Algebraic number theory — Exercise sheet 4

https://www.maths.tcd.ie/~mascotn/teaching/2022/MAU34109/index.html

Version: November 11, 2022

Email your answers to mascotn@tcd.ie by Wednesday November 23 noon.

Exercise 4.1: A Mordell-Weil equation (100 pts)

The goal of this exercise is to solve the Diophantine equation

$$y^2 = x^3 - 148 \qquad (x, y \in \mathbb{Z}) \tag{1}$$

We let $K = \mathbb{Q}(\alpha)$ where $\alpha = \sqrt{-37}$, and note that (1) can be rewritten as

$$(y + 2\alpha)(y - 2\alpha) = x^3.$$

You may use without proof the following facts:

- $148 = 4 \cdot 37$, and 37 is prime,
- $\mathbb{Z}_K^\times = \{\pm 1\}$.

1. (5 pts) Prove that the equation has no solution such that $37 \mid y$.
2. (30 pts) Determine $\mathbb{Z}_K$ and $\mathrm{Cl}(K)$, as well as the decomposition of 37 in K.
3. (15 pts) Let (x, y) be a hypothetical solution of (1). Prove that there is at most one prime $\mathfrak{p}$ of K that divides both $(y+2\alpha)$ and $(y-2\alpha)$. Which prime is that?
4. (35 pts) Deduce that at least one of $y + 2\alpha$ or $y - 2\alpha$ is a cube or twice a cube in $\mathbb{Z}_K$.

   Hint: Prove that $(y+2\alpha) = \mathfrak{b}^3\mathfrak{p}^r$ *and* $(y-2\alpha) = \mathfrak{b}'^3\mathfrak{p}^{r'}$ *for some ideals* $\mathfrak{b}, \mathfrak{b}' \triangleleft \mathbb{Z}_K$ *and integers* $r, r' \geqslant 0$*. How small can you make* r *and* r'*?*
5. (15 pts) Find all the solutions of (1).

Solution 4.1:

1. If $37 \mid y$, then $37 \mid x^3$ so $37 \mid x$. But then $37^2 \mid 37$, absurd.
2. As $-37 \equiv 3 \bmod 4$, we have $\mathbb{Z}_K = \mathbb{Z}[\alpha]$ and

$$M_K = \frac{2!}{2^2}\frac{4}{\pi}\sqrt{4 \cdot 37} = 7.74\cdots < 11.$$

   This is large, but fortunately 3, 5 and 7 are inert! So $\mathrm{Cl}(K)$ is generated by $[\mathfrak{p}_2]$ where $\mathfrak{p}_2 = (2, \alpha + 1)$ is such that $(2) = \mathfrak{p}_2^2$, and is thus either trivial or

isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Since $x^2 + 37y^2 = \pm 2$ has no solution in integers, we actually have

$$\mathrm{Cl}(K) = \langle [\mathfrak{p}_2] \rangle \simeq \mathbb{Z}/2\mathbb{Z}.$$

Finally, we have $(37) = \mathfrak{p}_{37}^2$ with $\mathfrak{p}_{37} = (37, \alpha)$ ($= (\alpha)$ since α has norm 37, but here this is irrelevant).

3. Let $\mathfrak{p}$ be a prime dividing $(y + 2\alpha, y - 2\alpha)$. Then $4\alpha = (y + 2\alpha) - (y - 2\alpha) \in \mathfrak{p}$, so $\mathfrak{p} \mid (4\alpha) = 4(\alpha) = \mathfrak{p}_2^4 \mathfrak{p}_{37}$. However, we also have $2y = (y + 2\alpha) + (y - 2\alpha) \in \mathfrak{p}$, so if $\mathfrak{p} = \mathfrak{p}_{37}$ then $y \in \mathfrak{p}_{37} \cap \mathbb{Z} = 37\mathbb{Z}$, and the first question tells us that this is not possible. So the only possibility is $\mathfrak{p} = \mathfrak{p}_2$.

4. Let us factor $(y + 2\alpha) = \mathfrak{a}\mathfrak{p}_2^m$, $(y - 2\alpha) = \mathfrak{a}'\mathfrak{p}_2^{m'}$, where $\mathfrak{a}$ and $\mathfrak{a}'$ are prime to $\mathfrak{p}_2$. By the previous question, $\mathfrak{a}$ and $\mathfrak{a}'$ are coprime, so since

$$\mathfrak{a}\mathfrak{a}'\mathfrak{p}_2^{m+m'} = (y + 2\alpha)(y - 2\alpha) = (x^3) = (x)^3$$

is the cube of an ideal, we must have $\mathfrak{a} = \mathfrak{b}^3$, $\mathfrak{a}' = \mathfrak{b}'^3$ for some ideals $\mathfrak{b}$ and $\mathfrak{b}'$, and $3 \mid m + m'$. Write $m = 3q + r$ and $m' = 3q' + r'$ with $0 \leqslant r, r' < 3$. Then we get $(y + 2\alpha) = \mathfrak{c}^3\mathfrak{p}_2^r$, $(y - 2\alpha) = \mathfrak{c}'^3\mathfrak{p}_2^{r'}$ with $\mathfrak{c} = \mathfrak{b}\mathfrak{p}_2^q$ and $\mathfrak{c}' = \mathfrak{b}'\mathfrak{p}_2^{q'}$.

If $r = 0$, then $(y + 2\alpha) = \mathfrak{c}^3$, and since 3 is coprime to $h_K = 2$, this means that $\mathfrak{c}$ is principal, say $\mathfrak{c} = (\gamma)$, $\gamma \in \mathbb{Z}_K$. Then $(y + 2\alpha) = \mathfrak{c}^3 = (\gamma^3)$, so there exists a unit $u \in \mathbb{Z}_K^\times$ such that $y + 2\alpha = u\gamma^3$. Since $u = \pm 1$, we deduce that $(y + 2\alpha) = (u\gamma)^3$ is a cube in $\mathbb{Z}_K$. Similarly, if $r' = 0$ we see that $y - 2\alpha$ is a cube in $\mathbb{Z}_K$.

Suppose now that r and r' are both nonzero. Since $3 \mid m + m'$, we must have $r = 1$, $r' = 2$, or vice versa. Suppose for instance that $r = 2$. Then we have $(y + 2\alpha) = \mathfrak{c}^3\mathfrak{p}_2^2 = 2\mathfrak{c}^3$, so by the same logic as above $\mathfrak{c} = (\gamma)$ is principal and therefore $y + 2\alpha = 2u\gamma^3 = 2(u\gamma)^3$ is twice a cube. Similarly, if $r' = 2$, then $y - 2\alpha$ is twice a cube.

5. Suppose first that one of $y \pm 2\alpha$ is a cube in $\mathbb{Z}_K$. Then there exist $u, v \in \mathbb{Z}$ such that

$$y \pm 2\alpha = (u + v\alpha)^3 = (u^2 - 3 \cdot 37v^2)u + (3u^2 - 37v^2)v\alpha.$$

Comparing the coefficients of α, we get that $(3u^2 - 37v^2)v = \pm 2$, whence $v = \pm 1$ or ± 2. For $v = \pm 1$ we get $3u^2 = \pm 2 + 37$ which is absurd, whereas for $v = \pm 2$ we get $3u^2 = \pm 1 + 37 \cdot 4$ which admits the solution $u = \pm 7$. This gives $y = (u^2 - 3 \cdot 37v^2)u = \pm 2765$, and indeed $x = 197$, $y = \pm 2765$ is a solution of (1).

If now one of $y \pm 2\alpha$ is a cube in $\mathbb{Z}_K$, then we get

$$y \pm 2\alpha = 2(u + v\alpha)^3 = 2(u^2 - 3 \cdot 37v^2)u + 2(3u^2 - 37v^2)v\alpha$$

whence $v = \pm 1$ and $3u^2 = \pm 1 + 37$, which is absurd, so we get no solutions this way.

Conclusion: the only solutions of (1) are $x = 197$, $y = \pm 2765$.

This was the only mandatory exercise, that you must submit before the deadline. The following exercises are not mandatory; they are not worth any points, and you do not have to submit them. However, I highly recommend that you try to solve them for practice (they may even give you inspiration to help you solve Exercise 1), and you are welcome to email me if you have questions about them. The solutions will be made available with the solution to the mandatory exercise.

Exercise 4.2: Class group computations

Determine the class group of the following number fields:

1. $\mathbb{Q}(\sqrt{-29})$,
2. $\mathbb{Q}(\sqrt{-33})$.

Solution 4.2:

1. Let $K = \mathbb{Q}(\alpha)$, where $\alpha = \sqrt{-29}$. As $-29 \equiv 3 \bmod 4$, we have $\mathbb{Z}_K = \mathbb{Z}[\alpha]$ and $\operatorname{disc} K = -4 \cdot 29$. Besides, $\operatorname{sign} K = (0, 1)$, so the Minkowski bound is

$$M_K = \frac{2!}{2^2}\frac{4}{\pi}\sqrt{4 \cdot 29} = 6.85\cdots < 7$$

so $\mathrm{Cl}(K)$ is generated by the primes above 2, 3, and 5.

As $\mathbb{Z}_K = \mathbb{Z}[\alpha]$, we compute by factoring $x^2 + 29$ mod these primes that

$$(2) = \mathfrak{p}_2^2, \quad \mathfrak{p}_2 = (2, \alpha + 1),$$

$$(3) = \mathfrak{p}_3\mathfrak{q}_3, \quad \mathfrak{p}_3 = (3, \alpha + 1), \mathfrak{q}_3 = (3, \alpha - 1),$$

$$(5) = \mathfrak{p}_5\mathfrak{q}_5, \quad \mathfrak{p}_5 = (5, \alpha + 1), \mathfrak{q}_5 = (5, \alpha - 1).$$

Thus in $\mathrm{Cl}(K)$ we have $[\mathfrak{p}_2]^2 = 1$, $[\mathfrak{q}_3] = [\mathfrak{p}_3]^{-1}$, and $[\mathfrak{q}_5] = [\mathfrak{p}_5]^{-1}$, so $\mathrm{Cl}(K)$ is generated by $[\mathfrak{p}_2]$, $[\mathfrak{p}_3]$ and $[\mathfrak{p}_5]$.

The norm of the generic element $x + y\alpha$ of $\mathbb{Z}_K$ is $x^2 + 29y^2$. We spot that $1 + \alpha$ has norm 30, whence the factorization $(1 + \alpha) = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5$ and the relation $[\mathfrak{p}_2][\mathfrak{p}_3][\mathfrak{p}_5] = 1$ in $\mathrm{Cl}(K)$, which is thus generated by $[\mathfrak{p}_2]$ and $[\mathfrak{p}_3]$ alone.

We next spot that $29 + 4^2 = 45 = 3^2 \cdot 5$, whence $(4 + \alpha) = \mathfrak{p}_3^2\mathfrak{q}_5$ and therefore $[\mathfrak{p}_5] = [\mathfrak{p}_3]^2$, which yields $[\mathfrak{p}_2] = [\mathfrak{p}_3]^{-4}$. Thus $\mathrm{Cl}(K)$ is cyclic and generated by $[\mathfrak{p}_3]$.

To conclude, we must determine the order of $[\mathfrak{p}_3]$. Suppose that $\mathfrak{p}_3^m = (\beta)$ is principal for some $m \in \mathbb{N}$; then $\beta \in \mathbb{Z}_K$ must be of norm $\pm 3^m$, so we have a solution to $x^2 + 29y^2 = \pm 3^m$. Since β cannot be divisible by 3 in $\mathbb{Z}_K$ (lest $(3) = \mathfrak{p}_3\mathfrak{q}_3$ divide $\mathfrak{p}_3^m$), we then have $3 \nmid x$ or $3 \nmid y$. Conversely, given x and y not both divisible by 3 and satisfying $x^2 + 29y^2 = 3^m$, we have that $\beta = x + y\alpha$ generates an ideal of norm 3^m, that factors either as $\mathfrak{p}_3^m$ or $\mathfrak{q}_3^m$ since β is not divisible by 3 in $\mathbb{Z}_K$. Since $[\mathfrak{p}_3]$ and $[\mathfrak{q}_3]$ are inverses of each other, they have the

same order, and so this common order is the smallest $m \in \mathbb{N}$ such that x^2+29y^2 has a solution with x and y not both divisible by 3.

For $m \leqslant 3$, we necessarily have $y = 0$, which is excluded since its forces x to be a power of 3. For $m = 4$, we want $x^2 = 81 - 29y^2$, which forces $y = \pm 1$ and leads to a contradiction. Similarly for $m = 5$, we must have $|y| \leqslant 2$, and hence no solution. But for $m = 6$, we find $2^2 + 29 \times 5^2 = 3^6$. In conclusion,

$$\mathrm{Cl}(K) = \langle [\mathfrak{p}_3] \rangle \simeq \mathbb{Z}/6\mathbb{Z}.$$

2. Let $K = \mathbb{Q}(\alpha)$, where $\alpha = \sqrt{-33}$. This time $\mathbb{Z}_K = \mathbb{Z}[\alpha]$, $\operatorname{disc} K = -4 \cdot 33$, $\operatorname{sign} K = (0, 1)$, and

$$M_K = \frac{2!}{2^2}\frac{4}{\pi}\sqrt{4 \cdot 33} = 7.31\cdots < 11$$

so $\mathrm{Cl}(K)$ is generated by the primes above 2, 3, 5, and 7.

We compute as previously

$$(2) = \mathfrak{p}_2^2, \quad \mathfrak{p}_2 = (2, \alpha + 1),$$

$$(3) = \mathfrak{p}_3^2, \mathfrak{p}_3 = (3, \alpha),$$

$$5 \text{ is inert},$$

$$(7) = \mathfrak{p}_7\mathfrak{q}_7, \quad \mathfrak{p}_7 = (7, \alpha + 3), \mathfrak{q}_7 = (7, \alpha - 3),$$

so $\mathrm{Cl}(K)$ is generated by $[\mathfrak{p}_2]$, $[\mathfrak{p}_3]$ and $[\mathfrak{p}_7]$, and we already have the relations $[\mathfrak{p}_2]^2 = [\mathfrak{p}_3]^2 = 1$.

The norm of $x+y\alpha \in \mathbb{Z}_K$ is x^2+33y^2. We spot that $3+\alpha$ has norm $42 = 2\times3\times7$, so $(3 + \alpha) = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_7$ and $\mathrm{Cl}(K)$ is generated by $[\mathfrak{p}_2]$ and $[\mathfrak{p}_3]$. Since these are of order at most 2, $\mathrm{Cl}(K)$ is a quotient of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

If this quotient were strict, at least one of $\mathfrak{p}_2$, $\mathfrak{p}_3$, or $\mathfrak{p}_2\mathfrak{p}_3$ would be principal. But $x^2 + 33y^2$ is clearly never 2 nor 3 nor 6, so in conclusion

$$\mathrm{Cl}(K) = \langle [\mathfrak{p}_2], [\mathfrak{p}_3] \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Exercise 4.3: A norm equation

Let $n \geqslant 0$ be an integer. The goal of this exercise is to determine the number of solutions to the Diophantine equation

$$x^2 + 10y^2 = 7^n \qquad (x, y \in \mathbb{Z}) \tag{2}$$

in terms of n.

We let $K = \mathbb{Q}(\alpha)$ where $\alpha = \sqrt{-10}$, and note that (2) can be rewritten as

$$N_{\mathbb{Q}}^K(x + \alpha y) = 7^n.$$

You may freely use the fact that $\mathbb{Z}_K^\times = \{\pm 1\}$.

1. Determine $\mathbb{Z}_K$ and $\mathrm{Cl}(K)$.

2. Determine the decomposition of 7 in $\mathbb{Z}_K$, and the image in $\mathrm{Cl}(K)$ of the primes appearing in this factorisation.

3. Let $\mathfrak{a}$ be an of $\mathbb{Z}_K$ of norm 7^n. What does the factorisation into primes of $\mathfrak{a}$ look like? What does this tell you about the image of $\mathfrak{a}$ in $\mathrm{Cl}(K)$?

4. Express the number of solutions to (2) in terms of n.

Solution 4.3:

1. Since $-10 \not\equiv 1 \pmod 4$, we have $\mathbb{Z}_K = \mathbb{Z}[\alpha] = \{x + y\alpha,\ x, y \in \mathbb{Z}\}$ and $\operatorname{disc} K = -40$, so $M_K = \frac{2!}{2^2}\frac{4}{\pi}\sqrt{40} \approx 4.03$ and $\mathrm{Cl}(K)$ is generated by the primes above 2 and 3. As $2 \mid 40$, 2 ramifies in K, say $2 = \mathfrak{p}_2^2$ (where $\mathfrak{p}_2 = (2, \alpha)$ since $x^2 + 10 \equiv x^2 \bmod 2$, but we will not use this), whereas 3 is inert as $x^2 + 10$ remains irreducible mod 3, so $\mathrm{Cl}(K)$ is generated by $[\mathfrak{p}_2]$ (and is thus cyclic). The norm of the generic element $x + y\alpha$ of $\mathbb{Z}_K$ is $x^2 + 10y^2$, and this is clearly never ± 2, so $\mathfrak{p}_2$ is not principal; so the relation $(2) = \mathfrak{p}_2^2$ implies that $[\mathfrak{p}_2]$ has order exactly 2. Thus $\mathrm{Cl}(K) \simeq \mathbb{Z}/2\mathbb{Z}$.

2. The polynomial $x^2 + 10$ has two distinct roots mod 7, namely 2 and $-2 = 5$. Therefore 7 splits in K, say $(7) = \mathfrak{p}_7\mathfrak{q}_7$ (and we can take $\mathfrak{p}_7 = (7, \alpha - 2)$, $\mathfrak{q}_7 = (7, \alpha+2)$, but again we will not use this). Since the equation $x^2+10y^2 = \pm 7$ has clearly no solution in integers, neither $\mathfrak{p}_7$ nor $\mathfrak{q}_7$ can be principal. But h_K is only 2, so necessarily $[\mathfrak{p}_7] = [\mathfrak{q}_7]$ is the non-trivial element of $\mathrm{Cl}(K)$, which is also $[\mathfrak{p}_2]$.

3. Since $N(\mathfrak{a}) = 7^n$, so only $\mathfrak{p}_7$ and $\mathfrak{q}_7$ can appear in the factorisation of $\mathfrak{a}$. More precisely, since $N(\mathfrak{p}_7) = N(\mathfrak{q}_7) = 7$, we must have $\mathfrak{a} = \mathfrak{p}_7^m\mathfrak{q}_7^{n-m}$ for some $0 \leqslant m \leqslant n$. This implies that

$$[\mathfrak{a}] = [p_7]^m[\mathfrak{q}_7]^{n-m} = [\mathfrak{p}_2]^m[\mathfrak{p}_2]^{n-m} = [\mathfrak{p}_2]^n.$$

   Since $[\mathfrak{p}_2]$ has order exactly 2, this means that $\mathfrak{a}$ is principal if n is even, and non-principal is n is odd. However $\mathfrak{a} = (x + y\alpha)$ is principal by construction, so if n is odd this contradiction shows that (2) has no solution.

4. Let $(x, y) \in \mathbb{Z}^2$, and let $\mathfrak{a} = (x + y\alpha)$. Then $\mathfrak{a}$ is principal by construction, and $N(\mathfrak{a}) = |N_{\mathbb{Q}}^K(x + y\alpha)| = x^2 + 10y^2$, so that we get a map between solutions of (2) and principal ideals of $\mathbb{Z}_K$ of norm 7^n. This map is 2-to-1, since a principal ideal has exactly $\#\mathbb{Z}_K^\times = 2$ generators (since any two generators are associate, and conversely).

   By the previous question, there are $n+1$ ideals of norm 7^n, namely the $\mathfrak{p}_7^m\mathfrak{q}_7^{n-m}$ for $0 \leqslant m \leqslant n$, and if n is even they are all principal, whereas none of them is principal if n is odd. Conclusion: the number of solutions to (2) is 0 if n is odd, and $2(n + 1)$ if n is even.

Exercise 4.4: Arbitrarily large class numbers

Let $d > 0$ be a squarefree integer, and let $K = \mathbb{Q}(\sqrt{-d})$. Suppose that $p \in \mathbb{N}$ is a prime which splits in K, and let $\mathfrak{p}$ be a prime ideal above p.

1. Prove that for all integers $i \geq 1$ such that $p^i < |\operatorname{disc} K|/4$, the ideal $\mathfrak{p}^i$ is not principal.

   Hint: consider the cases $d \not\equiv 1 \pmod 4$ *and* $d \equiv 1 \pmod 4$ *separately.*

2. What does this tell you about the class number of K?

3. Using without proof the fact that there exists infinitely many squarefree positive numbers of the form $8k + 7$ for $k \in \mathbb{N}$, prove that for every $X > 0$ there exists a number field K such that $h_K > X$.

Solution 4.4:

1. Let i be as above. Since p is split, $N(\mathfrak{p}) = p$, and by uniqueness of factorisation the ideal $\mathfrak{p}^i$ is not divisible by (p).

   - If $\operatorname{disc} K = -4d$, then $\mathbb{Z}_K = \mathbb{Z}[\sqrt{-d}]$. The norm of a generic element $z = x + y\sqrt{-d} \in \mathbb{Z}_K$ is
   $$x^2 + dy^2.$$
   If $\mathfrak{p}^i$ is principal, let γ be a generator. Then the norm of γ is p^i, giving $x^2 + dy^2 = p^i$, so $y^2 \leq p^i/d < 1$, so $y = 0$. But then $\gamma \in \mathbb{Z}$ has norm$\gamma^2 = p^i$, so γ is divisible by p, and this is impossible since $\mathfrak{p}^i$ is not divisible by (p).
   - If $\operatorname{disc} K = -d$, then $\mathbb{Z}_K = \mathbb{Z}[\alpha]$ with $\alpha = \frac{1+\sqrt{-d}}{2}$. The norm of a generic element $z = x + y\alpha$ is
   $$\left(x + \frac{y}{2}\right)^2 + d\left(\frac{y}{2}\right)^2.$$
   If $\mathfrak{p}^i$ is principal, let γ be a generator. Then the norm of γ is p^i, so $y^2 \leq 4p^i/d < 1$, so $y = 0$ and as before γ is divisible by p, which is impossible.

2. The number of i as in the previous question is
   $$\left\lfloor \frac{\log(|\operatorname{disc} K|/4)}{\log p} \right\rfloor,$$
   and by the previous question the order of $[\mathfrak{p}]$ in $\mathrm{Cl}(K)$ is larger than this. So, accounting for the trivial class, we have
   $$h_K \geq 1 + \left\lfloor \frac{\log(|\operatorname{disc} K|/4)}{\log p} \right\rfloor.$$

3. Let d be squarefree of the form $8k + 7$. Then $-d < 0$ is squarefree and $-d \equiv 1 \bmod 8$. Let $K = \mathbb{Q}(\sqrt{-d})$. Then $\operatorname{disc} K = -d$ and 2 is split in K. By the previous part we have $h_K \geq 1 + \left\lfloor \frac{\log(d/4)}{\log 2} \right\rfloor$, which tends to ∞ as $d \to \infty$. Using an infinite sequence of such d we obtain $h_K \to \infty$.

Exercise 4.5: A non-Euclidean PID

Recall that a domain R is Euclidean *if there exists a size function $s : R \setminus \{0\} \longrightarrow \mathbb{N}$ such that for all $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ such that $a = bq + r$ and either $r = 0$ or $s(r) < s(b)$ (example: $R = K[x]$ where K is a field, $s = \deg$).*

One proves in commutative algebra that every Euclidean domain is automatically a PID, and one usually mentions that the converse does not hold, but counter-examples are not easy to exhibit.

The purpose of this exercise is to provide an example of a PID which is not Euclidean. As such, unlike other exercises, this exercise is more about commutative algebra than algebraic number theory, and will therefore not really help you to prepare for the exam; but I thought some of you might like to see this example since it is a nice application of algebraic number theory.

Let $K = \mathbb{Q}(\sqrt{-19})$.

1. Determine $\mathbb{Z}_K$.
2. Prove that $\mathbb{Z}_K$ is a PID.
3. Prove that $\mathbb{Z}_K^\times = \{\pm 1\}$.
4. Prove that $\mathbb{Z}_K$ has no ideal of norm 2 nor 3.
5. Let R be a Euclidean domain with size function s which is not a field, let $R^\times$ be the group of units of R, and let $U = R^\times \cup \{0\}$. Prove that there exists an $m \in R \setminus U$ such that every element of the quotient ring $R/(m)$ can be represented by an element of U (in other words, such that the restriction to U of the projection morphism $R \longrightarrow R/(m)$ remains surjective).

   Hint: Consider an element of $R \setminus U$ of minimal size.
6. Prove that the does not exist any size function for which $\mathbb{Z}_K$ is Euclidean.

Solution 4.5:

1. Since $-19 \equiv 1 \bmod 4$, $\mathbb{Z}_K = \mathbb{Z}[\alpha] = \{x + y\alpha \mid x, y \in Z\}$ where $\alpha = \frac{1+\sqrt{-19}}{2}$.

   We note for future reference that $N_{\mathbb{Q}}^K(x+y\alpha) = (x+1/2)^2 + \frac{19}{4}y^2 = x^2 + xy + 5y^2$.
2. We have $\operatorname{sign}(K) = (0, 10$ and $\operatorname{disc} K = -19$, so $M_K = \frac{2!}{2^2}\frac{4}{\pi}\sqrt{19} = 2.77\cdots$, so we only need to check the primes above 2. However $-19 \equiv 5 \bmod 8$, so 2 is inert, so the only prime above 2 is (2), which is obviously principal.
3. Solving $(x + 1/2)^2 + \frac{19}{4}y^2 = \pm 1$ for $x, y \in \mathbb{Z}$, we immediately see that $y = 0$ since $19/4 > 1$.

4. An ideal of norm 2 would be a prime above 2, and we have already seen that no such prime exists. For 3, we could conclude in a similar way b observing that 3 is also inert in K since $-19 \equiv -1$ is not a square mod 3; alternatively, since we know that $\mathbb{Z}_K$ is principal, it is enough to show that $(x+1/2)^2 + \frac{19}{4}y^2 = \pm 3$ has no solutions in integers, which is clear since $19/4 > 3$ (so $y = 0$) and 3 is not a square.

5. Since R is not a field, $R \setminus U$ is not empty, so $s(R \setminus U)$ is a non-empty subset of $\mathbb{N}$. It therefore admits a smallest element, so there exists $m \in R \setminus U$ such that $s(x) \geqslant s(m)$ for all $x \in R \setminus U$.

   Let now $x \in R$. Since $m \notin U$, $m \neq 0$, so we can perform a Euclidean division of x by m, and get $q, r \in R$ such that $x = mq + r$ with $r = 0$ or $s(r) < s(m)$. If $s(r) < s(m)$, then $r \in U$ by construction of m; and if $r = 0$, then $r \in U$ as well. But x and r represent the same class in the quotient ring $R/(m)$.

6. By contradiction, if $R = \mathbb{Z}_K$ were Euclidean for any size function, the previous question would grant us with an $m \in \mathbb{Z}_K \setminus U$ such that every element of $\mathbb{Z}_K/(m)$ can be represented by an element of U. But $U = \mathbb{Z}_K^\times \cup \{0\} = \{1, -1, 0\}$ has only three elements, so $R/(m)$ would have cardinal at most 3. On the other hand, $R/(m)$ cannot have cardinal 1 since $m \notin U$ is not a unit, so $R/(m)$ would have cardinal 2 or 3. But this would mean that (m) is an ideal of norm 2 or 3, which contradicts question 4.