Exercise Sheet 4

1. Let K be a number field of degree $n = [K : \mathbb{Q}]$. For $x \in K$, the *norm* of x, denoted $N(x)$, is defined to the determinant of the $\mathbb{Q}$-linear map $m_x \colon K \to K$ defined by $m_x(y) = xy$. (Note that $N(x)$ is not necessarily ≥ 0, even when $K = \mathbb{Q}$.)

1. For $K = \mathbb{Q}(\sqrt{d})$, compute $N(a + b\sqrt{d})$ as a function of the rational numbers a and b.

   Solution: Assume throughout that d is not a square, so that $K \neq \mathbb{Q}$. Consider the $\mathbb{Q}$-basis $\{1, \sqrt{d}\}$ of K. In this basis, multiplication by $a + b\sqrt{d}$ is given by the matrix
   $$\begin{bmatrix} a & bd \\ b & a \end{bmatrix},$$
   which has determinant $a^2 - db^2$. Thus $N(a + b\sqrt{d}) = a^2 - db^2$.

2. Show that N defines a group homomorphism $K^\times \to \mathbb{Q}^\times$.

   Solution: Note first that $N(x) \in \mathbb{Q}$ for all $x \in K$. Moreover, if $x = a + b\sqrt{d}$ and $N(x) = 0$, then $a^2 = db^2$. Since d is not a square, a and b must both be 0, so that $x = 0$. Thus the norm defines a function $N : K^\times \to \mathbb{Q}^\times$.

   It remains to show that this function is a group homomorphism. For two elements $x, y \in K^\times$, and for any $z \in K$, we have $(xy)z = x(yz)$, so that as maps $K \to K$, we have $m_{xy} = m_x \circ m_y$. The determinant is multiplicative with respect to composition of linear maps (that is, matrix multiplication), so
   $$N(xy) = \det(m_{xy}) = \det(m_x)\det(m_y) = N(x)N(y),$$
   and thus $N : K^\times \to \mathbb{Q}^\times$ is a group homomorphism.

3. Let $\mathcal{E}(K)$ be the set of embeddings of K in $\mathbb{C}$. Show that
   $$N(x) = \prod_{\iota \in \mathcal{E}(K)} \iota(x).$$

   Solution: Recall that the constant term of the characteristic polynomial of a matrix M is precisely $\det(-M) = (-1)^n \det(M)$, where M is an $n \times n$ matrix. By Corollary 2.5.2, for $x \in K$, the characteristic polynomial of m_x is
   $$\prod_{\iota \in \mathcal{E}(K)} (X - \iota(x)),$$

so that

$$(-1)^n \det(m_x) = \prod_{\iota\in\mathcal{E}(K)} (-\iota(x))$$
$$\Rightarrow \det(m_x) = \prod_{\iota\in\mathcal{E}(K)} \iota(x),$$

where the second line follows from the first because $|\mathcal{E}(K)| = n$. This completes the proof.

4. Let $x \in \mathbb{Z}_K$. Show that $N(x) \in \mathbb{Z}$. Show also that x is a unit in $\mathbb{Z}_K^\times$ if and only if $N(x) \in \{-1, 1\}$.

   Solution: Since x is an algebraic integer, every embedding $\iota : K \to \mathbb{C}$ must have the property that $\iota(x)$ is also an algebraic integer, because ι fixes both $\mathbb{Z}$ and polynomial equations. Thus $\prod_{\iota\in\mathcal{E}(K)} \iota(x)$ is also an algebraic integer, so $N(x)$ is an algebraic integer. The norm $N(x)$ is also the determinant of a matrix with rational coefficients by definition, so $N(x) \in \mathbb{Q}$ as well. But the only algebraic integers in $\mathbb{Q}$ are in $\mathbb{Z}$, so $N(x) \in \mathbb{Z}$ whenever $x \in \mathbb{Z}_K$.

   If x is a unit in $\mathbb{Z}_K^\times$, then there exists $y \in \mathbb{Z}_K^\times$ with $xy = 1$. Thus $N(x)N(y) = N(xy) = N(1) = 1$, so the integers $N(x)$ and $N(y)$ are invertible and thus $N(x), N(y) \in \{\pm 1\}$.

   Finally assume that $x \in \mathbb{Z}_K^\times$ with $N(x) = \pm 1$; we want to show that x is a unit in $\mathbb{Z}_K^\times$. Any x is a root of its characteristic polynomial; since $x \in \mathbb{Z}_K^\times$, this polynomial has integer coefficients. Write

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$$

   for this polynomial. As we saw in the problem (1.3), the constant term of this polynomial satisfies $a_0 = \pm N(x)$, so $a_0 = \pm 1$. Then consider

$$g(Y) = \sum_{j=0}^{m} a_0 a_{m-j} Y^j = a_0 + a_0 a_{m-1} Y + \cdots + a_0 a_1 Y^{m-1} + Y^m,$$

   where here we are writing $a_m := 1$ and noting that $a_0^2 = 1$. The polynomial $g(Y)$ is monic and has integer coefficients, and x^{-1} is a root of Y. Thus the element $y = x^{-1} \in K$ is an algebraic integer, so $y \in \mathbb{Z}_K$ and thus x is a unit in $\mathbb{Z}_K$.

5. Let $x \in \mathbb{Z}_K \setminus \{0\}$. Show that there exists a $\mathbb{Z}$-basis $(e_1, \ldots, e_n)$ of $\mathbb{Z}_K$ and integers $a_1 \mid a_2 \mid \cdots \mid a_n$ such that

$$x\mathbb{Z}_K = a_1\mathbb{Z}e_1 \oplus \cdots \oplus a_n\mathbb{Z}e_n.$$

   (Hint: use the classification of finitely-generated abelian groups.)

   Solution: Consider the $\mathbb{Z}$-module $\mathbb{Z}_K/x\mathbb{Z}_K$. By the classification of finitely-generated abelian groups,

$$\mathbb{Z}_K/x\mathbb{Z}_K \cong \mathbb{Z}^b \oplus (\mathbb{Z}/a_1\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/a_k\mathbb{Z}),$$

where $a_1|a_2|\cdots|a_k$ are integers.

Note that $N(x) \in x\mathbb{Z}_K$, since $N(x)$ is the constant term of the characteristic polynomial of x, which has integer coefficients. Thus $N(x) \in x\mathbb{Z}_K \cap \mathbb{Z}$, so $x\mathbb{Z}_K \cap \mathbb{Z}$ is nonempty. For any $y \in \mathbb{Z}_K$, this implies that $N(x)y \in x\mathbb{Z}_K$, so every element $\bar{y} \in \mathbb{Z}_K/x\mathbb{Z}_K$ must be a torsion element. Thus $b = 0$.

Let $\bar{e_i} \in \mathbb{Z}_K/x\mathbb{Z}_K$ represent an (arbitrary) generator of the factor $\mathbb{Z}/a_i\mathbb{Z}$, and let $e_i \in \mathbb{Z}_K$ be equivalent to $\bar{e_i}$ modulo x. Then $\{e_1, \ldots, e_k\}$ must be $\mathbb{Z}$-independent, and $k \leq n$. Let M be the $\mathbb{Z}$-submodule of $\mathbb{Z}_K$ generated by $e_1, \ldots, e_k$. Note that any $y \in \mathbb{Z}_K$ with $y \notin M$ satisfies $y \in x\mathbb{Z}_K$.

Assume by contradiction that $\mathbb{Z}_K/M$ is not free, and let $y \in \mathbb{Z}_K \setminus M$ and $m \in \mathbb{Z}_{\geq 2}$ be such that $y \notin M$ but $my \in M$. Since $y \in x\mathbb{Z}_K$, $my \in M \cap x\mathbb{Z}_K \cong a_1\mathbb{Z}e_1 \oplus \cdots \oplus a_k\mathbb{Z}e_k$. Write $my = a_1b_1e_1 + \cdots + a_kb_ke_k$. Then $m|a_ib_i$ for all i, but then $y = \sum_i \frac{a_ib_i}{m} e_i \in M$, a contradiction.

Thus $\mathbb{Z}_K/M$ is free, so $e_1, \ldots, e_k$ can be extended via $f_1, \ldots, f_{n-k}$ to a $\mathbb{Z}$-basis of $\mathbb{Z}_K/M$. Then

$$\mathbb{Z}_K/x\mathbb{Z}_K = (\mathbb{Z}/\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/\mathbb{Z}) \oplus (\mathbb{Z}/a_1\mathbb{Z}) \oplus (\mathbb{Z}/a_k\mathbb{Z})$$

and

$$x\mathbb{Z}_K = \mathbb{Z}f_1 \oplus \cdots \oplus \mathbb{Z}f_{n-k} \oplus a_1\mathbb{Z}e_1 \oplus \cdots \oplus a_k\mathbb{Z}e_k,$$

where $1|\cdots|1|a_1|\cdots|a_n$, as desired.

6. Deduce that for all $x \in \mathbb{Z}_K$, we have $|N(x)| = |x\mathbb{Z}_K|$, where the right-hand side is the norm of a principal ideal.

Solution: Taking the norm of a principal ideal, we have by the previous question that

$$|x\mathbb{Z}_K| = \prod_{j=1}^{n} a_j.$$

Let $\{e_j\}_{j=1}^n$ be the basis described in the previous question. Consider the elements $f_1, \ldots, f_n$ of $\mathbb{Z}_K$ such that $xf_j = e_j$ for all j. Note that the f_i's are a $\mathbb{Q}$-basis of K, since multiplication by x is an invertible map on K, and thus $\mathbb{Q}$- (and thus $\mathbb{Z}$-) linearly independent. Moreover, for each $z \in \mathbb{Z}_K$, there exist coefficients $b_i \in \mathbb{Z}_K$ such that

$$xz = b_1a_1e_1 + \cdots + b_na_ne_n = x(b_1f_1 + \cdots + b_nf_n),$$

and thus $z = b_1f_1 + \cdots + b_nf_n$, so the $\mathbb{Z}$-span of the f_i's is $\mathbb{Z}_K$. Thus the f_i's form a $\mathbb{Z}$-basis of $\mathbb{Z}_K$. Let S be the invertible change of basis matrix from e_j to f_j; then written in the basis e_j, we have

$$m_xS = \begin{bmatrix} \pm a_1 & 0 & \cdots & 0 \\ 0 & \pm a_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \pm a_n, \end{bmatrix}$$

$$|N(x)| = |\det(m_x)| = |\det(m_x)||\det(S)| = |\det(m_x S)| = \prod_{j=1}^{n} a_j = |x\mathbb{Z}_K|,$$

where we are using that $|\det(S)| = 1$ by invertability of S. This completes the argument.

2. A number field K is said to be *euclidean* (with respect to the norm) if, for any x and y in $\mathbb{Z}_K$, with $y \neq 0$, there exists q and r in $\mathbb{Z}_K$ with $|N(r)| < |N(y)|$ such that $x = qy+r$.

1. Show that if K is euclidean, then the class group of K is trivial.

   Solution: Let $I \subset \mathbb{Z}_K$ be an ideal. We would like to show that I is principal. By the previous problem, for all nonzero $x \in I$, $N(x) \in \mathbb{Z}$ and $N(x) \neq -1, 0, 1$ (since if $N(x) = \pm 1$ then I contains a unit). Let $a \in I$ be a nonzero element such that $|N(a)|$ is minimal. Then $a\mathbb{Z}_K \subset I$, so it remains to show that $I \subset a\mathbb{Z}_K$. Let $b \in I$ be an arbitrary nonzero element. Since K is euclidean, there exist q and r with $b = aq + r$ and $|N(r)| < |N(a)|$. But then $r \in I$, so by the minimality of a, we must have $N(r) = 0$ and thus $r = 0$. This implies that $b = aq$, and thus $b \in a\mathbb{Z}_K$, so we have $I \subset a\mathbb{Z}_K$. Thus I is principal, as desired.

2. Show that $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$ are euclidean.

   Solution: For each we provide a euclidean algorithm, that is, an algorithm for producing q and r.

   Let $a + b\sqrt{-2}, c + d\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$. Let $e, f \in \mathbb{Q}$ be such that

   $$\frac{a + b\sqrt{-2}}{c + d\sqrt{-2}} = e + f\sqrt{-2}.$$

   Now pick $q, s \in \mathbb{Z}$ such that $|e - q| \leq 1/2$ and $|f - s| \leq 1/2$. Then

   $$\begin{aligned} a + b\sqrt{-2} &= (c + d\sqrt{-2})(e + f\sqrt{-2}) \\ &= (c + d\sqrt{-2})(q + s\sqrt{-2} + (e - q) + (f - s)\sqrt{-2}) \\ &= (c + d\sqrt{-2})(q + s\sqrt{-2}) + (c + d\sqrt{-2})((e - q) + (f - s)\sqrt{-2}). \end{aligned}$$

   Note that $(c + d\sqrt{-2})(q + s\sqrt{-2}) \in \mathbb{Z}_K$, so the second product must be as well. It suffices to show that $N(c + d\sqrt{-2}) > N((c + d\sqrt{-2})((e - q) + (f - s)\sqrt{-2}))$. But $N((e-q)+(f-s)\sqrt{-2}) =\leq (1/2)^2+2(1/2)^2 = 3/4 < 1$, so by multiplicativity of the norm this inequality must hold. Thus $q+s\sqrt{-2}$ and $(c+d\sqrt{-2})((e-q)+(f-s)\sqrt{-2})$ are the desired values.

   The argument for $\mathbb{Z}[\sqrt{2}]$ is nearly identical, with perhaps the one difference being that for $|e - q| \leq 1/2$ and $|f - s| \leq 1/2$, we have

   $$|N((e - q) + (f - s)\sqrt{2})| = |(e - q)^2 - 2(f - s)^2| \leq 1/2 < 1.$$

3. Let K be a euclidean number field. Show that there exists a non-zero element $\delta \in \mathbb{Z}_K$, which is not a unit, and has the following property: the restriction to $\mathbb{Z}_K^\times \cup \{0\}$ of the reduction map modulo δ is surjective (i.e., any element of $\mathbb{Z}_K$ is congruent modulo δ to either 0 or a unit of $\mathbb{Z}_K$.)

   Solution: Define $\delta \in \mathbb{Z}_K^\times$ to be an element of minimal norm among non-units in $\mathbb{Z}_K^\times$. Let $a \in \mathbb{Z}_K$ be an arbitrary element. Since K is euclidean there exist $q, r \in \mathbb{Z}_K$ such that $a = q\delta + r$ and $|N(r)| < |N(\delta)|$. Since δ has minimal norm, r must be either zero or a unit. But this directly implies that a is congruent modulo δ either to zero or to a unit of $\mathbb{Z}_K$.

4. Determine all possible choices of the element δ of the previous question for $K = \mathbb{Q}$, and determine one choice for $K = \mathbb{Q}(i)$?

   Solution: First say $K = \mathbb{Q}$, so that $\mathbb{Z}_K = \mathbb{Z}$. The units of $\mathbb{Z}$ are ± 1, so we would like to find δ such that every element of $\mathbb{Z}/\delta\mathbb{Z}$ is congruent to 0 or ± 1. Thus there can be at most 3 elements of $\mathbb{Z}/\delta\mathbb{Z}$, and equivalently $|\delta| \leq 3$. Since δ is not a unit, $\delta \in \{\pm 2, \pm 3\}$; any of these choices work.

   Now let $K = \mathbb{Q}(i+1)$. Let $\delta = 1 + i$. Then $(1+i)\mathbb{Z}[i]$ contains $1+i$ as well as $2 = (1+i)(1-i)$ and $2i = (1+i)^2$, so that $\bar{0}$ and $\bar{1}$ are a set of representatives of $\mathbb{Z}[i]/(1+i)\mathbb{Z}[i]$, as desired.

5. Deduce that $\mathbb{Q}(\sqrt{-19})$ and $\mathbb{Q}(\sqrt{-163})$ are not euclidean. (Hint: determine the units in the corresponding rings of integers.) Note: one can show that both of these fields have trivial class group, so the statement in Question 1 is not an equivalence.

   Solution: Start with $\mathbb{Q}(\sqrt{-19})$, which has ring of integers $\mathbb{Z}_{19} = \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$. The norm of $a + b\left(\frac{1+\sqrt{-19}}{2}\right) \in \mathbb{Z}_{19}$ is $a^2 + ab + 5b^2$, and by for example the quadratic equation one can see that the only units in $\mathbb{Z}_{19}$ are ± 1.

   Assume by contradiction that $\mathbb{Q}(\sqrt{-19})$ is not euclidean and define δ as in part 4. Then $|\delta\mathbb{Z}_{19}| \leq 3$, where $|\delta\mathbb{Z}_{19}|$ is the norm of the ideal, since each congruence class must be represented by ± 1 or 0. The only possible residue rings of size ≤ 3 are modulo primes dividing 2 and 3, but since $-19 \equiv 1 \mod 4$, 2 is inert in $\mathbb{Q}(\sqrt{-19})$. Also, $-19 \equiv 2 \mod 3$ and thus $\left(\frac{-19}{3}\right) = -1$, so 3 is also inert in $\mathbb{Z}_{19}$.

   The argument for $\mathbb{Q}(\sqrt{163})$ is nearly identical, so we omit it.

3. Prove that any prime number p such that $p \equiv 1 \bmod 8$ or $p \equiv 7 \bmod 8$ is of the form $a^2 - 2b^2$, where a and b are integers. Show that there are infinitely many such representations. (Hint: use the field $\mathbb{Q}(\sqrt{2})$.)

Solution: Let p be a prime congruent to 1 or 7 mod 8. Then (for example by exercise sheet 2, problem 2.4) the Legendre symbol $\left(\frac{2}{p}\right) = 1$. By example 2.7.5, $\mathbf{p}$ is unramified and totally split in $\mathbb{Q}(\sqrt{2})$. Let $\mathbf{p} = \mathbf{p}_1\mathbf{p}_2$ as ideals in $\mathbb{Z}[\sqrt{2}]$. Since $\mathbb{Z}[\sqrt{2}]$ has class number 1 (for example because it is euclidean), there exists a generator π_1 of $\mathbf{p}_1$, which has norm p. Then for some $a_0, b_0 \in \mathbb{Z}$, $\pi_1 = a_0 + b_0\sqrt{2}$. Since π_1 is a generator, $|N(\pi_1)| = |\pi_1\mathbb{Z}[\sqrt{2}]| = p$, so $a_0^2 - 2b_0^2 = \pm p$.

Let u be a fundamental unit of $\mathbb{Z}[\sqrt{2}]$ (say $u = 1+\sqrt{2}$), and note that $N(u) = -1$. For all $n \in \mathbb{N}$, $u^n\pi_1$ represent pairwise distinct elements of $\mathbb{Z}[\sqrt{2}]$, so if $u^n\pi_1 = a_n + b_n\sqrt{2}$, we have $(a_i, b_i) \neq (a_j, b_j)$ for all $i \neq j$. But $N(u^n\pi_1) = a_n^2 - 2b_n^2 = (-1)^n N(\pi_1)$, so either odd values or even values of n furnish infinitely many solutions to $a^2 - 2b^2 = p$.

4. Let d be a squarefree positive integer such that $-d \not\equiv 1 \bmod 4$. Assume that d is not a prime number. The goal of this exercise is to prove that the class group of $K = \mathbb{Q}(\sqrt{-d}) = \mathbb{Q}(i\sqrt{d})$ is not trivial.

1. Prove that there exist integers a, b with $1 < a < b$ such that $d = ab$.

   Solution: Since d is not prime, d admits a factorization $d = ab$ where a and b are nonunits, so we can assume that $1 < a$ and $1 < b$. Assume without loss of generality that $a \leq b$. If $a = b$, then $d = a^2$, which contradicts d being squarefree, so $a < b$ as desired.

2. Let u and $v \neq 0$ be integers. Show that any element of $(u + v\sqrt{-d})\mathbb{Z}_K$ has norm $\geq d$.

   Solution: The norm of $x + y\sqrt{d} \in \mathbb{Z}_K$ is $x^2 + dy^2$, which is always nonnegative and in fact ≥ 1 for x and y not both zero. If $v \neq 0$, then $v^2 \geq 1$. Thus for any $x \in \mathbb{Z}_K$ nonzero,

$$N((u + v\sqrt{-d}x) \geq N(u + v\sqrt{-d})N(x) \geq u^2 + dv^2 \geq dv^2 \geq d,$$

   as desired.

3. Prove that the ideal generated by a and $i\sqrt{d}$ in $\mathbb{Z}_K$ is not principal.

   Solution: Let I be the ideal generated by a and $i\sqrt{d}$. Note that $1 \notin I$, since for any $x + iy\sqrt{d}, z + iw\sqrt{d} \in \mathbb{Z}_K$,

$$\begin{aligned} 1 = (x + iy\sqrt{d})a + (z + iw\sqrt{d})i\sqrt{d} &\Leftrightarrow 1 = (ax - wd) + (ay + z)i\sqrt{d} \\ &\Leftrightarrow \begin{cases} ax - wd &= 1 \\ ay + z &= 0. \end{cases} \end{aligned}$$

   But $ax - wd = a(x - wb) \neq 1$ since $a > 1$, so this is impossible.

   We now show that I is not principal. Assume by contradiction that $I = (x + iy\sqrt{d})\mathbb{Z}_K$. Then $|N(x+iy\sqrt{d})| = |I|$, which must divide $|N(a)| = a^2$ and $|N(i\sqrt{d})| = d$. Since d is squarefree, $\gcd(a, b) = 1$, and $\gcd(a^2, d) = a$. Thus $|N(x + iy\sqrt{d})|$ divides $a < d$. By part 2, this implies that $y = 0$; otherwise $|N(x + iy\sqrt{d})| \geq d$. Thus $I = x\mathbb{Z}_K$ with $x \in \mathbb{Z}$. Since $i\sqrt{d} \in I$, this implies that $x = 1$ and $I = \mathbb{Z}_K$, a contradiction.

5. The goal of this exercise is to prove that the Fermat equation $x^3 + y^3 = z^3$ has no integral solution with $xyz \neq 0$, which was first proved by Euler. This is a fairly long exercise – the more interesting part start at Question 3, and the first two questions may be assumed without proof.

We denote $\omega = e^{2i\pi/3} = (-1+i\sqrt{3})/2$ and $K = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\omega)$. We have $\mathbb{Z}_K = \mathbb{Z}[\omega]$.

We consider the equation

$$x^3 + y^3 = uz^3 \tag{1}$$

where $u \in \mathbb{Z}_K^\times$ is a parameter and the unknowns (x, y, z) are in $\mathbb{Z}_K$.

1. Show that $\mathbb{Z}_K$ is a euclidean domain and that $\mathbb{Z}_K^\times = \{-1, 1, \omega, \omega^2, -\omega, -\omega^2\}$.
Solution: Note that for $a, b \in \mathbb{Z}$, $N(a + b\omega) = (a + b\omega)(a + b\bar{\omega}) = a^2 - ab + b^2$.
We now show that $\mathbb{Z}_K$ is euclidean; this argument is very similar to problem 2.2. For $a + b\omega, c + d\omega \in \mathbb{Z}_K$, let $e, f \in \mathbb{Q}$ such that

$$\frac{a + b\omega}{c + d\omega} = e + f\omega.$$

Let $q, s \in \mathbb{Z}$ such that $|e - q| \leq \frac{1}{2}$ and $|f - s| \leq \frac{1}{2}$, and consider the elements $\varkappa = q + s\omega \in \mathbb{Z}_K$ and $\varrho = a + b\omega - \varkappa(c + d\omega) \in \mathbb{Z}_K$. The elements $\varkappa$ and ϱ satisfy the constraints on q and r respectively if we can show that $|N(\varrho)| < |N(c + d\omega)|$. But

$$\begin{aligned} |N(\varrho)| &= |N(c + d\omega)||N(\tfrac{a+b\omega}{c+d\omega} - \varkappa)| \\ &= |N(c + d\omega)||N((e - q) + (f - s)\omega)| \\ &= |N(c + d\omega)||(e - q)^2 - (e - q)(f - s) + (f - s)^2| \\ &\leq \frac{3}{4}|N(c + d\omega)| < |N(c + d\omega)|. \end{aligned}$$

By problem 1.4, $a + b\omega \in \mathbb{Z}_K$ is a unit if and only if $N(a + b\omega) = \pm 1$, which happens if and only if $a^2 - ab + b^2 = \pm 1$. If $a^2 - ab + b^2 = 1$, then

$$a = \frac{b \pm \sqrt{b^2 - 4(b^2 - 1)}}{2} = \frac{b \pm \sqrt{4 - 3b^2}}{2}.$$

This has (real) integer solutions only if $b = 0$ or $b = \pm 1$. If $b = 0$, then $a = \pm 1$, corresponding to the units ± 1; if $b = 1$, then $a = 0$ or $a = 1$, corresponding to the units ω and $1 + \omega = -\omega^2$ respectively; and if $b = -1$, then $a = -1$ or $a = 0$, corresponding to the units $-1 - \omega = \omega^2$ and $-\omega$ respectively.

2. Let $\lambda = 1 - \omega$. Show that $\lambda\mathbb{Z}_K$ is a prime ideal with norm 3. In particular, the field $\mathbb{Z}_K/\lambda\mathbb{Z}_K$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$. We denote by v the λ-adic valuation on (non-zero) ideals.
Solution: First note that $\omega \equiv 1 \mod \lambda$, and thus

$$3 \equiv 1 + 2\omega \equiv 1 + \omega + \omega^2 = 0 \mod \lambda.$$

Then for any $a, b \in \mathbb{Z}$,

$$a + b\omega \equiv a + b \mod \lambda,$$

and thus by combining both of these we get that $a + b\omega$ modulo λ is given by the value of $a + b$ modulo 3. Thus $\mathbb{Z}_K/\lambda\mathbb{Z}_K$ is either trivial or isomorphic to $\mathbb{Z}/3\mathbb{Z}$. Since $N(\lambda) = N(1 - \omega) = 1 + 1 + 1 = 3$, $\mathbb{Z}_K/\lambda\mathbb{Z}_K$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$. Since this is a domain, $\lambda\mathbb{Z}_K$ must be prime.

3. Show that if $x \in \mathbb{Z}_K$ satisfies $x \equiv 1 \bmod \lambda$, then $x^3 \equiv 1 \bmod \lambda^4$. (Hint: write $x^3 - 1 = (x-1)(x-\omega)(x-\omega^2)$ and use the fact that $\omega^2 \equiv 1 \bmod \lambda$.)

   Solution: Since $x \equiv 1 \mod \lambda$, we also have $x \equiv \omega$ and $x \equiv \omega^2 \mod \lambda$, so λ divides each of $(x-1)$, $(x-\omega)$, and $(x-\omega^2)$.

   Now note that $\frac{x-1}{\lambda} + 1 = \frac{x-1+\lambda}{\lambda} = \frac{x-\omega}{\lambda}$, and similarly $\frac{x-\omega}{\lambda} + 1 = \frac{x-\omega^2}{\lambda}$. Thus the three values $\frac{x-1}{\lambda}$, $\frac{x-\omega}{\lambda}$, and $\frac{x-\omega^2}{\lambda} \in \mathbb{Z}_K$ must represent the three different elements of $\mathbb{Z}_K/\lambda\mathbb{Z}_K$, so one of these three values is divisible by λ. Equivalently, one of $x-1$, $x-\omega$, and $x-\omega^2$ is divisible by λ^2, so there are at least four factors of λ dividing $(x-1)(x-\omega)(x-\omega^2) = x^3 - 1$. Thus $x^3 \equiv 1 \mod \lambda^4$.

4. Show that (1) has no solution with λ not dividing xyz. (Hint: reduce modulo λ and check cases.)

   Solution: Note that the same argument in the previous part with the polynomial $x^3 + 1 = (x+1)(x+\omega)(x+\omega^2)$ shows that if $x \equiv -1 \mod \lambda$, then $x^3 \equiv -1 \mod \lambda^4$.

   Assume by contradiction that x, y, z satisfy (1) and λ does not divide xyz. Then x, y, z are all nonzero mod λ. By multiplying x, y, and z by -1 if necessary, we can assume that $x \equiv 1 \mod \lambda$.

   Assume first that $y \equiv -1 \mod \lambda$. Then

   $$uz^3 \equiv x^3 + y^3 \equiv 1 - 1 \equiv 0 \mod \lambda^4,$$

   so by multiplying both sides by u^{-1} we get $z^3 \equiv 0 \mod \lambda^4$, and thus $\lambda | z$, so $\lambda | xyz$, a contradiction.

   Now assume that $y \equiv 1 \mod \lambda$. Then $x^3 + y^3 \equiv 2 \mod \lambda^4$. We also know that $z \equiv \pm 1 \mod \lambda$, and thus $z^3 \equiv \pm 1 \mod \lambda^4$, so $2 \equiv \pm u \mod \lambda^4$ or equivalently $\lambda^4 | (2 \pm u)$. But this is impossible; for example note that $N(\lambda^4) = N(\lambda)^4 = 81$, whereas $N(2 \pm u) \in \{1, 3, 7, 9\}$ for the units in $\mathbb{Z}_K$.

5. Let (x, y, z) be a solution of (1) for a given $u \in \mathbb{Z}_K^\times$ with $v(xy) = 0$. Show that $v(z) \geq 2$. (Hint: use the previous question and reduce modulo λ^2.)

   Solution: From the previous question, we can assume that $x \equiv 1 \mod \lambda$, and the case when $y \equiv 1 \mod \lambda$ is impossible, so $y \equiv -1 \mod \lambda$. Then as before this implies that $z^3 \equiv 0 \mod \lambda^4$. Thus $3v(z) \geq 4$, so $v(z) \geq 2$.

6. We fix from now on a solution (x, y, z) of (1) for a given $u \in \mathbb{Z}_K^\times$ with $v(xy) = 0$ and x coprime to y. Show that one of $x + y$, $x + \omega y$ or $x + \omega^2 y$ has λ-valuation ≥ 2, and that one may assume that $x + y$ has this property, which we consider to be the case from now on.

   Solution: As before, we know that

   $$\begin{aligned} x^3 + y^3 &\equiv 0 \mod \lambda^4 \\ \Rightarrow (x+y)(x+\omega y)(x+\omega^2 y) &\equiv 0 \mod \lambda^4 \\ \Rightarrow v(x+y) + v(x+\omega y) + v(x+\omega^2 y) &\geq 4. \end{aligned}$$

   Thus at least one of the three must be ≥ 2.

Note that we can always replace y by ωy or $\omega^2 y$, and the triple (x, y, z) is a solution of (1) if and only if $(x, \omega y, z)$ and $(x, \omega^2 y, z)$ are, because $y^3 = (\omega y)^3 = (\omega^2 y)^3$. This substitution permutes transitively the values $x + y$, $x + \omega y$, and $x + \omega^2 y$, so we can always fix (x, y, z) satisfying this question and such that $v(x + y) \geq 2$.

7. Show then that $v(x + \omega y) = v(x + \omega^2 y) = 1$ and that $v(x + y) = 3v(z) - 2$.

   Solution: Since

$$x + \omega y = x + y + \lambda y,$$

   we can reduce modulo λ^2 to get

$$x + \omega y \equiv \lambda y \mod \lambda^2.$$

   Since $y \equiv \pm 1 \not\equiv 0 \mod \lambda$, $\lambda y \not\equiv 0 \mod \lambda^2$. Thus $\lambda | (x + \omega y)$ but $\lambda^2 \nmid (x + \omega y)$, so $v(x + \omega y) = 1$. By the same argument with $-\lambda y$ in place of $+\lambda y$ we get that $v(x + \omega^2 y) = 2$.

   Since (x, y, z) are a solution to (1), we have

$$\begin{aligned} x^3 + y^3 &= uz^3 \\ \Rightarrow (x + y)(x + \omega y)(x + \omega^2 y) &= uz^3 \\ \Rightarrow v(x + y) + v(x + \omega y) + v(x + \omega^2 y) &= v(u) + 3v(z). \end{aligned}$$

   Since λ is prime and u is a unit, $v(u) = 0$. Then

$$\begin{aligned} \Rightarrow v(x + y) + 2 &= 3v(z) \\ \Rightarrow v(x + y) &= 3v(z) - 2, \end{aligned}$$

   as desired.

8. Show that $\gcd(x+y, x+\omega y) = \gcd(x+y, x+\omega^2 y) = \gcd(x+\omega y, x+\omega^2 y) = \lambda \mathbb{Z}_K$ (where the gcds are in the sense of ideals).

   Solution: Let π be any irreducible with $(\pi) \neq (\lambda)$. Assume by contradiction that $\pi | (x+y)$ and $\pi | (x+\omega y)$. Then $\pi | (1-\omega) y = \lambda y$, and similarly $\pi | (x+\omega y-\omega(x+y)) = (1 - \omega)x = \lambda x$, so since $(\pi) \neq (\lambda)$ we have $\pi | y$ and $\pi | x$. But x is coprime to y, a contradiction.

   Since $v(x + y), v(x + \omega y)$, and $v(x + \omega^2 y)$ are all ≥ 1, all of these gcds must be contained in $\lambda \mathbb{Z}_K$ but not in $\lambda^2 \mathbb{Z}_K$; thus they are all $\lambda \mathbb{Z}_K$.

9. Deduce that there exist units (ξ, η, ϑ) and elements (a, b, c) of $\mathbb{Z}_K$, each coprime to λ, such that

$$\xi a^3 \lambda^{v(x+y)} + \omega \eta b^3 \lambda + \omega^2 \vartheta c^3 \lambda = 0.$$

   (Hint: use unique factorization in $\mathbb{Z}_K$ and combine the resulting expressions for $x + y$, $x + \omega y$, $x + \omega^2 y$.)

   Solution: Since the three factors of $x^3 + y^3 (= uz^3)$ share no prime factors apart from λ, but the product is a cube, each prime appearing in the prime factorization of each of $(x+y)$, $(x+\omega y)$, and $(x+\omega^2 y)$ must appear to a cubic power. By unique factorization, there must therefore exist units ξ, η, and ϑ and elements $a, b, c \in \mathbb{Z}_K$ coprime to λ such that

$$\begin{aligned} x + y &= \xi a^3 \lambda^{v(x+y)}, \\ x + \omega y &= \eta b^3 \lambda, \\ x + \omega^2 y &= \vartheta c^3 \lambda. \end{aligned}$$

Thus

$$\begin{aligned} \xi a^3 \lambda^{v(x+y)} + \omega \eta b^3 \lambda + \omega^2 \vartheta c^3 \lambda &= (x+y) + \omega(x + \omega y) + \omega^2(x + \omega^2 y) \\ &= (1 + \omega + \omega^2)x + (1 + \omega^2 + \omega)y \\ &= 0, \end{aligned}$$

as desired.

10. Deduce that there exist units ϵ and ϵ' and elements r, s and $t \in \mathbb{Z}_K$ such that

$$r^3 + \epsilon s^3 = \epsilon' t^3$$

and $v(t) = v(z) - 1$.

Solution: We can divide the previous equation by λ and do some algebraic manipulations, recalling that $v(x+y) = 3v(z) - 2$, to get

$$\begin{aligned} \xi a^3 \lambda^{v(x+y)-1} + \omega \eta b^3 + \omega^2 \vartheta c^3 &= 0 \\ \Rightarrow \omega \eta b^3 + \omega^2 \vartheta c^3 &= -\xi a^3 \lambda^{3(v(z)-1)} \\ \Rightarrow b^3 + \omega \eta^{-1} \vartheta c^3 &= -\omega^2 \eta^{-1} \xi (a \lambda^{v(z)-1})^3. \end{aligned}$$

Choosing $r = b$, $s = c$, $t = a\lambda^{v(z)-1}$, and $\epsilon = \omega \eta^{-1} \vartheta$ and $\epsilon' = -\omega^2 \eta^{-1} \xi$, satisfies the constraint. Note that a and λ are relatively prime, so that $v(t) = v(\lambda^{v(z)-1}) = v(z) - 1$.

11. Show that $\epsilon \in \{-1, 1\}$ and deduce that there is a solution (x', y', z') of (1), possibly for a different unit than u, with $v(z') = v(z) - 1$.

Solution: Since $r = a$ and $s = c$ are relatively prime to λ, we must have $r = \pm 1 \mod \lambda$ and thus $r^3 = \pm 1 \mod \lambda^4$, and the same for s. Also, $v(z) \geq 2$, so $v(t) \geq 1$ and $v(t^3) > 2$. Thus

$$\begin{aligned} r^3 + \epsilon s^3 &\equiv 0 \mod \lambda^2 \\ \Rightarrow \pm 1 \pm \epsilon &\equiv 0 \mod \lambda^2, \end{aligned}$$

so that $\lambda^2 | (\epsilon \pm 1)$. By looking at the set of units individually and, for example, comparing norms, one can see that this is only possible when $\epsilon \pm 1 = 0$, or when $\epsilon = \pm 1$.

If $\epsilon = \pm 1$ then $\epsilon = \epsilon^3$, so by choosing $x' = r$, $y' = \epsilon s$, and $z' = t$, we get a different solution of (1), possibly for a different unit than u, with $v(z') = v(z) - 1$.

12. Conclude that (1), and the Fermat equation with exponent 3, have no solutions with $xyz \neq 0$. (This method of proof is known as *infinite descent*, and has its origin in the proof by Fermat himself that the equation for exponent 4 has no solution, which is easier as it does not require any algebraic number theory.)

    Solution: Note that shared factors of x and y must also be shared by z and thus can be divided out, so it suffices to consider solutions with x and y relatively prime.

    We can also assume without loss of generality that $v(xy) = 0$; if say $\lambda | x$, then $x^3 = (-y)^3 + uz^3$, and by the same argument in part 11 we have $u = \pm 1$, so we have a new solution $(-y, \pm z, x)$ where λ does not divide either of the first two coordinates.

    We showed in part 5 that $v(z) \geq 2$ for any such solution, so there exists a minimum attained value of $v(z)$ among these solutions. But we have also shown that a solution (x', y', z') exists with $v(z') < v(z)$, a contradiction.

Due date: 11.11.2024