Algebraic number theory — Exercise sheet 2

https://www.maths.tcd.ie/~mascotn/teaching/2026/MAU34109/index.html

Version: October 20, 2026

Submit your answers in class or to neumayec@tcd.ie by Thursday October 22, 1pm.

Exercise 2.1: A cubic field with an elusive maximal order (100pts)

Let $A(x) = x^3 + 2x^2 + 5x - 1 \in \mathbb{Q}[x]$.
We admit without proof that $\operatorname{disc} A = -575 = -5^2 \cdot 23$.
We also observe that $A(0) = -1$ whereas $A(1) = 7$.

1. (12 pts) Prove that $A(x)$ has no repeated root in $\mathbb{C}$, and determine how many roots it has in $\mathbb{R}$.

2. (12 pts) Use the notion of algebraic integer to prove that if $A(x)$ were reducible over $\mathbb{Q}$, then it would have a root in $\mathbb{Z}$. *You are NOT allowed to invoke the rational root theorem for this question.*

3. (4 pts) Hence deduce that $A(x)$ is irreducible over $\mathbb{Q}$.

In what follows, we let $K = \mathbb{Q}(\alpha)$, where α is a root of $A(x)$.

4. (8 pts) Prove that $\mathbb{Z}[\alpha]$ is an order in K, and specify a $\mathbb{Z}$-basis of it.

5. (16 pts) Find an upper bound on the index of $\mathbb{Z}[\alpha]$ in $\mathbb{Z}_K$.

Let $\beta = 1 + \dfrac{\alpha^2 - 6\alpha - 2}{5} \in K$.
We admit without proof that the characteristic polynomial of β is $x^3 + 11x + 7$.

6. (10 pts) Prove that $\mathbb{Z}_K \neq \mathbb{Z}[\alpha]$.

7. (10 pts) Determine $\operatorname{disc} K$.

8. (16 pts) Prove that $1, \alpha, \beta$ is a $\mathbb{Z}$-basis of $\mathbb{Z}_K$.

9. (12 pts) Is it true that $\mathbb{Z}_K = \mathbb{Z}[\beta]$? If not, what is the index of $\mathbb{Z}[\beta]$ in $\mathbb{Z}_K$?

Solution 2.1:

1. Since $\operatorname{disc} A \neq 0$, A does not have repeated roots.

   Furthermore, we have $r_1 + 2r_2 = \deg A = 3$ where r_1 (resp. r_2) is the number of real (resp. pairs of complex-conjugate) roots of A, so either $(r_1, r_2) = (3, 0)$ or $(r_1, r_2) = (1, 1)$. But we know that $(-1)^{r_2}$ is the sign of $\operatorname{disc} A$, so r_2 is odd, so the only possibility is $(r_1, r_2) = (1, 1)$.

2. Since $\deg A = 3$, if A were reducible over $\mathbb{Q}$, it would have a linear factor over $\mathbb{Q}$ and hence a root in $\mathbb{Q}$. Furthermore, A is monic and has integer coefficients, so this root would in fact lie in $\mathbb{Z}_{\mathbb{Q}} = \mathbb{Z}$.

3. On the one hand, we know from the first question that A has exactly one real root; on the other hand, the fact that $A(0) < 0 < A(1)$ shows that this root is strictly between 0 and 1 by the intermediate value theorem. It follows that this root is not an integer, and we conclude by the previous question.

4. This follows from the fact that α is a primitive element for K which lies in $\mathbb{Z}_K$, as a root of A which is monic and has coefficients in $\mathbb{Z}$. In particular, since $\deg A = 3$, we have that $1, \alpha, \alpha^2$ is a $\mathbb{Z}$-basis of $\mathbb{Z}[\alpha]$; in other words,

$$\mathbb{Z}[\alpha] = \{\underbrace{a + b\alpha + c\alpha^2}_{\text{uniq.}} \mid a, b, c \in \mathbb{Z}\}.$$

5. On the one hand, A is the minimal polynomial of α since it is monic and irreducible, so $\operatorname{disc} \mathbb{Z}[\alpha] = \operatorname{disc} A = -5^2 \cdot 23$. On the other hand, we have the formula $\operatorname{disc} \mathbb{Z}[\alpha] = [Z_K : \mathbb{Z}[\alpha]]^2 \operatorname{disc} K$. As 23 is prime, we conclude that $[Z_K : \mathbb{Z}[\alpha]]$ can only be 1 or 5.

6. The characteristic polynomial of β lies in $\mathbb{Z}[x]$, so $\beta \in \mathbb{Z}_K$. However, $\beta \notin \mathbb{Z}[\alpha]$ as its coordinates $-\frac{2}{5}, -\frac{6}{5}, \frac{1}{5}$ on our $\mathbb{Z}$-basis of $\mathbb{Z}[\alpha]$ are not all integers.

7. It follows that $[\mathbb{Z}_K : \mathbb{Z}[\alpha]] \neq 1$ (and even that $5 \mid [Z_K : \mathbb{Z}[\alpha]]$ since $\beta \in \mathbb{Z}_K$ has denominator 5 with respect ot $\mathbb{Z}[\alpha]$. In view of question 5., we deduce that $[\mathbb{Z}_K : \mathbb{Z}[\alpha]] = 5$, whence

$$\operatorname{disc} K = \frac{\operatorname{disc} \mathbb{Z}[\alpha]}{[\mathbb{Z}_K : \mathbb{Z}[\alpha]]^2} = -23.$$

8. Let

$$P = \begin{pmatrix} 1 & 0 & -2/5 \\ 0 & 1 & -6/5 \\ 0 & 0 & 1/5 \end{pmatrix}$$

be the matrix expressing $1, \alpha, \beta$ on the $\mathbb{Q}$-basis $1, \alpha, \alpha^2$ of K. Plainly $\det P = -1/2 \neq 0$ (triangular matrix), so $1, \alpha, \beta$ is another $\mathbb{Q}$-basis of K and thus spends a lattice I inside K. Furthermore, $1, \alpha, \beta$ are all in $\mathbb{Z}_K$, so I is a sublattice of $\mathbb{Z}_K$. Moreover, clearly $1, \alpha \in I$, and also $\alpha^2 \in I$ since $\alpha^2 = 5\beta + 6\alpha + 2$, so $\mathbb{Z}[\alpha]$ is a sublattice of I:

$$\mathbb{Z}[\alpha] \subseteq I \subseteq \mathbb{Z}_K.$$

But $[\mathbb{Z}_K : \mathbb{Z}[\alpha]] = 5$ whereas $I \supsetneq \mathbb{Z}[\alpha]$ as $\beta \notin \mathbb{Z}[\alpha]$, so necessarily $I = \mathbb{Z}_K$. An alternative way to conclude consists in noticing that since $\det P = 1/5$, we have $[I : \mathbb{Z}[\alpha]] = 5$, whence $\operatorname{disc} I = \frac{\operatorname{disc} \mathbb{Z}[\alpha]}{[I:\mathbb{Z}[\alpha]]^2} = -23 = \operatorname{disc} K$, so that $[\mathbb{Z}_K : I]^2 = \operatorname{disc} I / \operatorname{disc} \mathbb{Z}_K = 1$ meaning that $[\mathbb{Z}_K : I] = 1$ and thus $\mathbb{Z}_K = I$.

9. First of all, $\beta \in \mathbb{Z}_K$ so the minimal polynomial of β has integer coefficients. We know that its characteristic polynomial is a power of it, but since its constant term 7 is not a cube, we can conclude that the minimal and characteristic polynomial of β agree so β is another primitive element for K (alternative argument: $\mathbb{Q} \subseteq \mathbb{Q}(\beta) \subseteq K$ and $[K : \mathbb{Q}] = 3$ is prime so $\mathbb{Q}(\beta)$ is either $\mathbb{Q}$ or K by the tower law. But $\beta \notin \mathbb{Q}$ as clearly seen on its coordinates on the $\mathbb{Q}$-basis $1, \alpha, \alpha^2$ of K, so $\mathbb{Q}(\beta) \supsetneq \mathbb{Q}$). Therefore $\mathbb{Z}[\beta]$ is indeed an order in K. In order to check if it agrees with $\mathbb{Z}_K$, we compare discriminants:

$$\operatorname{disc} \mathbb{Z}[\beta] = \operatorname{disc}(x^3 + 11x + 7) = -4(11)^3 - 27(7)^2 = -6647 = 17^2 \operatorname{disc} \mathbb{Z}_K,$$

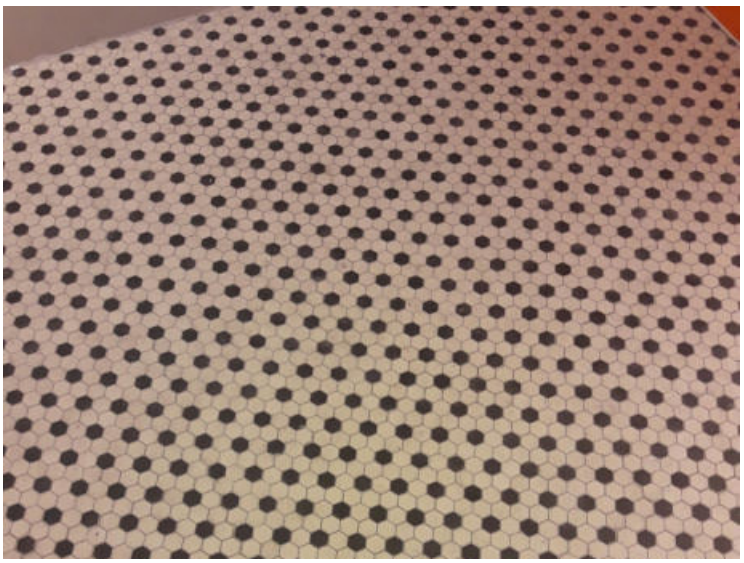
so $\mathbb{Z}[\beta] \neq \mathbb{Z}_K$ and in fact $\mathbb{Z}[\beta]$ has index 17 in $\mathbb{Z}_K$.

Remark: It can be proved that this particular number field K has the property that there does not exist any $\gamma \in K$ such that $\mathbb{Z}_K = \mathbb{Z}[\gamma]$ (we will see why in the next assignment), which explains why we were unable to find one.

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.

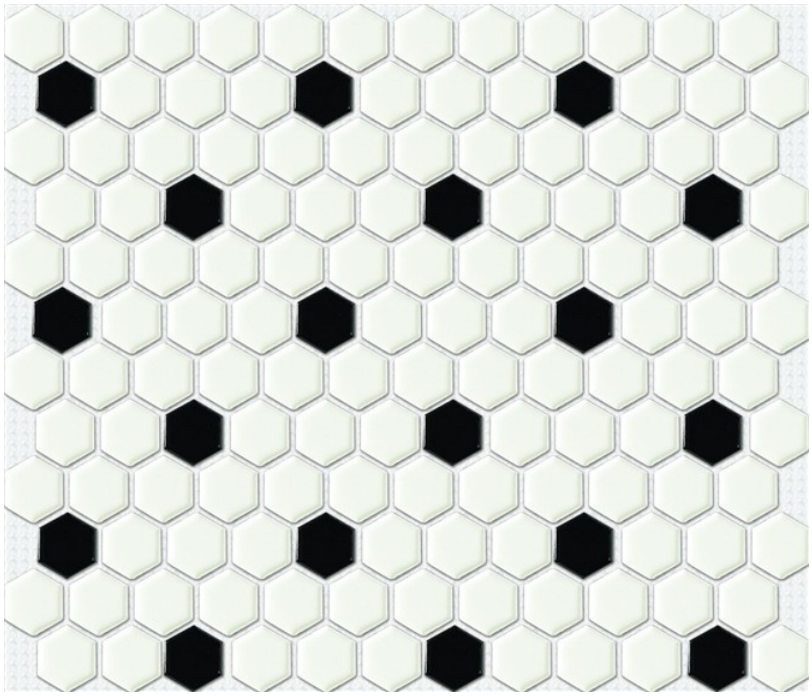
Exercise 2.2: Floor tilings

1. In the picture below[1], (the centre of) the hexagonal floor tiles (both the black ones and the white ones) form a lattice, and (the centre of) the black tiles form a sublattice. Compute the index of this sublattice by writing down a change-of-basis (= transition) matrix. What is the proportion of black tiles?



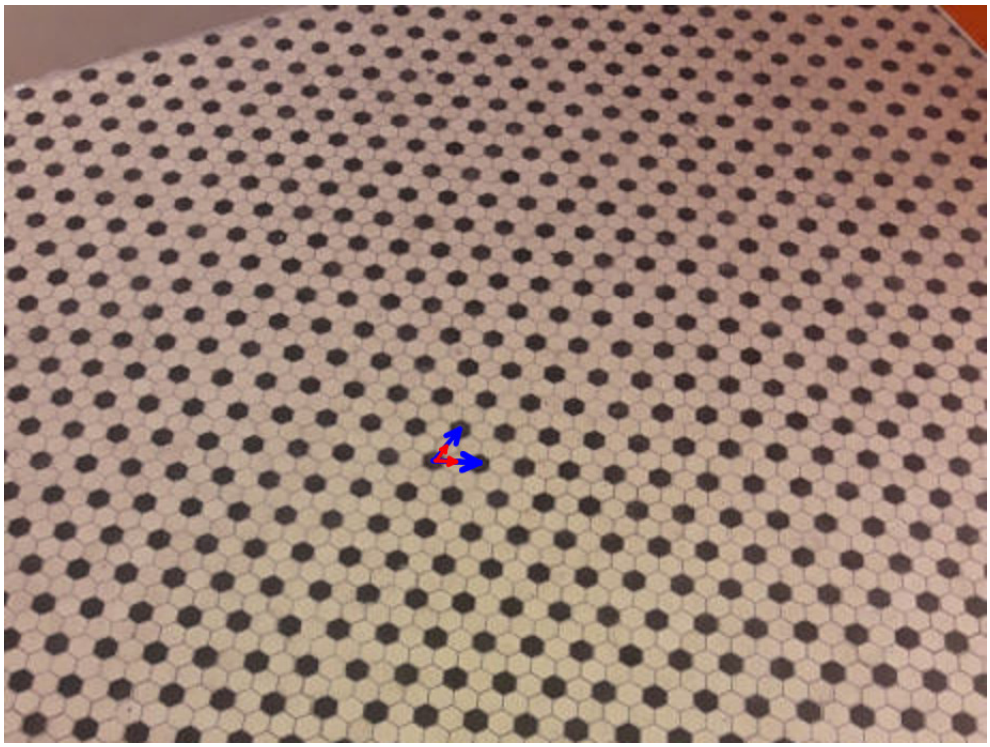
[1] In case you were wondering, no, that's not my home; I just googled "floor tiling".

2. Same questions for this other tiling pattern.



Solution 2.2:

1. Let us choose a $\mathbb{Z}$-basis (in red) for the whole lattice, and another (in blue) for the black sublattice, as shown on the picture.

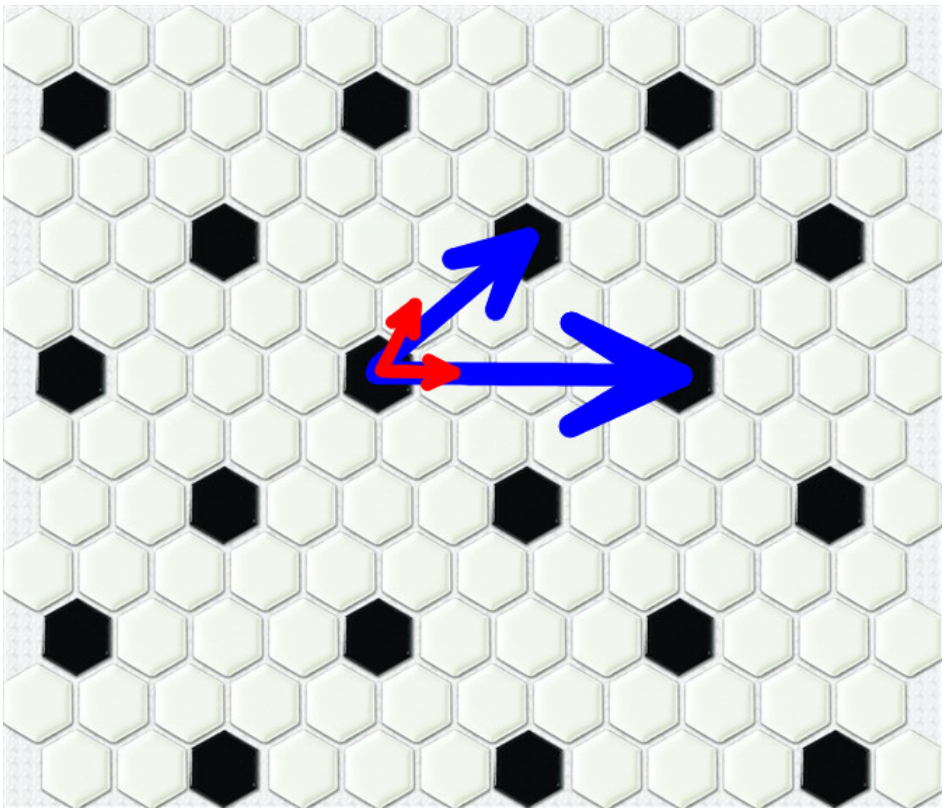


The change-of-basis matrix expressing the blue vectors in terms of the red ones is

$$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix},$$

whose determinant is 4, so the index is 4. In other words, 1 out of 4 tiles is black.

2. Let us choose again $\mathbb{Z}$-basis (in red) for the whole lattice, and another (in blue) for the black sublattice.



This time, the change-of-basis matrix looks like

$$\begin{pmatrix} 4 & 1 \\ 0 & 2 \end{pmatrix}$$

(depending on how you order the bases). The determinant is 8, so the index is 8. In other words, 1 out of 8 tiles is black.

Exercise 2.3: To be or not to be integral

Is $\dfrac{3+2\sqrt{6}}{\sqrt{6}-2}$ an algebraic integer ?

Solution 2.3:

Let us first express this number as a polynomial in $\sqrt{6}$. In principle, we should use the $U(x)A(x) + B(x)V(x) = 1$ method as in sheet 1 for that, but here we are in degree only 2, so we can just apply the good old "conjugate expression" trick:

$$\frac{3+2\sqrt{6}}{\sqrt{6}-2} = \frac{(3+2\sqrt{6})(\sqrt{6}+2)}{(\sqrt{6}-2)(\sqrt{6}+2)} = \frac{3\sqrt{6}+6+2(\sqrt{6})^2+4\sqrt{6}}{(\sqrt{6})^2-2^2} = 9+\frac{7}{2}\sqrt{6}.$$

Now, there are (at least) three ways to conclude:

- As $\sqrt{6}$ is algebraic of degree 2 over $\mathbb{Q}$, every element of $\mathbb{Q}(\sqrt{6})$ can be written *uniquely* as $a+b\sqrt{6}$ with $a, b \in \mathbb{Q}$; besides, 6 is squarefree and $6 \not\equiv 1 \bmod 4$ so the ring of integers is $\mathbb{Z}[\sqrt{6}]$, in other words, an element $a+b\sqrt{6}$ is an algebraic integer if and only if a and b are both integers. This is not the case for $9+\frac{7}{2}\sqrt{6}$, so it is NOT an algebraic integer.

- The characteristic polynomial of this number (with respect to the extension $\mathbb{Q}(\sqrt{6})/\mathbb{Q}$) is

$$\left(x-\left(9+\frac{7}{2}\sqrt{6}\right)\right)\left(x-\left(9-\frac{7}{2}\sqrt{6}\right)\right) = x^2-18x+\frac{15}{2}$$

  (because of complex embeddings; we could also have written down the matrix of course). This does not lie in $\mathbb{Z}[x]$, so this number is NOT an algebraic integer.

- If this number were an algebraic integer, then since algebraic integers form a ring containing $\mathbb{Z}$ and $\sqrt{6}$, we would have that $(9+\frac{7}{2}\sqrt{6}) - 9 - 3\sqrt{6} = \frac{1}{2}\sqrt{6}$ is also an algebraic integer. However, this is not the case, since its minimal polynomial, which is $x^2 - 6/4$, does not lie in $\mathbb{Z}[x]$.

Exercise 2.4: Another cubic field

Let $A(x) = x^3 - 5x + 1 \in \mathbb{Q}[x]$.

1. Prove that $A(x)$ is irreducible over $\mathbb{Q}$.

2. Let $K = \mathbb{Q}(\alpha)$, where $A(\alpha) = 0$. Determine the degree of K, the ring of integers of K, the discriminant of K, and the signature of K. Needless to say, justify your answers.

Solution 2.4:

1. The degree of $A(x)$ is only 3, so if it factored over $\mathbb{Q}$, it would have either one factor of degree 1 and one of degree 2, or 3 factors of degree 1 (possibly not all distinct); anyway, it would have at least one factor of degree 1, and therefore a root in $\mathbb{Q}$. But the rational root theorem shows that the only possible rational roots of $A(x)$ are ± 1 (NB such a root would be a rational number and also an algebraic integer since $A(x) \in \mathbb{Z}[x]$ is monic, and therefore a rational integer), and those are not actual roots. Therefore $A(x)$ is irreducible over $\mathbb{Q}$.

2. Since $A(x)$ is irreducible over $\mathbb{Q}$ and monic, it is the minimal polynomial of α over $\mathbb{Q}$, so
$$[K : \mathbb{Q}] = \deg A(x) = 3.$$
Next, since actually $A(x) \in \mathbb{Z}[x]$ and is monic, α is an algebraic integer, so $\mathbb{Z}[\alpha]$ is an order in K, and we have
$$\big[\mathbb{Z}_K : \mathbb{Z}[\alpha]\big]^2 \operatorname{disc} K = \operatorname{disc} \mathbb{Z}[\alpha] = \operatorname{disc} A = -4(-5)^3 - 27(-1)^2 = 500 - 27 = 473,$$
which factors as $473 = 11 \times 43$ and is thus squarefree. Therefore $\big[\mathbb{Z}_K : \mathbb{Z}[\alpha]\big] = 1$, so the ring of integers of K is
$$\mathbb{Z}_K = \mathbb{Z}[\alpha]$$
and its discriminant is
$$\operatorname{disc} K \stackrel{\text{def}}{=} \operatorname{disc} \mathbb{Z}_K = \operatorname{disc} \mathbb{Z}[\alpha] = 11 \times 43.$$
Finally, let (r_1, r_2) be the signature of K. Then $r_1 + 2r_2 = [K : \mathbb{Q}] = 3$, so this signature is either $(3, 0)$ or $(1, 1)$. But we know that $(-1)^{r_2}$ is the sign of $\operatorname{disc} K$, so r_2 is even, so the only possibility is that the signature of K is $(3, 0)$. This means that K is *totally real*; in other words, all 3 complex roots of $A(x)$ are actually real.

Exercise 2.5: And finally, a quartic field

Reminder: $\operatorname{disc}(x^n + bx + c) = (-1)^{n(n-1)/2}\big((1-n)^{n-1}b^n + n^n c^{n-1}\big)$.

Let $f(x) = x^4 - 2x + 4$, which you may assume without proof is irreducible over $\mathbb{Q}$, and let $K = \mathbb{Q}(\alpha)$, where α satisfies $f(\alpha) = 0$.

1. Prove that $\mathbb{Z}[\alpha]$ is an order in K.

2. Compute and factor the discriminant of $\mathbb{Z}[\alpha]$.
Hint: $2^{10} - 3^3 = 997$ *is prime.*

3. At this point, what are the possibilities for $\operatorname{disc} K$, and the corresponding values of the index of $\mathbb{Z}[\alpha]$?

4. Let $\beta = \frac{\alpha^3}{2} \in K$, and consider the lattice $\mathcal{O} \subset K$ with $\mathbb{Z}$-basis

$$1, \alpha, \alpha^2, \beta.$$

Prove that $\mathcal{O}$ is stable under multiplication by β.

Hint: what is $\beta \cdot \alpha$?.

5. Deduce that β is an algebraic integer.

6. Which of the possibilities listed in question 2. remain?

7. Prove that $\mathcal{O}$ is actually an order in K.

Hint: Prove that $\mathcal{O}$ is also stable under multiplication by α.

8. It turns out that $\mathbb{Z}_K = \mathcal{O}$. Give the discriminant of K in factored form.

Solution 2.5:

Let $f(x) = x^4 - 2x + 4$, which you may assume without proof is irreducible over $\mathbb{Q}$, and let $K = \mathbb{Q}(\alpha)$, where α satisfies $f(\alpha) = 0$.

1. We know that $\operatorname{disc} \mathbb{Z}[\alpha] = \operatorname{disc} f$, and according to the formula

$$\operatorname{disc}(x^n + bx + c) = (-1)^{n(n-1)/2}\big((1-n)^{n-1}b^n + n^n c^{n-1}\big),$$

we have

$$\operatorname{disc} \mathbb{Z}[\alpha] = +(-3^3 \cdot 2^4 + 4^4 \cdot 4^3) = 2^{14} - 3^3 \cdot 2^4 = 2^4 \cdot (2^{10} - 3^3) = 2^4 \cdot 997.$$

2. We know that

$$\operatorname{disc} \mathbb{Z}[\alpha] = m^2 \operatorname{disc} K,$$

where m is the index of $\mathbb{Z}[\alpha]$. Since 997 is prime, this leaves 3 possibilities:

- Either $m = 1$ (which means that $\mathbb{Z}_K = \mathbb{Z}[\alpha]$), and so $\operatorname{disc} K = 2^4 \cdot 997$,
- or $m = 2$ (so $\mathbb{Z}[\alpha]$ is not 2-maximal, but is p-maximal for all primes $p \neq 2$), and $\operatorname{disc} K = 2^2 \cdot 997$,
- or $m = 2^2$ (so again $\mathbb{Z}[\alpha]$ is not 2-maximal, but is p-maximal for all primes $p \neq 2$), and $\operatorname{disc} K = 997$.

In the last two cases, the fact that $\mathbb{Z}[\alpha]$ is not 2-maximal would imply that the elements of $\mathbb{Z}_K$ would in general have denominators which are powers of 2 when we write then as polynomial of degree $< 4 = \deg f$ in α. In the first case, the elements of $\mathbb{Z}_K$ would have no denominators at all.

3. We have $\mathcal{O} = \{a + b\alpha + c\alpha^2 + d\beta,\ a, b, c, d \in \mathbb{Z}\}$.

   The relation $f(\alpha) = 0$ yields $\alpha^4 = 2\alpha - 4$, whence $\beta \cdot \alpha = \alpha - 2 \in \mathcal{O}$. Similarly, we find that $\beta \cdot \alpha^2 \in \mathcal{O}$, $\beta \cdot \beta \in \mathcal{O}$, and of course $\beta \cdot 1 \in \mathcal{O}$. Therefore,

   $$\beta \cdot (a + b\alpha + c\alpha^2 + d\beta) = a\beta \cdot 1 + b\beta \cdot \alpha + c\beta \cdot \alpha^2 + d\beta \cdot \beta \in \mathcal{O}$$

   as soon as $a, b, c, d \in \mathbb{Z}$, so $\beta \cdot \mathcal{O} \subset \mathcal{O}$.

4. Multiplication by β stabilises a lattice, so β is an algebraic integer (Recall the proof: we can write down the matrix of multiplication by β w.r.t. a $\mathbb{Z}$-basis of $\mathcal{O}$, and this matrix will have coefficients in $\mathbb{Z}$ since $\beta \cdot \mathcal{O} \subset \mathcal{O}$, so the characteristic polynomial of β lies in $\mathbb{Z}[x]$).

5. We have just seen that $\beta \in \mathbb{Z}_K$, but $\beta \notin \mathbb{Z}[\alpha]$ (because $\mathbb{Z}[\alpha] = \{a + b\alpha + c\alpha^2 + d\alpha^3,\ a, b, c, d \in \mathbb{Z}\}$ since α is an algebraic integer), so $\mathbb{Z}_K \neq \mathbb{Z}[\alpha]$. So only the second and third possibilities remain.

   Alternative, quicker proof : $\beta = \alpha^3/2 \in \mathbb{Z}_K$ has a denominator divisible by the prime 2, so $\mathbb{Z}[\alpha]$ is not 2-maximal.

6. We find that $\alpha \cdot 1$, $\alpha \cdot \alpha$, $\alpha \cdot \alpha^2$ and $\alpha \cdot \beta$ all lie in $\mathcal{O}$, which as in question 3. proves that $\mathcal{O}$ is stable under multiplication by α. It is therefore also stable under multiplication by α^2, and also by β by question 3., and of course also by 1. Therefore, $\mathcal{O}$ is stable under multiplication by any $\mathbb{Z}$-linear combination of $1, \alpha, \alpha^2$ and β, i.e. $\mathcal{O} \cdot \mathcal{O} \subset \mathcal{O}$. As $1 \in \mathcal{O}$, this proves that $\mathcal{O}$ is a subring of K. By construction, $\mathcal{O}$ is also a lattice in K, so it is an order in K.

7. Thanks to the relation

   $$\operatorname{disc} \mathbb{Z}[\alpha] = m^2 \operatorname{disc} K,$$

   finding $\operatorname{disc} K$ amounts to computing the index m of $\mathbb{Z}[\alpha]$ in $\mathbb{Z}_K = \mathcal{O}$. We do so by writing a change-of-basis matrix between a $\mathbb{Z}$-basis of $\mathcal{O}$ and a $\mathbb{Z}$-basis of $\mathbb{Z}[\alpha]$.

   A $\mathbb{Z}$-basis of $\mathcal{O}$ is $1, \alpha, \alpha^2, \beta = \alpha^3/2$, and a $\mathbb{Z}$-basis of $\mathbb{Z}[\alpha]$ is $1, \alpha, \alpha^2, \alpha^3$ since α is an algebraic integer of degree $4 = \deg f$. (Technically we could use any $\mathbb{Z}$-bases, but why make things complicated?). The matrix expressing the latter in terms of the former is

   $$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix},$$

   whose determinant is clearly 2, so the index is

   $$m \overset{\text{def}}{=} [\mathcal{O} : \mathbb{Z}[\alpha]] = 2.$$

   Therefore, we are in the second of the three cases listed in question 2., so

   $$\operatorname{disc} K = 2^2 \cdot 997.$$

In conclusion, the factor 2^4 of $\operatorname{disc}\mathbb{Z}[\alpha]$ actually came *both* from $\operatorname{disc} K$ and from the index !

Note that we could also have expressed $1, \alpha, \alpha^2, \beta = \alpha^3/2$ in terms of $1, \alpha, \alpha^2, \alpha^3$; this would lead us to the inverse change-of-basis matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \frac{1}{2} \end{pmatrix}$$

whose determinant is (up to sign) the inverse of the index. Doing things this way is sometimes easier. Also, don't worry if you can't remember if you should express this basis in terms of that basis, or the other way round: you'll either get a matrix with integer coefficients, whose determinant is (up to sign) the index, or a matrix with rational coefficients, whose determinant is (up to sign) the inverse of the index, and since the index is an integer, the result that you get will tell you which case you are in!