpha_1), \ldots, \lambda(\alpha_{r+s-1})$ and $\lambda(\beta_1), \ldots, \lambda(\beta_{r+s-1})$ are both $\mathbb{Z}$-bases of the free abelian group $\lambda(R_K^\times)$. Therefore we have $\lambda(\beta_j) = \sum_{i=1}^{r+s-1} \lambda(\alpha_i) c_{ij}$ with $c_{ij} \in \mathbb{Z}$. If C denotes the matrix $(c_{ij})_{1 \le i,j \le r+s-1}$ then

$$(\lambda(\beta_1), \ldots, \lambda(\beta_{r+s-1})) = (\lambda(\alpha_1), \ldots, \lambda(\alpha_{r+s-1})) \cdot C.$$

Similarly

$$(\lambda(\alpha_1), \ldots, \lambda(\alpha_{r+s-1})) = (\lambda(\beta_1), \ldots, \lambda(\beta_{r+s-1})) \cdot D$$

for an $(r+s-1) \times (r+s-1)$-matrix D with entries in $\mathbb{Z}$. It follows that CD is equal to the $(r+s-1) \times (r+s-1)$ unit matrix. In particular $\det(C) \det(D) = 1$, so $\det(C) = \pm 1$ since these determinants are integers. Now the equation

$$(\lambda(\beta_1), \ldots, \lambda(\beta_{r+s-1})) = (\lambda(\alpha_1), \ldots, \lambda(\alpha_{r+s-1})) \cdot C.$$

shows that an $(r+s-1) \times (r+s-1)$-minor of the matrix with columns $\lambda(\beta_1), \ldots, \lambda(\beta_{r+s-1})$ is equal to $\det(C)$ times an $(r+s-1) \times (r+s-1)$-minor of the matrix with columns $\lambda(\alpha_1), \ldots \lambda(\alpha_{r+s-1})$. Hence the absolute values of these minors are equal. This shows that the definition of the regulator does not depend on the choice of system of fundamental units.