

Algebraic number theory — Exercise sheet 1

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

Version: September 23, 2022

Email your answers to mascotn@tcd.ie by Friday October 7 noon.

Exercise 1.1: Review of methods (26 pts)

Let $K = \mathbb{Q}(\sqrt{3})$, and let $\alpha = a + b\sqrt{3}$ ($a, b \in \mathbb{Q}$) be an element of K . Express the trace, norm, and characteristic polynomial of α (with respect to the extension K/\mathbb{Q}) in terms of a and b

- (13 pts) by writing down the matrix of the multiplication-by- α map with respect to the \mathbb{Q} -basis of K of your choice,
- (13 pts) by considering complex embeddings (*Hint: $K = \mathbb{Q}(\alpha)$ where $\alpha^2 = 3$*).

Remark: This exercise is meant as a warm-up for the next exercises, so as to remind you that some computations can be done in different ways. In the next exercises, remember that depending on the situation, some methods require less efforts than others!

Solution 1.1:

- Since $x^2 - 3 \in \mathbb{Q}[x]$ is irreducible by Eisenstein at $p = 3$, we find that $\sqrt{3}$ is algebraic over \mathbb{Q} of degree 2, so that $(\sqrt{3})^0 = 1$ and $(\sqrt{3})^1 = \sqrt{3}$ form a \mathbb{Q} -basis of K .

With respect to this basis, the matrix of the multiplication-by- α map is

$$M = \begin{pmatrix} a & 3b \\ b & a \end{pmatrix}$$

since $\alpha \cdot 1 = a + b\sqrt{3}$ and $\alpha \cdot \sqrt{3} = 3b + a\sqrt{3}$, so that

$$\mathrm{Tr}_{\mathbb{Q}}^K(\alpha) = \mathrm{Tr} M = 2a,$$

$$N_{\mathbb{Q}}^K(\alpha) = \det M = a^2 - 3b^2,$$

$$\text{and } \chi_{\mathbb{Q}}^K(\alpha) = \chi_M = x^2 - 2ax + (a^2 - 3b^2).$$

- Since α is algebraic of degree 2, we have $[K : \mathbb{Q}] = 2$, so there are 2 embeddings of K into \mathbb{C} , which correspond to the complex roots of the minimal polynomial $x^2 - 3$ of α in that they send α to the root they correspond to. Here, these complex roots are $\pm\sqrt{3}$, so one of the embeddings sends α to $\sqrt{3}$, and the other one sends α to $-\sqrt{3}$. As they are embeddings, they are also \mathbb{Q} -linear, so the first one sends α to $u = a + b\sqrt{3}$, and the other one sends α to $v = a - b\sqrt{3}$

(so actually both these embeddings are actually embeddings in $\mathbb{R} \subset \mathbb{C}$). As a result,

$$\mathrm{Tr}_{\mathbb{Q}}^K(\alpha) = u + v = 2a,$$

$$N_{\mathbb{Q}}^K(\alpha) = uv = a^2 - 3b^2,$$

$$\text{and } \chi_{\mathbb{Q}}^K(\alpha) = (x - u)(x - v) = x^2 - 2ax + (a^2 - 3b^2).$$

Exercise 1.2: A biquadratic extension (74 pts)

1. (10 pts) Let $K = \mathbb{Q}(\sqrt{2})$. Prove that $\sqrt{5} \notin K$.
2. (10 pts) Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{5})$. Determine $[L : \mathbb{Q}]$, and find a \mathbb{Q} -basis of L .
3. (10 pts) What is the signature of L ?
4. (10 pts) Let $\alpha = \sqrt{2} + \sqrt{5} \in L$. Write down the matrix of

$$\begin{array}{ccc} \mu_{\alpha} : L & \longrightarrow & L \\ x & \longmapsto & \alpha x \end{array}$$

with respect to the \mathbb{Q} -basis of L that you found in question 2.

5. (4 pts) Deduce the value of $\mathrm{Tr}_{\mathbb{Q}}^L(\alpha)$.
6. (10 pts) Determine the norm $N_{\mathbb{Q}}^L(\alpha)$ of α .
Note: It is possible to do this without computing a big determinant.
7. (10 pts) The characteristic polynomial $\chi_{\mathbb{Q}}^L(\alpha)$ of α turns out to be $x^4 - 14x^2 + 9$ (we admit this without proof). Is it squarefree? What does this tell us about α ?
8. (10 pts) Compute the characteristic polynomial $\chi_K^L(\alpha)$ of α with respect to the extension L/K .

Solution 1.2:

1. The minimal polynomial of $\sqrt{2}$ over \mathbb{Q} is $x^2 - 2$, because it is irreducible over \mathbb{Q} by Eisenstein. Therefore $((\sqrt{2})^0 = 1, (\sqrt{2})^1 = \sqrt{2})$ is a \mathbb{Q} -basis of K . So if $\sqrt{5} \in K$, we would have (unique) $a, b \in \mathbb{Q}$ such that $\sqrt{5} = a + b\sqrt{2}$. Squaring yields $5 = (a^2 + 2b^2) + 2ab\sqrt{2} \in K$. As $(1, \sqrt{2})$ is a \mathbb{Q} -basis, we may conclude that $a^2 + 2b^2 = 5$ and that $2ab = 0$, whence $a = 0$ or $b = 0$. Neither alternative yields rational solutions to $a^2 + 2b^2 = 5$, whence a contradiction.
2. Because $\sqrt{5} \notin K$, the polynomial $x^2 - 5 \in K[x]$ must be irreducible over K (else it would split into factors of degree 1 whence $\pm\sqrt{5} \in K$, absurd), so it is the minimal polynomial of $\sqrt{5}$ over K . Therefore $[L : K] = 2$, and $(1, \sqrt{5})$ is a K -basis of L . The tower law then shows that

$$[L : \mathbb{Q}] = [L : K][K : \mathbb{Q}] = 2 \times 2 = 4,$$

and that

$$(1 \cdot 1, 1 \cdot \sqrt{2}, \sqrt{5} \cdot 1, \sqrt{5} \cdot \sqrt{2}) = (1, \sqrt{2}, \sqrt{5}, \sqrt{10})$$

is a \mathbb{Q} -basis of L .

3. We have $L = \mathbb{Q}(\beta, \gamma)$ where $\beta^2 = 2$ and $\gamma^2 = 5$. Therefore, if σ is one of the $[L : \mathbb{Q}] = 4$ embeddings of L into \mathbb{C} , then $\sigma(\beta)^2 = \sigma(\beta^2) = \sigma(2) = 2$ so $\sigma(\beta) = \pm\sqrt{2} \in \mathbb{R}$, and similarly $\sigma(\gamma) = \pm\sqrt{5} \in \mathbb{R}$. Besides σ must act as the identity on \mathbb{Q} , so either way $\sigma(L) \subset \mathbb{R}$. Therefore L is totally real and has signature $(4, 0)$.

4. We look at the effect of multiplying by α on the elements of our basis. We find

- $\alpha \cdot 1 = \sqrt{2} + \sqrt{5}$,
- $\alpha \cdot \sqrt{2} = 2 + \sqrt{10}$,
- $\alpha \cdot \sqrt{5} = 5 + \sqrt{10}$,
- $\alpha \cdot \sqrt{10} = 5\sqrt{2} + 2\sqrt{5}$,

so the matrix is

$$\begin{pmatrix} 0 & 2 & 5 & 0 \\ 1 & 0 & 0 & 5 \\ 1 & 0 & 0 & 2 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

5. $\text{Tr}_{\mathbb{Q}}^L(\alpha)$ is the trace of this matrix, which is clearly 0.

6. We use the transitivity of the norm to write $N_{\mathbb{Q}}^L(\alpha) = N_{\mathbb{Q}}^K N_K^L(\alpha)$. Now $L = K(\sqrt{5}) = K(\beta)$ where $\beta^2 = 5$, so the $[L : K] = 2$ embeddings of L into \mathbb{C} which restrict to the identity on K are characterised by $\beta \mapsto \pm\sqrt{5}$. In particular, they take $\alpha = \sqrt{2} + \beta$ to $\sqrt{2} \pm \sqrt{5}$, whence

$$N_K^L(\alpha) = (\sqrt{2} + \sqrt{5})(\sqrt{2} - \sqrt{5}) = 2 - 5 = -3.$$

As a result,

$$N_{\mathbb{Q}}^L(\alpha) = N_{\mathbb{Q}}^K(3) = 3^2 = 9$$

(because multiplication μ_3 by 3 on K has a scalar matrix, or if you prefer, because the $[K : \mathbb{Q}] = 2$ embeddings of K into \mathbb{C} must take 3 to 3 because $3 \in \mathbb{Q}$).

7. We could determine if this polynomial is squarefree by computing its GCD with its derivative by successive Euclidian divisions, but this would be rather tedious. Instead, we can just notice from the logic of the previous question that the complex roots of this characteristic polynomial, which are the images of α under the $[L : \mathbb{Q}] = 4$ embeddings of L into \mathbb{C} , are the $\pm\sqrt{2} \pm \sqrt{5}$, which are distinct; therefore $\chi_{\mathbb{Q}}^L(\alpha)$ is squarefree.

Now as $\chi_{\mathbb{Q}}^L(\alpha)$ is always a power of the minimal polynomial m_α of α , it follows that actually $\chi_{\mathbb{Q}}^L(\alpha) = m_\alpha$. In particular,

$$[L : \mathbb{Q}(\alpha)] = \frac{[L : \mathbb{Q}]}{[\mathbb{Q}(\alpha) : \mathbb{Q}]} = \frac{\deg \chi_{\mathbb{Q}}^L(\alpha)}{\deg m_\alpha} = 1,$$

so $L = \mathbb{Q}(\alpha)$; in other words, α is a *primitive element* for L/\mathbb{Q} .

8. Again, two methods : matrix and complex embeddings. Here, both are reasonable, so we explain both.

Matrix: With respect to the K -basis $1, \sqrt{5}$ of L , the matrix of the multiplication by α is

$$\begin{pmatrix} \sqrt{2} & 5 \\ 1 & \sqrt{2} \end{pmatrix},$$

whose characteristic polynomial is

$$\chi_K^L(\alpha) = x^2 - 2\sqrt{2}x - 3.$$

Embeddings: As discussed in our answer to question 6, the $[L : K] = 2$ embeddings of L into \mathbb{C} which restrict to the $\sigma = \text{Id}$ on K take $\alpha = \sqrt{2} + \beta$ to $\sqrt{2} \pm \sqrt{5}$, so

$$\chi_K^L(\alpha)^\sigma = (x - (\sqrt{2} + \sqrt{5}))(x - (\sqrt{2} - \sqrt{5})) = x^2 - 2\sqrt{2}x - 3.$$

To recover $\chi_K^L(\alpha)$ from $\chi_K^L(\alpha)^\sigma$, we apply σ^{-1} to the coefficients and we find

$$\chi_K^L(\alpha) = x^2 - 2\sqrt{2}x - 3 \in K[x].$$

Just for completeness, here is what would happen if, for some obscure reason, we had picked σ such that $\sigma(\sqrt{2}) = -\sqrt{2}$: The embeddings of L that extend σ send α to $-\sqrt{2} \pm \sqrt{5}$, so

$$\chi_K^L(\alpha)^\sigma = (x - (-\sqrt{2} + \sqrt{5}))(x - (-\sqrt{2} - \sqrt{5})) = x^2 + 2\sqrt{2}x - 3.$$

Applying σ^{-1} affects the coefficient of x nontrivially, and we find again that

$$\chi_K^L(\alpha) = x^2 - 2\sqrt{2}x - 3 \in K[x].$$

These were the only mandatory exercises, 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, 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 1.3: Computations in $\mathbb{Q}(\sqrt[3]{2})$

1. Prove that $x^3 - 2$ is irreducible over \mathbb{Q} .
2. Let $K = \mathbb{Q}(\sqrt[3]{2})$, and let $\alpha = \frac{\sqrt[3]{2}+1}{\sqrt[3]{2}-1} \in K$. Find $a, b, c \in \mathbb{Q}$ such that $\alpha = a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2$.
3. Are these rational numbers a, b, c unique ?
4. What is the degree of K over \mathbb{Q} ?
5. Prove that $\sqrt{2} \notin K$.
Hint: Think in terms of degrees.
6. Prove that $K = \mathbb{Q}(\alpha)$.
7. Compute the trace, norm, and characteristic polynomial of α .
8. What is the minimal polynomial of α over \mathbb{Q} ?

Solution 1.3:

1. This is because it is Eisenstein at $p = 2$. Alternatively, because it has degree 3, if it factored, it would have a factor of degree 1 and therefore a root, which it does not because the only possible roots are ± 1 and ± 2 by the rational root theorem, and none of those are actual roots.
2. Let us first express $\frac{1}{\sqrt[3]{2}-1}$ as a polynomial in $\sqrt[3]{2}$. For this, we want to find polynomials $U, V \in \mathbb{Q}[x]$ such that $U(x)(x^3 - 2) + V(x)(x - 1) = 1$; indeed, evaluating at $x = \sqrt[3]{2}$ will then yield $V(\sqrt[3]{2})(\sqrt[3]{2} - 1) = 1$ (notice that this is a concrete example of the argument used in the proof of the fact that $K[\alpha]$ is a field whenever α is algebraic over K).

To find U and V , we perform the Euclidian division of $x^3 - 2$ by $x - 1$, which yields

$$x^3 - 2 = (x^2 + x + 1)(x - 1) - 1.$$

We may thus take $U = -1$, $V = x^2 + x + 1$, and we find that

$$\frac{1}{\sqrt[3]{2}-1} = \sqrt[3]{2}^2 + \sqrt[3]{2} + 1.$$

Therefore,

$$\alpha = (\sqrt[3]{2} + 1)(\sqrt[3]{2}^2 + \sqrt[3]{2} + 1) = 2\sqrt[3]{2}^2 + 2\sqrt[3]{2} + 3,$$

we may thus take $a = 3$, $b = c = 2$.

3. Yes. Indeed, since $x^3 - 2$ is irreducible over \mathbb{Q} , it is the minimal polynomial of $\sqrt[3]{2}$ over \mathbb{Q} , so $1, \sqrt[3]{2}, \sqrt[3]{2}^2$ is a \mathbb{Q} -basis of K .

4. This degree is the same as the degree of the minimal polynomial of $\sqrt[3]{2}$ over \mathbb{Q} , that is to say 3.
5. If we had $\sqrt{2} \in K$, then we would have $\mathbb{Q}(\sqrt{2}) \subseteq K$. But this would imply

$$3 = [K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2[K : \mathbb{Q}(\sqrt{2})],$$

which is impossible since $[K : \mathbb{Q}(\sqrt{2})]$ is an integer.

6. (7 pts) If α were rational, then writing $\alpha = a + 0 \cdot \sqrt[3]{2} + 0 \cdot (\sqrt[3]{2})^2$ would contradict the unicity of the rationals a, b, c . So $\alpha \notin \mathbb{Q}$, and thus $[\mathbb{Q}(\alpha) : \mathbb{Q}] > 1$.

But we also have

$$3 = [K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}],$$

and since 3 is prime and $[\mathbb{Q}(\alpha) : \mathbb{Q}] > 1$, we must have $[K : \mathbb{Q}(\alpha)] = 1$, which means that $\mathbb{Q}(\alpha) = K$.

7. Using complex embeddings would lead us to computing with both $\sqrt[3]{2}$ and $e^{2\pi i/3}$, which sounds really tedious, so instead we compute that the matrix of the multiplication-by- α map with respect to the \mathbb{Q} -base $1, \sqrt[3]{2}, \sqrt[3]{2}^2$ of K , which turns out to be

$$\begin{pmatrix} 3 & 4 & 4 \\ 2 & 3 & 4 \\ 2 & 2 & 3 \end{pmatrix}.$$

We then compute $\chi_{\mathbb{Q}}^K(\alpha)$ as the characteristic polynomial of this matrix; after some effort, we find

$$\chi_{\mathbb{Q}}^K(\alpha) = x^3 - 9x^2 + 3x - 3.$$

From the coefficients of x^2 and x^0 respectively, we finally deduce that $\text{Tr}_{\mathbb{Q}}^K(\alpha) = 9$ and that $N_{\mathbb{Q}}^K(\alpha) = 3$.

8. Since $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [K : \mathbb{Q}] = 3$ by the previous questions, the degree of the minimal polynomial of α over \mathbb{Q} is 3. But $\chi_{\mathbb{Q}}^K(\alpha) = x^3 - 9x^2 + 3x - 3$ has degree 3, kills α , and is monic, so it is the minimal polynomial of α over \mathbb{Q} . (Remember that in general, the characteristic polynomial is a power of the minimal polynomial).

Exercise 1.4: Resultant practice

1. Let $\gamma = \sqrt{3} - \sqrt[3]{2}$. Express a non-zero polynomial in $\mathbb{Q}[x]$ vanishing at γ as a resultant, and then express this resultant as a determinant.

You are not required to compute this determinant explicitly. All this questions asks is to express this polynomial as a resultant, and then as a determinant, but you are not required to compute this polynomial explicitly.

2. Let $K = \mathbb{Q}(\alpha)$ be a number field, let $A(x) \in \mathbb{Q}[x]$ be the minimal polynomial of α , and let $\beta = B(\alpha) \in K$, where $B(x) \in \mathbb{Q}[x]$ is some polynomial. Express the characteristic polynomial $\chi_{\mathbb{Q}}^K(\beta)$ of β in terms of a resultant involving A and B .

Hint: Think in terms of complex embeddings.

Solution 1.4:

1. $\alpha = \sqrt[3]{2}$ is killed by $A(x) = x^3 - 2$, and $\beta = \sqrt{3}$ is killed by $x^2 - 3$. (These are in fact minimal polynomials, but it does not matter here.) Therefore, a polynomial killing $\gamma = \beta - \alpha$ is

$$C(x) = \prod_{\substack{a \in \mathbb{C} \\ A(a)=0}} B(x+a) = \text{Res}_y (A(y), B(x+y)).$$

Since the coefficients of $B(x+y) = (x+y)^2 - 3 = y^2 + 2xy + x^2 - 3$ are $(1, 2x, x^2 - 3)$ when seen as a polynomial in y , we have

$$C(x) = \begin{vmatrix} 1 & 0 & 0 & -2 & 0 \\ 0 & 1 & 0 & 0 & -2 \\ 1 & 2x & x^2 - 3 & 0 & 0 \\ 0 & 1 & 2x & x^2 - 3 & 0 \\ 0 & 0 & 1 & 2x & x^2 - 3 \end{vmatrix}.$$

Remark: Although the exercise explicitly said you did not have to do it, this evaluates to $x^6 - 9x^4 + 4x^3 + 27x^2 + 36x - 23$, if you wanted to know. In fact this is irreducible over \mathbb{Q} (I checked on a computer that it is irreducible mod 7), so this is the minimal polynomial of γ over \mathbb{Q} .

2. Let Σ be the set of embeddings of K into \mathbb{C} . When σ ranges over Σ , $\sigma(\alpha)$ ranges over the complex roots of $A(x)$, so that

$$\begin{aligned} \chi_{\mathbb{Q}}^K(\beta) &= \prod_{\sigma \in \Sigma} (x - \sigma(\beta)) \\ &= \prod_{\sigma \in \Sigma} (x - \sigma(B(\alpha))) \\ &= \prod_{\sigma \in \Sigma} (x - B(\sigma(\alpha))) \\ &= \prod_{\substack{a \in \mathbb{C} \\ A(a)=0}} (x - B(a)) \\ &= \text{Res}_y (A(y), x - B(y)). \end{aligned}$$

Remark: Algorithmically speaking, this is in general the fastest way to compute characteristic polynomials.

Exercise 1.5: (Non)-repeated values of complex embeddings

Let K be a number field of degree $n = [K : \mathbb{Q}]$, let $\alpha \in K$, and let $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$.

Prove that α is a primitive element for K/\mathbb{Q} if and only if the values $\{\sigma(\alpha), \sigma \in \text{Hom}(K, \mathbb{C})\}$ are all distinct.

More generally (without assuming that α is a primitive element), relate the values $\{\sigma(\alpha), \sigma \in \text{Hom}(K, \mathbb{C})\}$ to the roots of the characteristic polynomial and of the minimal polynomial of α , and explain what their multiplicities are. How many times is each value $\sigma(\alpha)$ repeated in $\{\sigma(\alpha), \sigma \in \text{Hom}(K, \mathbb{C})\}$?

Solution 1.5:

Let m_α and χ_α be the minimal and characteristic polynomials of α , respectively. We know that $\deg m_\alpha = d$ and that $\deg \chi_\alpha = n$; besides χ_α is a power of m_α , so necessarily $\chi_\alpha = m_\alpha^{n/d}$ by considering the degrees.

Therefore, if α is a primitive element, then $\mathbb{Q}(\alpha) = K$ so $d = n$ so $\chi_\alpha = m_\alpha$ is irreducible and therefore has no repeated roots. Conversely, if $\chi_\alpha = m_\alpha^{n/d}$ has no repeated roots, then $n/d = 1$, so $[K : \mathbb{Q}(\alpha)] = [K : \mathbb{Q}]/[\mathbb{Q}(\alpha) : \mathbb{Q}] = n/d = 1$, so $K = \mathbb{Q}(\alpha)$, so α is a primitive element.

In general, we know that

$$\chi_\alpha = \prod_{\sigma: K \hookrightarrow \mathbb{C}} (x - \sigma(\alpha)),$$

so the roots of χ_α are the $\sigma(\alpha)$ counted **with** multiplicity.

In contrast, the roots of m_α are the $\sigma(\alpha)$ counted **without** multiplicity. To see why, first notice that m_α has no repeated roots, as it is irreducible; therefore all we have to show is that a complex number is a root of m_α if and only if it is of the form $\sigma(\alpha)$ for some $\sigma : K \hookrightarrow \mathbb{C}$. And indeed, first of all that the $\sigma(\alpha)$ are roots of m_α since $0 = \sigma(0) = \sigma(m_\alpha(\alpha)) = m_\alpha(\sigma(\alpha))$, and conversely, if $z \in \mathbb{C}$ is a root of m_α , then there exists an embedding τ of $\mathbb{Q}(\alpha) \simeq \mathbb{Q}[x]/(m_\alpha)$ that takes α to z , and this τ extends (in exactly $[L : \mathbb{Q}(\alpha)] = n/d$ ways) to K , so that there does exist a $\sigma : K \hookrightarrow \mathbb{C}$ (and in fact n/d of them) such that $\sigma(\alpha) = z$.

This logic also shows that the quantity $\sigma(\alpha)$ assumes $d = \deg m_\alpha$ distinct values as σ ranges over $\text{Hom}(K, \mathbb{C})$, each value being repeated n/d times. This is also visible on the identity

$$\prod_{\sigma: K \hookrightarrow \mathbb{C}} (x - \sigma(\alpha)) = \chi_\alpha = m_\alpha^{n/d}.$$

The case $d = n$ corresponds to the special case where α is a primitive element (so in $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq K$, the **right** inclusion is an equality). The other extreme case is $d = 1$, which happens iff. $\alpha \in \mathbb{Q}$ (meaning that in $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq K$, the **left** inclusion is an equality), in which case $m_\alpha = x - \alpha$ and $\chi_\alpha = (x - \alpha)^n = m_\alpha^{n/1}$.