Algebraic number theory
Solutions to exercise sheet for chapter 4

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 $d > 0$ be a squarefree integer, let $K = \mathbb{Q}(\sqrt{-d})$ and let Δ_K be the discriminant of K. Let p be a prime that splits in K and let $\mathfrak{p}$ be a prime ideal above p.*

1. *Prove that for all integers $i \geq 1$ such that $p^i < |\Delta_K|/4$, the ideal $\mathfrak{p}^i$ is not principal. Hint: consider the cases $\Delta_K = -d$ and $\Delta_K = -4d$ separately.*

   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 $\Delta_K = -4d$, 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 z be a generator. Then the norm of z is p^i, giving $x^2 + dy^2 = p^i$, so $y^2 \leq p^i/d < 1$, so $y = 0$. But then $z \in \mathbb{Z}$ has norm $z^2 = p^i$, so z is divisible by p. But this is impossible since $\mathfrak{p}^i$ is not divisible by (p).
   - If $\Delta_K = -d$, 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 z be a generator. Then the norm of z is p^i, so $y^2 \leq 4p^i/d < 1$, so $y = 0$ and as before z is divisible by p, which is impossible.

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

   The number of i as in the previous question is
   $$\left\lfloor \frac{\log(|\Delta_K|/4)}{\log p} \right\rfloor$$
   so, accounting for the trivial class, we have
   $$h_K \geq 1 + \left\lfloor \frac{\log(|\Delta_K|/4)}{\log p} \right\rfloor.$$

Exercise 2. *Let* $K = \mathbb{Q}(\sqrt{-87})$.

1. *Write down without proof the ring of integers, the discriminant and the signature of* K.

   Since $-87 = -3 \cdot 29$ is squarefree and $-87 \equiv 1 \bmod 4$, the ring of integers of K is $\mathbb{Z}_K = \mathbb{Z}[\alpha]$ with $\alpha = \frac{1+\sqrt{-87}}{2}$, the discriminant is $\Delta_K = -87$ and the signature is $(0, 1)$.

2. *Describe all the integral ideals of* K *of norm up to* 5 *(give generators for some prime ideals, and express the integral ideals as products of these prime ideals). What does this tell you about the class number of* K*?*

   We first compute the decomposition of primes up to 5. Note that the minimal polynomial of α is $x^2 - x + 22$.

   - Since $-87 \equiv 1 \bmod 8$, the prime 2 splits. Since $\mathbb{Z}[\alpha]$ is 2-maximal and $x^2 - x + 22 \equiv x(x+1) \bmod 2$, we have $(2) = \mathfrak{p}_2\mathfrak{p}_2'$ with $\mathfrak{p}_2 = (2, \alpha+1)$ and $\mathfrak{p}_2' = (2, \alpha)$.
   - Since 87 is divisible by 3, the prime 3 is ramified. Since $\mathbb{Z}[\alpha]$ is 3-maximal and $x^2 - x + 22 \equiv x^2 + 2x + 1 \equiv (x+1)^2 \bmod 3$, we have $(3) = \mathfrak{p}_3^2$ with $\mathfrak{p}_3 = (3, \alpha + 1)$.
   - Since $-87 \equiv 3 \bmod 5$ is not a square modulo 5, the prime 5 is inert in K.

   The integral ideals of K of norm up to 5 are $\mathbb{Z}_K, \mathfrak{p}_2, \mathfrak{p}_2', \mathfrak{p}_3, \mathfrak{p}_2^2, (2)$, and $\mathfrak{p}_2'^2$. The Minkowski bound is

   $$M_K = \frac{2}{4} \cdot \frac{4}{\pi}\sqrt{87} \approx 5.94 < 6,$$

   so every ideal class is represented by an integral ideal of norm at most 5. Since (2) is principal, this implies that $h_K \leq 6$.

3. *Factor the ideal* $(\frac{3+\sqrt{-87}}{2})$ *into primes.*

   We have $z = \frac{3+\sqrt{-87}}{2} = 1 + \alpha$, so this element z is an integer, and $N_{\mathbb{Q}}^K(z) = (3/2)^2 + 87(1/2)^2 = 24 = 3 \cdot 8$. Since (z) is an integral ideal, (z) is a product of a prime of norm 3 and an integral ideal of norm 8. There is only one prime of norm 3, namely $\mathfrak{p}_3$. The integral ideals of norm 8 are $\mathfrak{p}_2^3$, $2\mathfrak{p}_2$, $2\mathfrak{p}_2'$ and $\mathfrak{p}_2'^3$. Since $z = 1 + \alpha$ is not divisible by 2 and $z = 1 + \alpha \in \mathfrak{p}_2$, we obtain

   $$(z) = \mathfrak{p}_2^3\mathfrak{p}_3.$$

4. *Prove that* $\mathrm{Cl}(K) \cong \mathbb{Z}/6\mathbb{Z}$.

   By Minkowski's theorem, the class group is generated by $\mathfrak{p}_2, \mathfrak{p}_2'$ and $\mathfrak{p}_3$. By the decomposition of primes, we have the relations $[\mathfrak{p}_2'] = [\mathfrak{p}_2]^{-1}$ and $[\mathfrak{p}_3]^2 = 1$. By Question 3 we have the additional relation $[\mathfrak{p}_2]^3 = [\mathfrak{p}_3]^{-1} = [\mathfrak{p}_3]$. Since $[\mathfrak{p}_3]$ is of order 1 or 2, the class $[\mathfrak{p}_2]$ is of order 1, 3 or 6. By Exercise 1, $\mathfrak{p}_2^3$ is not principal since $2^3 < 87/4$, so $\mathfrak{p}_2$ has order 6. By Question 2, we obtain $\mathrm{Cl}(K) \cong \mathbb{Z}/6\mathbb{Z}$, with generator $[\mathfrak{p}_2]$.

Exercise 3. *In this exercise we consider the equation*

$$y^2 = x^5 - 2, \quad x, y \in \mathbb{Z}.$$

1. *Let $K = \mathbb{Q}(\sqrt{-2})$. Write down the signature, the discriminant, the ring of integers and then class number of K.*

   The integer -2 is squarefree and we have $-2 \equiv 2 \bmod 4$, so the ring of integers of K is $\mathbb{Z}_K = \mathbb{Z}[\sqrt{-2}]$, the discriminant is $\Delta_K = -8$. The signature of K is $(0, 1)$. Since the Minkowski bound is

   $$M_K = \frac{2}{4} \cdot \frac{4}{\pi}\sqrt{8} \approx 1.80 < 2,$$

   the class number of K is $h_K = 1$.

2. *Let (x, y) be a solution of the equation. Prove that the ideals $(y+\sqrt{-2})$ and $(y-\sqrt{-2})$ are coprime. Hint: reduce the equation modulo 4 to prove that y must be odd.*

   If y is even, then modulo 4 we obtain $0 = x^5 - 2$, but 2 is not a 5-th power in $\mathbb{Z}/4\mathbb{Z}$ so y is odd.

   Let $\mathfrak{p}$ be a prime dividing both $(y + \sqrt{-2})$ and $(y - \sqrt{-2})$. The it divides the difference $2\sqrt{-2}$, which has norm a power of 2. Since 2 is ramified, there is a unique prime $\mathfrak{p}_2$ above 2. Since $\sqrt{-2} \in \mathfrak{p}_2$, we have $y \in \mathfrak{p}_2$, but $\mathfrak{p}_2 \cap \mathbb{Z} = 2\mathbb{Z}$, so y is even, which is not possible. So $(y + \sqrt{-2})$ and $(y - \sqrt{-2})$ are coprime.

3. *You may assume without proof that $\mathbb{Z}_K^\times = \{\pm 1\}$. Prove that $y + \sqrt{-2}$ is a 5-th power in $\mathbb{Z}_K$.*

   Since $x^5 = (y + \sqrt{-2})(y - \sqrt{-2})$, and since $(y + \sqrt{-2})$ and $(y - \sqrt{-2})$ are coprime, the ideal $(y + \sqrt{-2})$ is a 5-th power. Since the class number of K is 1, we have $(y + \sqrt{-2}) = (a)^5 = (a^5)$ for some $a \in \mathbb{Z}_K$, and so $y + \sqrt{-2}$ is a 5-th power in $\mathbb{Z}_K$ up to a unit. But since $\mathbb{Z}_K^\times = \{\pm 1\}$, every unit is a 5-th power, so finally $y + \sqrt{-2}$ is a 5-th power in $\mathbb{Z}_K$.

4. *Prove that the equation has no solution.*

   Since $\mathbb{Z}_K = \mathbb{Z}[\sqrt{-2}]$, there exists $a, b \in \mathbb{Z}$ be such that $(a+b\sqrt{-2})^5 = y+\sqrt{-2}$. We expand

   $$(a + b\sqrt{-2})^5 = a^5 - 20b^2a^3 + 20b^4a + (5ba^4 - 20b^3a^2 + 4b^5)\sqrt{-2}.$$

   This gives $b(5a^4 - 20b^2a^2 + 4b^4) = 1$, so that $b = \pm 1$.

   - If $b = 1$, then $5a^4 - 20a^2 + 3 = 0$. The discriminant of $5x^2 - 20x + 3$ is $(-20)^2 - 4 \cdot 5 \cdot 3 = 20 \cdot 17$, which is not a square in $\mathbb{Q}$, so this polynomial does not have any roots in $\mathbb{Z}$. So there is no solution with $b = 1$.
   - If $b = -1$, then $5a^4 - 20a^2 + 5 = 0$, which simplifies into $a^4 - 4a^2 + 1 = 0$. The discriminant of $x^2 - 4x + 1$ is 12, which is not a square in $\mathbb{Q}$. Again, we have no solution.

So the equation has no solution.

UNASSESSED QUESTIONS

Exercise 4. *Let* $K = \mathbb{Q}(\sqrt{-29})$.

1. *Determine the ring of integers and discriminant of* K.

   Since -29 is squarefree and $-29 \equiv 3 \bmod 4$, we have $\mathbb{Z}_K = \mathbb{Z}[\sqrt{-29}]$ and the discriminant is $\Delta_K = -4 \cdot 29$. Let $\alpha = \sqrt{-29}$.

2. *Determine the decomposition of* 2, 3 *and* 5 *in* K.

   - $x^2+29 \equiv (x+1)^2 \bmod 2$, so 2 is ramified and $(2) = \mathfrak{p}_2^2$ with $\mathfrak{p}_2 = (2, \alpha+1)$.
   - $x^2 + 29 \equiv x^2 - 1 \equiv (x-1)(x+1) \bmod 3$, so 3 splits and $(3) = \mathfrak{p}_3\mathfrak{p}_3'$ where $\mathfrak{p}_3 = (3, \alpha+1)$ and $\mathfrak{p}_3' = (3, \alpha+2)$.
   - $x^2 + 29 \equiv x^2 - 1 \equiv (x-1)(x+1) \bmod 5$, so 5 splits and $(5) = \mathfrak{p}_5\mathfrak{p}_5'$ where $\mathfrak{p}_5 = (5, \alpha+1)$ and $\mathfrak{p}_5' = (5, \alpha+4)$.

3. *Factor the ideals* $(1+\sqrt{-29})$ *and* $(3+2\sqrt{-29})$ *into primes.*

   - We have $N_{\mathbb{Q}}^K(1+\alpha) = 1+29 = 30 = 2\cdot3\cdot5$. Clearly $1+\alpha \in \mathfrak{p}_3$ so $\mathfrak{p}_3 \mid (1+\alpha)$ and $1+\alpha \in \mathfrak{p}_5$ so $\mathfrak{p}_5 \mid (1+\alpha)$, so that $(1+\alpha) = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5$.
   - We have $N_{\mathbb{Q}}^K(3+2\alpha) = 3^2 + 29 \cdot 2^2 = 125 = 5^3$. Since $(5) \nmid 3+2\alpha$ and $3+2\alpha \equiv 3 + 2\cdot 1 \equiv 0 \bmod \mathfrak{p}_5'$, we have $(3+2\alpha) = (\mathfrak{p}_5')^3$.

4. *Determine the order in the class group of* K *of the images of the primes above* 2 *and of the primes above* 5.

   - Since $(2) = \mathfrak{p}_2$, the class $[\mathfrak{p}_2]$ has order 1 or 2. Since the equation $x^2+29y^2 = 2$ clearly has no integer solution, there is no element of norm 2 in $\mathbb{Z}_K$ so $\mathfrak{p}_2$ is not principal. So $[\mathfrak{p}_2]$ has order 2.
   - Since $(5) = \mathfrak{p}_5\mathfrak{p}_5'$, the classes $[\mathfrak{p}_5]$ and $[\mathfrak{p}_5']$ are inverse of each other and hence have the same order. Since $(3+2\alpha) = (\mathfrak{p}_5')^3$, the class $[\mathfrak{p}_5']$ has order 1 or 3. Since $5 < |\Delta_K|/4 = 29$, $\mathfrak{p}_5$ is not principal by Exercise 1. So $[\mathfrak{p}_5]$ and $[\mathfrak{p}_5']$ have order 3.

5. *Prove that* $\mathrm{Cl}(K) \cong \mathbb{Z}/6\mathbb{Z}$.

   The Minkowski bound is $M_K \approx 5.29$, so the class group $\mathrm{Cl}(K)$ is generated by the classes of prime ideals of norm up to 5. Since $(1+\alpha) = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5$, the class $[\mathfrak{p}_3]$ is in the subgroup generated by $[\mathfrak{p}_2]$ and $[\mathfrak{p}_5]$. Since $[\mathfrak{p}_3'] = [\mathfrak{p}_3]^{-1}$ and $[\mathfrak{p}_5'] = [\mathfrak{p}_5]^{-1}$, the class group is generated by $[\mathfrak{p}_2]$ and $[\mathfrak{p}_5]$. Since $[\mathfrak{p}_2]$ has order 2 and $[\mathfrak{p}_5]$ has order 3, the element $g = [\mathfrak{p}_2][\mathfrak{p}_5]$ generates the class group ($[\mathfrak{p}_2] = g^3$ and $[\mathfrak{p}_5] = g^4$) and has order 6, so $\mathrm{Cl}(K) \cong \mathbb{Z}/6\mathbb{Z}$.

Exercise 5 (Difficult)**.** *Let* K *be a number field, and let* $m \geq 1$ *be an integer. In this exercise we write* $\mathrm{Cl}(K)[m] = \{c \in \mathrm{Cl}(K) \mid c^m = 1\}$.

1. *Prove that if h_K is coprime to m, then $\mathrm{Cl}(K)[m] = \{1\}$.*

   Since h_K is coprime to m, there exists $u, v \in \mathbb{Z}$ such that $um + vh_K = 1$. Let $c \in \mathrm{Cl}(K)[m]$. Then $c = c^{um+vh_K} = (c^m)^u(c^{h_K})^v = 1$. So $\mathrm{Cl}(K)[m] = 1$.

2. *Let $G_m(K) = \{x^m : x \in K^\times\}$, and let $L_m(K)$ be the set of elements $x \in K^\times$ such that in the prime ideal factorisation of (x), all the exponents are multiples of m.*

   (a) *Prove that $G_m(K)$ is a subgroup of $L_m(K)$.*

   Let $x \in K^\times$, and let $(x) = \prod_i \mathfrak{p}_i^{a_i}$ be its prime ideal factorisation. Then $(x^m) = \prod_i \mathfrak{p}_i^{ma_i} \in L_m(K)$. So $G_m(K) \subset L_m(K)$, and it is obviously stable by multiplication and contains $1 = 1^m$.

   We define $S_m(K) = L_m(K)/G_m(K)$.

   (b) *Let $x \in L_m(K)$. Prove that there exists a unique fractional ideal $\mathfrak{a}_x$ such that $(x) = \mathfrak{a}_x^m$.*

   Let $x \in L_m(K)$, and let $(x) = \prod_i \mathfrak{p}_i^{ma_i}$ be its prime ideal factorisation. Then $\mathfrak{a}_x = \prod_i \mathfrak{p}_i^{a_i}$ satisfies the required property, and it is unique by uniqueness of factorisation into prime ideals.

   (c) *Prove that the map $f\colon S_m(K) \to \mathrm{Cl}(K)[m]$, defined by $f(x) = [\mathfrak{a}_x]$, is well-defined, and is a group homomorphism.*

   To prove that f is well-defined, we need to prove that $\mathfrak{a}_x$ is principal whenever $x \in G_m(K)$ and that $[\mathfrak{a}_x] \in \mathrm{Cl}(K)[m]$ for all $x \in L_m(K)$.

   - Let $x = y^m \in G_m(K)$. Then $\mathfrak{a}_x^m = (x) = (y)^m$ so $\mathfrak{a}_x = (y)$ and $[\mathfrak{a}_x] = 1$.
   - Let $x \in L_m(K)$. Then $(x) = \mathfrak{a}_x^m$, so $[\mathfrak{a}_x]^m = 1$ and $[\mathfrak{a}_x] \in \mathrm{Cl}(K)[m]$.

   For all $x, y \in L_m(K)$ we have $(\mathfrak{a}_x\mathfrak{a}_y)^m = \mathfrak{a}_x^m\mathfrak{a}_y^m = (x)(y) = (xy)$ so $\mathfrak{a}_{xy} = \mathfrak{a}_x\mathfrak{a}_y$ by uniqueness. This gives $f(xy) = f(x)f(y)$. Since $a_1 = (1)$, we have $f(1) = 1$ and f is a group homomorphism.

   (d) *Prove that f is surjective.*

   Let $[\mathfrak{a}] \in \mathrm{Cl}(K)[m]$. Then $[\mathfrak{a}]^m = 1$ so $\mathfrak{a}^m$ is principal, say $\mathfrak{a}^m = (x)$. But then $x \in L_m(K)$ and $\mathfrak{a} = \mathfrak{a}_x$, so that $[\mathfrak{a}] = f(x)$. So f is surjective.

   (e) *What is the kernel of f?*

   Let $x \in L_m(K)$ be such that $f(x) = 1$. Then $[a_x] = 1$, so $\mathfrak{a}_x$ is principal, say $\mathfrak{a}_x = (y)$. We have $(x) = \mathfrak{a}_x^m = (y^m)$, so there exists a unit $u \in \mathbb{Z}_K^\times$ such that $x = y^m u$. This proves that the kernel of f is the image of $\mathbb{Z}_K^\times$ in $S_m(K)$, that is, $\mathbb{Z}_K^\times/(\mathbb{Z}_K^\times)^m$.

   From now on, K is an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-d})$ with $d > 0$ squarefree. We write $\bar{\cdot}$ for the complex conjugation in K.

3. *Let $x = a + b\sqrt{-d} \in K$ be an element such that $N_{\mathbb{Q}}^K(x) = 1$. Let $\phi : K \to K$ be defined by $\phi(y) = \bar{y} - xy$.*

(a) *Prove that ϕ is $\mathbb{Q}$-linear.*

Conjugation is additive and does not change rational numbers, so conjugation is $\mathbb{Q}$-linear. Since multiplication by x is also $\mathbb{Q}$-linear, ϕ is $\mathbb{Q}$-linear.

(b) *Compute the matrix of ϕ on the basis $(1, \sqrt{-d})$.*

We have $\phi(1) = 1 - x = (1-a) + (-b)\sqrt{-d}$ and $\phi(\sqrt{-d}) = -\sqrt{-d} - (a + b\sqrt{-d})\sqrt{-d} = -\sqrt{-d} - a\sqrt{-d} + bd = bd + (-1-a)\sqrt{-d}$, so the matrix of ϕ is

$$\begin{pmatrix} 1-a & -b \\ bd & -1-a \end{pmatrix}.$$

(c) *Compute the determinant of ϕ. Is ϕ injective?*

The determinant of ϕ is $-(1-a)(1+a)+b^2d = a^2+db^2-1 = 0$ since $N^K_{\mathbb{Q}}(x) = 1$. So ϕ is not invertible, and hence not injective.

(d) *Prove that there exists $y \in K^\times$ such that $x = \bar{y}/y$.*

Let $y \neq 0$ be an element of $\ker \phi$. Then $\bar{y} - xy = 0$, so $xy = \bar{y}$ and finally $x = \bar{y}/y$ since $y \neq 0$.

4. *Let $[\mathfrak{a}] \in \mathrm{Cl}(K)[2]$ and let $a = N(\mathfrak{a})$.*

(a) *Prove that there exists $x \in K^\times$ such that $\mathfrak{a}^2 = (x)$.*

We have $[\mathfrak{a}^2] = 1$ so $\mathfrak{a}^2$ is principal: there exists $x \in K^\times$ such that $\mathfrak{a}^2 = (x)$.

(b) *Prove that there exists $y \in K^\times$ such that $x = a\bar{y}/y$.*

We have $N^K_{\mathbb{Q}}(x/a) = N(\mathfrak{a})^2/a^2 = 1$, so by Question 4 (d), there exists $y \in K^\times$ such that $x/a = \bar{y}/y$, i.e. $x = a\bar{y}/y$.

(c) *Let $\mathfrak{b} = y\mathfrak{a}$. Prove that there exists $b \in \mathbb{Q}^\times$ such that $\mathfrak{b}^2 = (b)$.*

We have $\mathfrak{b}^2 = y^2\mathfrak{a}^2 = (y^2x) = (y^2a\bar{y}/y) = (N^K_{\mathbb{Q}}(y)a)$, so $b = N^K_{\mathbb{Q}}(y)a \in \mathbb{Q}^\times$ is a generator of $\mathfrak{b}^2$.

(d) *Prove that $\mathfrak{a}$ is in the same ideal class as a product of the ramified prime ideals of $\mathbb{Z}_K$.*

Since $\mathfrak{b} = y\mathfrak{a}$, $\mathfrak{a}$ and $\mathfrak{b}$ are in the same ideal class. Write $b = ef^2$, where $e \in \mathbb{Z}$ is a squarefree integer and $f \in \mathbb{Q}^\times$ (which is possible by reducing the exponents modulo 2 in the prime factorisation of b), and let $\mathfrak{c} = f^{-1}\mathfrak{b}$, which is in the same ideal class as $\mathfrak{a}$. Then $\mathfrak{c}^2 = (f^{-2}b) = (e)$. By uniqueness of factorisation into prime ideals, every prime divisor of e is ramified, and $\mathfrak{c}$ is a product of the ramified prime ideals of $\mathbb{Z}_K$.

Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ be the ramified prime ideals of K.

5. *Prove that if the product $\mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_t^{e_t}$ with $0 \leq e_i \leq 1$ is principal then $\mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_t^{e_t} = (\sqrt{-d})$ or all the e_i are zero. Hint: consider the norm of such an ideal, and look at elements of $\mathbb{Z}_K$ of that norm.*

Let $n = N(\mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_t^{e_t})$, and we assume that then e_i are not all zero, so that $n > 1$ and n is squarefree. Assume $z = x + y\sqrt{-d} \in \mathbb{Z}_K$ is a generator of $\mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_t^{e_t}$. Since n is squarefree we have $y \neq 0$. We distinguish two cases:

- If $\Delta_K = -d$: we have $n \mid d$, and $x^2 + dy^2 = n$, so $y^2 \leq n/d \leq 1$: we get $y = \pm 1/2$ or $y = \pm 1$. In the first case we get $4x^2 + d = 4n$ which is impossible by reduction modulo 4. In the second case we must have $n = d$, so that $x = 0$ and $z = \pm\sqrt{-d}$.
- If $\Delta_K = -4d$: we have $n \mid 2d$, and $x^2 + dy^2 = n$, so that $n \geq d$: we get $n = d$ or $n = 2d$. In the first case we must have $x = 0$, $y = \pm 1$ and $z = \pm\sqrt{-d}$. In the second case we get $y^2 \leq 2$ so that $y = \pm 1$, giving $x^2 + d = 2d$ or equivalently $x^2 = d$, which is impossible.

6. *Prove that* $\mathrm{Cl}(K)[2] \cong (\mathbb{Z}/2\mathbb{Z})^{t-1}$.

   By Question 4 (d) the group $\mathrm{Cl}(K)[2]$ is generated by the classes $[\mathfrak{p}_1], \ldots, [\mathfrak{p}_t]$, and we have $[\mathfrak{p}_i]^2 = 1$ for all i. So $\mathrm{Cl}(K)[2]$ is the quotient of $(\mathbb{Z}/2\mathbb{Z})^t$ by the relations of the form $[\mathfrak{p}_1^{e_1}] \ldots [\mathfrak{p}_t^{e_t}] = 1$ where for all i we have $0 \leq e_i \leq 1$. By Question 5 there is only one such nontrivial relation, so $\mathrm{Cl}(K)[2] \cong (\mathbb{Z}/2\mathbb{Z})^{t-1}$.