Algebraic number theory
Solutions to exercise sheet for chapter 5

Nicolas Mascot (n.a.v.mascot@warwick.ac.uk)
Aurel Page (a.r.page@warwick.ac.uk)
TA: Pedro Lemos (lemos.pj@gmail.com)

Version: March 2, 2017

Exercise 1. *Let $K = \mathbb{Q}(\sqrt{21})$.*

1. *Let $u = 55 + 12\sqrt{21}$. Prove that $u \in \mathbb{Z}_K^\times$.*

   We have $u \in \mathbb{Z}[\sqrt{21}] \subset \mathbb{Z}_K$. In addition, $N_\mathbb{Q}^K(u) = 55^2 - 21 \cdot 12^2 = 1$, so $u \in \mathbb{Z}_K^\times$.

2. *Is u a fundamental unit of $\mathbb{Z}_K^\times$?*

   Since 21 is squarefree and $21 \equiv 1 \pmod 4$, the ring of integers of K is $\mathbb{Z}[\alpha]$ where $\alpha = \frac{1+\sqrt{21}}{2}$. More precisely,

   $$\mathbb{Z}_K = \mathbb{Z}[\alpha] = \mathbb{Z} \cdot 1 \oplus \mathbb{Z} \cdot \frac{1+\sqrt{21}}{2} = \left\{ \frac{x + y\sqrt{21}}{2}, \ x, y \in \mathbb{Z}, x + y \text{ even} \right\}.$$

   We have $N_\mathbb{Q}^K\left(\frac{x+y\sqrt{21}}{2}\right) = \frac{1}{2^2} N_\mathbb{Q}^K(x + y\sqrt{21}) = \frac{x^2-21y^2}{4}$, so we look for a fundamental unit in $\mathbb{Z}_K$ by computing the smallest solution to $x^2 - 21y^2 = \pm 4$ with $x, y \in \mathbb{Z}_{>0}$ and $x + y$ even.

   - $y = 1$: $x^2 = \pm 4 + 21y^2 = \pm 4 + 21 = 17$ or 25, which is 5^2.

   So the smallest solution is $(5, 1)$ and $\varepsilon = \frac{1+5\sqrt{21}}{2}$ is a fundamental unit in $\mathbb{Z}_K^\times$. The other fundamental units are $\pm\varepsilon^{\pm 1}$, and none of these is equal to u, so u is not a fundamental unit of $\mathbb{Z}_K^\times$.

   Remark : it can be checked that in fact, $u = \varepsilon^3$.

3. *Prove that for all $v \in \mathbb{Z}_K^\times$, $N_\mathbb{Q}^K(v) = 1$.*

   Let $v \in \mathbb{Z}_K^\times$. Then there exists a sign $s \in \{\pm 1\}$ and an integer $n \in \mathbb{Z}$ such that $v = s\varepsilon^n$. We have

   $$N_\mathbb{Q}^K(v) = N_\mathbb{Q}^K(s) N_\mathbb{Q}^K(\varepsilon)^n = 1 \cdot 1^n = 1,$$

   since $N_\mathbb{Q}^K(\pm 1) = (\pm 1)^2 = 1$ and $N_\mathbb{Q}^K(\varepsilon) = 1$.

Exercise 2. *Let K be a number field of degree 3 such that* $\operatorname{disc} K < 0$.

1. *Prove that the signature of K is* $(1,1)$.

   Let (r_1, r_2) be the signature of K, so that $r_1 + 2r_2 = 3$. Since $\operatorname{disc} K < 0$ has the same sign as $(-1)^{r_2}$, we see that r_2 is odd. This forces $r_1 = r_2 = 1$.

2. *From now on, we use the unique real embedding of K to view it as a subfield of $\mathbb{R}$. Prove that there exists $\varepsilon \in K$ such that $\mathbb{Z}_K^\times = \{\pm\varepsilon^n,\ n \in \mathbb{Z}\}$. Why can we assume that $\varepsilon > 1$? We make this assumption from now on.*

   Since K has a real embedding, the group of roots of unity in K is $W_K = \{\pm 1\}$. By Dirichlet's theorem, the rank of the unit group is $r_1 + r_2 - 1 = 1$. Let ε be a fundamental unit of $\mathbb{Z}_K^\times$. Then we have

   $$\mathbb{Z}_K^\times = \{\pm\varepsilon^n \colon n \in \mathbb{Z}\}.$$

   The other fundamental units are the $\pm\varepsilon^{\pm 1}$, and exactly one of these is in the interval $(1, \infty)$.

3. *Express the regulator of K in terms of ε.*

   The matrix defining the regulator has two rows, one for the real embedding of K and one for the pair of complex embeddings of K. We choose to delete the row corresponding to the complex embedding. The resulting matrix is a 1×1 matrix, with only coefficient

   $$\log|\varepsilon| = \log\varepsilon \text{ since } \varepsilon > 0,$$

   so the regulator of K is $|\log\varepsilon| = \log\varepsilon$ since $\varepsilon > 1$.

4. *Prove that ε is a primitive element for K, and deduce that the minimal polynomial of ε factors as $(x-\varepsilon)(x-u^{-1}e^{i\theta})(x-u^{-1}e^{-i\theta})$ for some $\theta \in \mathbb{R}$, where $u = \sqrt{\varepsilon}$.*

   Since $\mathbb{Z}$ does not have any unit of infinite order, $\varepsilon \notin \mathbb{Q}$. So the field $\mathbb{Q}(\varepsilon) \subset K$ is not $\mathbb{Q}$, but its degree over $\mathbb{Q}$ divides that of K, which is 3. So $[\mathbb{Q}(\varepsilon) : \mathbb{Q}] = 3$ and $\mathbb{Q}(\varepsilon) = K$: ε is a primitive element of K.

   Let P be the minimal polynomial of ε over $\mathbb{Q}$. Since ε is a primitive element of K, the polynomial P has degree 3, is irreducible over $\mathbb{Q}$, and has one real root and two conjugate complex roots since the signature of K is $(1,1)$. The real root is ε, and let $z, \bar{z}$ be the complex roots. Since ε is a unit, it has norm ± 1. This norm is also the product of the complex embeddings of ε, so

   $$\pm 1 = \varepsilon z\bar{z} = \varepsilon|z|^2 > 0, \text{ so } \varepsilon|z|^2 = 1.$$

   We get $|z|^2 = \varepsilon^{-1}$, so the polar decomposition of z is $z = u^{-1}e^{i\theta}$ with $u = \sqrt{\varepsilon}$ and $\theta \in \mathbb{R}$.

5. *Given that*

$$\left(\frac{u^3+u^{-3}}{2}-\cos\theta\right)^2\sin^2\theta<\frac{u^6}{4}+\frac{3}{2}$$

for all $\theta\in\mathbb{R}$ (you are ***NOT*** *required to prove this), prove that*

$$\varepsilon>\sqrt[3]{\frac{|\operatorname{disc}K|}{4}-6}.$$

Hint: Prove that

$$\operatorname{disc}\mathbb{Z}[\varepsilon]=-16\left(\frac{u^3+u^{-3}}{2}-\cos\theta\right)^2\sin^2\theta.$$

Since ε is a primitive element of K and is an algebraic integer, $\mathbb{Z}[\varepsilon]$ is an order in K, so $|\operatorname{disc}K|\leq|\operatorname{disc}\mathbb{Z}[\varepsilon]|=|\operatorname{disc}P|$. We compute

$$\begin{aligned}\operatorname{disc}P&=\left[(\varepsilon-u^{-1}e^{i\theta})(\varepsilon-u^{-1}e^{-i\theta})(u^{-1}e^{i\theta}-u^{-1}e^{-i\theta})\right]^2\\&=\left[(\varepsilon^2-2\varepsilon u^{-1}\cos\theta+u^{-2})u^{-1}2i\sin\theta\right]^2\\&=-16\left(\frac{u^3+u^{-3}}{2}-\cos\theta\right)^2\sin^2\theta\text{ since }u^2=\varepsilon.\end{aligned}$$

Taking absolute values, we have

$$\begin{aligned}|\operatorname{disc}K|&\leq|\operatorname{disc}P|\\&<16\left(\frac{u^6}{4}+\frac{3}{2}\right)\\&=4(\varepsilon^3+6).\end{aligned}$$

Dividing by 4, subtracting 6 and taking cube roots, we obtain

$$\varepsilon>\sqrt[3]{\frac{|\operatorname{disc}K|}{4}-6}.$$

6. *Application: given that $\sqrt[3]{151/4}\approx 3.354$ and that the complex roots of $x^3-5x+5=0$ are $-2.627\dots$ and $1.314\dots\pm0.421\dots i$, find a fundamental unit for $K=\mathbb{Q}(\alpha)$, where $\alpha^3-5\alpha+5=0$.*

   Hint: Prove first that the decomposition of 5 in $\mathbb{Z}_K$ is $5\mathbb{Z}_K=(\alpha)^3$, use this to find a nontrivial unit in K, and prove that this unit is a fundamental unit.

   We are first going to use the decomposition of 5 in K to find a unit in K, and then use the previous question to prove that this unit is fundamental.

   The number field K was studied in assignment sheet 3, and we saw that $\mathbb{Z}_K=\mathbb{Z}[\alpha]$, $\operatorname{disc}K=-175$, and that $5\mathbb{Z}_K=\mathfrak{p}_5^3$ is totally ramified in K, where $\mathfrak{p}_5=(5,\alpha)$. We also proved that actually $\mathfrak{p}_5=(\alpha)$. As a result, we have

$$(5)=\mathfrak{p}_5^3=(\alpha)^3=(\alpha^3),$$

so we have discovered the unit $v = \frac{\alpha^3}{5} = \alpha - 1$.

Now, as $\operatorname{disc} K < 0$, we may try to apply the previous questions to see if v is fundamental. By question 2 we have $\mathbb{Z}_K^\times = \{\pm\varepsilon^n,\ n \in \mathbb{Z}\}$ for some $\varepsilon \in \mathbb{Z}_K^\times$, and, seeing K as a subfield of $\mathbb{R}$ via the embedding $\alpha \mapsto -2.627\ldots$, we may assume that $\varepsilon > 1$. Since v is a unit, we have $v = \pm\varepsilon^n$ for some $n \in \mathbb{Z}$, and since $v = \alpha - 1 \approx -3.627 < -1$ we must actually have $v = -\varepsilon^n$ with $n \in \mathbb{N}$. As a consequence, v is fundamental iff. $n = 1$.

But according to question 4, we have $\varepsilon > \sqrt[3]{\frac{175}{4} - 6} = \sqrt[3]{151/4} \approx 3.354$, and the equality $\varepsilon^n = -v \approx 3.627$ implies that $n < 2$. As a result, we must have $n = 1$, and so v is fundamental (and also $\varepsilon = 1 - \alpha$).

UNASSESSED QUESTIONS

Exercise 3. *What are the possible values of $\#W_K$ for K a number field of degree 4? Give an example for each possible value.*

Suppose that K contains ζ_n, a primitive n-th root of 1, for some $n \in \mathbb{N}$. Then $\mathbb{Q}(\zeta_n)$, the n-th cyclotomic field, is a subfield of K, and so $\varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ divides $[K : \mathbb{Q}] = 4$. The formula

$$\varphi(\prod_i p_i^{v_i}) = \prod_i (p_i - 1)p_i^{v_i - 1}$$

then shows that the primes dividing n are all $\leqslant 5$, and that 2, 3 and 5 divide n with multiplicity at most 3, 1 and 1 respectively. By trying all the possible values, we deduce that the integers n such that $\varphi(n) \mid 4$ are 1, 2, 3, 4, 5, 6, 8, 10 and 12.

Besides, we always have $-1 \in K$, so $\#W_K$ is always even. This leaves 2, 4, 6, 8, 10 and 12 as possibilities for $\#W_K$.

It turns out that all of these possibilities occur. In the extreme cases, this is easy to prove : we have $\#W_K = 8$ (respectively 10, 12) for $K = \mathbb{Q}(\zeta_8)$ (respectively $\mathbb{Q}(\zeta_{10})$, $\mathbb{Q}(\zeta_12)$), in view of the formula (caveat : $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{2m})$ when m is odd, because $-\zeta_m$ is then a primitive $2m$-th root of 1). Besides, $\#W_K = 2$ when K is totally real, e.g when $K = \mathbb{Q}(\alpha)$ where α satisfies an irreducible equation of degree 4 whose roots are all real.

For 4 and 6, this is more difficult. The fields $\mathbb{Q}(\zeta_4) = \mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\zeta_6) = \mathbb{Q}(\sqrt{-3})$ are quadratic, so we can try to take a "random" extension of degree 2 of them, and hope that this extension does not enlarge the number of roots of 1.

Let us find an example with $\#W_K = 4$ first. The minimal polynomial of $i = \sqrt{-1}$ over $\mathbb{Q}$ is $x^2 + 1$, so the one of $1 + i$ is $x^2 - 2x + 2$ (just translate the variable), and so $\sqrt{1+i}$ is a root of $f(x) = x^4 - 2x^2 + 2$. This polynomial is Eisenstein at 2, so it is irreducible and so $K = \mathbb{Q}(\sqrt{1+i})$ is a number field of degree 4. Besides, $i \in K$, so $\#W_K$ is a multiple of 4; it can thus be either 4, 8 or 12. We are going to prove that K is not isomorphic to $\mathbb{Q}(\zeta_8)$ nor to $\mathbb{Q}(\zeta_{12})$, which will prove that $\#W_K = 4$. Indeed, we have $x^2 - 2x + 2 \equiv (x+1)(x+2) \bmod 5$, so $f(x) \equiv (x-2)(x+2)(x^2+2) \bmod 5$, and -2 is not a square mod 5 so this is the complete factorisation of $f(x)$ mod 5. In particular, f mod 5 is squarefree, so $5 \nmid \operatorname{disc} f$, and so the order $\mathbb{Z}[\sqrt{1+i}]$ is maximal at 5; therefore, we may read the decomposition of 5 in K off the factorisation of $f \bmod 5$. We conclude that $5\mathbb{Z}_K$ is a product of three primes, two of which have degree 1 and one of which has degree 2. However, the theorem on the decomposition of primes in cyclotomic fields tells us that for all prime $p \in \mathbb{N}$ the primes occurring in the decomposition of p in a cyclotomic field all have the same degree, so K is not a cyclotomic field. This proves that $\#W_K = 4$. We could also have applied proposition 5.2.9 to a prime of degree 1 above 5.

Let us now do $\#W_K = 6$. The minimal polynomial of $j = \zeta_3$ over $\mathbb{Q}$ is $x^2 + x + 1$, so the one of $j - 1$ is $x^2 + 3x + 3$, and so $\sqrt{j-1}$ is a root of $g(x) = x^4 + 3x^2 + 3$, which is Eisenstein at 3 so that $K = \mathbb{Q}(\sqrt{j-1})$ is of degree 4. Besides, $j \in K$, so $\#W_K = 6$ or 12. However, the factorisation of $g \bmod 7$ is $(x+1)(x-1)(x^2+4)$, so $7\mathbb{Z}_K$ decomposes as degree 1 × degree 1 × degree 2, and again, because the degrees are not all the same or by proposition 5.2.9, this shows that $K \not\supset \mathbb{Q}(\zeta_{12})$, whence $\#W_K = 6$.

Exercise 4 (The battle of Hastings)**.** *"The men of Harold stood well together, as their wont was, and formed thirteen squares, with a like number of men in every square thereof. (...) When Harold threw himself into the fray the Saxons were one mighty square of men, shouting the battle cries 'Ut!', 'Olicrosse!', 'Godemite!'."*

How many troops does this fictional historical text[1] *suggest Harold II had at the battle of Hastings?*

We are looking for solutions to $13y^2 + 1 = x^2$ with some $x, y \in \mathbb{N}$. This translates as $x^2 - 13y^2 = 1$, so we are looking for units of norm $+1$ in $\mathbb{Z}[\sqrt{13}]$.

Let $K = \mathbb{Q}(\sqrt{13})$. We have $\mathbb{Z}_K = \mathbb{Z}[\frac{1+\sqrt{13}}{2}]$, and by the same technique as in exercise 1 we find that a fundamental unit is $\varepsilon = \frac{3+\sqrt{13}}{2}$, which as norm -1. The units of norm $+1$ are thus the $\pm\varepsilon^{2n}$, $n \in \mathbb{Z}$. We try small values of n until we find a number of the form $x + y\sqrt{13}$ with $x, y \in \mathbb{N}$.

- For $n = \pm 1$ we have $\varepsilon^{\pm 2} = \frac{11 \pm 3\sqrt{13}}{2}$, which doesn't do as we want a unit in the order $\mathbb{Z}[\sqrt{13}]$;
- for $n = \pm 2$ we get $\varepsilon^{\pm 4} = \frac{119 \pm 33\sqrt{13}}{2}$, same problem;
- for $n = \pm 3$ we finally get $\varepsilon^{\pm 6} = 649 \pm 180\sqrt{13}$, whence our first solution : $x = 180, y = 649$.

This corresponds to an army of $13 \cdot 180^2 = 421,200$ men plus Harold, which seems a bit exaggerated ! Larger values of n only lead to larger solutions, so we are led to suspecting that this historical text is, indeed, fictitious.

[1] Cf. problem no. 129 in *Amusement in Mathematics* (H.E. Dundeney, 1917).