Solutions of exercise sheet 11

The content of the marked exercises **(*)** should be known for the exam.

1. For the following values of $\alpha \in \mathbb{C}$, find the minimal polynomial of α over $\mathbb{Q}$:

- $\alpha = \sqrt{2} + \sqrt{5}$
- $\alpha = \sqrt{3} - \sqrt[3]{3}$
- $\alpha = \lambda + i\lambda$, where $\lambda \in \mathbb{R}_{>0}$, $\lambda^4 = 5$.

Solution:

- Suppose that $\alpha = \sqrt{2} + \sqrt{5}$. Then we have $\alpha^2 = 7 + 2\sqrt{10}$, which implies (by subtracting 7 from both sides and squaring them) $\alpha^4 - 14\alpha^2 + 49 = 40$, so that α satisfies the polynomial $f(X) = X^4 - 14X^2 + 9$. To prove that f is the minimal polynomial of α, we need to check that it is irreducible over $\mathbb{Q}$. Notice that the complex roots of f are $\pm\alpha$ and $\pm(\sqrt{2} - \sqrt{5})$ so that there is no linear factor in the decomposition of f. The only remaining possibility for f not to be irreducible would be that it factors into two rational polynomials of degree 2, in which case one of two factors would be $(X - \alpha)(X - \beta) \in \mathbb{Q}[X]$ for β equal to one of the remaining roots. It can be easily checked that none of those polynomials have rational coefficients, contradiction. Hence $f(X) = X^4 - 14X^2 + 9$ is the minimal polynomial of $\alpha = \sqrt{2} + \sqrt{5}$.
- Suppose that $\alpha = \sqrt{3} - \sqrt[3]{3}$. Then $(\alpha - \sqrt{3})^3 = (-\sqrt[3]{3})^3$, i.e., $\alpha^3 + 9\alpha + 3 = \sqrt{3}(3\alpha^2 + 3)$, which implies, by squaring both sides,
$$\begin{aligned} &\alpha^6 + 81\alpha^2 + 9 + 18\alpha^4 + 6\alpha^3 + 54\alpha = 27(\alpha^4 + 2\alpha^2 + 1) \iff \\ &\alpha^6 - 9\alpha^4 + 6\alpha^3 + 27\alpha^2 + 54\alpha - 18 = 0. \end{aligned}$$
Then α is a root of $f(X) = X^6 - 9X^4 + 6X^3 + 27X^2 + 54X - 18$ and we claim this polynomial is irreducible. This is true if and only if $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$. Notice that $\alpha \in \mathbb{Q}(\sqrt[6]{3})$, which is a degree-6 extension of $\mathbb{Q}$ (because the polynomial $X^6 - 3$ is irreducible in $\mathbb{Q}[X]$ by Eisenstein Criterion and Gauss's Lemma below). Hence f is irreducible if and only if $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[6]{3})$, which is true if and only if $(1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5)$ are generators for $\mathbb{Q}(\sqrt[6]{3})$. Denote $\beta = \sqrt[6]{3}$, so that $\alpha = \beta^3 - \beta^2 = \beta^2(\beta - 1)$. Then we have
$$\begin{aligned} &\alpha^2 = 3 + \beta^4 - 2\beta^5, \\ &\alpha^3 = 3(\beta - 1)^3 = -3 + 9\beta - 9\beta^2 + 3\beta^3 \\ &\alpha^4 = 3\beta^2(\beta - 1)^4 = 9 + 3\beta^2 - 12\beta^3 + 18\beta^4 - 12\beta^5 \\ &\alpha^5 = 3\beta^4(\beta - 1)^5 = -90 + 90\beta - 45\beta^2 + 9\beta^3 - 3\beta^4 + 15\beta^5, \end{aligned}$$

Please turn over!

which can be written in matrix notation as

$$\begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \\ \alpha^3 \\ \alpha^4 \\ \alpha^5 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 \\ 3 & 0 & 0 & 0 & 1 & -2 \\ -3 & 9 & -9 & 3 & 0 & 0 \\ 9 & 0 & 3 & -12 & 18 & -12 \\ -90 & 90 & -45 & 9 & -3 & 15 \end{pmatrix} \begin{pmatrix} 1 \\ \beta \\ \beta^2 \\ \beta^3 \\ \beta^4 \\ \beta^5 \end{pmatrix}.$$

Since the determinant of the square matrix can be computed to be $-3^4 \cdot 73$, it is invertible, making $(1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5)$ a $\mathbb{Q}$-basis for $\mathbb{Q}(\beta)$, so that $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$ and $f(X) = X^6 - 9X^4 + 6X^3 + 27X^2 + 54X - 18$ is the minimal polynomial of α.

- Suppose that $\alpha = \lambda + i\lambda$, with $\lambda = \sqrt[4]{5}$. Then $\alpha = \lambda\sqrt{2}e^{i\pi/4}$ and $\alpha^4 = 5 \cdot 4 \cdot e^{i\pi} = -20$ and α is a root of $f(X) = X^4 + 20$. This is a polynomial with integer coefficients which is irreducible in $\mathbb{Z}[X]$ by Eisenstein's Criterion (Exercise 2.3 from Exercise sheet 9). As it is monic, it has coprime coefficients, so that it is also irreducible in $\mathbb{Q}[X]$ by Gauss's Lemma (see below). Then $f(X) = X^4 + 20$ is the minimal polynomial of α.

We say that a polynomial $f \in \mathbb{Z}[X]$ is *primitive* if the coefficients of f are coprime.

Gauss's Lemma. The product of two primitive polynomials in $\mathbb{Z}[X]$ is a primitive polynomial. If $f(X) \in \mathbb{Z}[X]$ is primitive, then it is irreducible in $\mathbb{Z}[X]$ if and only if it is irreducible in $\mathbb{Q}[X]$.

Proof: For the first part of the statement, notice that a polynomial $f \in \mathbb{Z}[X]$ is primitive if and only if for every prime p one has $0 \neq \bar{f} \in \mathbb{Z}/p\mathbb{Z}[X]$ (via the reduction map $\mathbb{Z}[X] \to \mathbb{Z}/p\mathbb{Z}$ from Exercise 2.1 in Exercise sheet 9). Then if f and g are primitive, the reduction modulo each p of fg, which is $\bar{f} \cdot \bar{g}$, cannot be zero, as $\mathbb{Z}/p\mathbb{Z}[X]$ is an integral domain and $\bar{f}, \bar{g} \neq 0$. Hence fg is primitive.

For the second part, it is easy to see that when $f \in \mathbb{Z}[X]$ is irreducible in $\mathbb{Q}[X]$, then so is in $\mathbb{Z}[X]$, because if $f = gh$ is a non-trivial factorization in $\mathbb{Z}[X]$ (that is, $g, h \notin \mathbb{Z}[X]^\times$), then g and h are non-constant (as f is primitive), so that $f = gh$ is also a non-trivial factorization in $\mathbb{Q}[X]$.

Conversely, assume that f is irreducible in $\mathbb{Z}[X]$, and that $f = gh$ is a factorization in $\mathbb{Q}[X]$. Let $n = \deg(f)$, $d = \deg(g)$ and $e = \deg(h)$. Computing common denominators and putting together common factors of the resulting numerator, one can find $\gamma, \tau \in \mathbb{Q}$ and primitive polynomials $\tilde{g}, \tilde{h} \in \mathbb{Z}[X]$ such that $g = \gamma\tilde{g}$ and $h = \tau\tilde{h}$. Then $f = \gamma\tau\tilde{g}\tilde{h}$. Since $\tilde{g}\tilde{h}$ is primitive by previous part, we get $\gamma\tau \in \mathbb{Z}$ (actually, $\gamma\tau = \pm 1$, as f is also primitive). □

2. Suppose that the field extension $L = K(\alpha)$ over K is finite of odd degree. Prove: $L = K(\alpha^2)$.

Solution:

See next page!

Of course, one has $K \subseteq K(\alpha^2) \subseteq K(\alpha) = L$, and by multiplicativity of degrees in towers, we have $[L : K] = [L : K(\alpha^2)][K(\alpha^2), K]$, and since $[L : K]$ is odd by hypothesis, we get that $[L : K(\alpha^2)]$ is also odd. Moreover, α satisfies the polynomial $f(X) = X^2 - \alpha^2 \in K(\alpha^2)$, so that $[L : K(\alpha^2)] \leq 2$. This degree can then only be equal to 1, which implies $L = K(\alpha^2)$.

3. (*) (Trace and norm for finite field extensions) Let L over K be a finite field extension.

1. For $x \in L$, show that the following is a K-linear map:

$$\begin{aligned} m_x : L &\to L \\ y &\mapsto xy. \end{aligned}$$

When $K = \mathbb{R}$, $L = \mathbb{C}$ and $\alpha \in \mathbb{C}$, compute the matrix representing m_α with respect to the basis $(1, i)$.

2. Show that we have an injective ring homomorphism

$$\begin{aligned} r_{L/K} : L &\to \mathrm{End}_K(L) \\ x &\mapsto m_x. \end{aligned}$$

3. Consider the maps

$$\begin{aligned} \mathrm{Tr}_{L/K} : L &\to K \\ x &\mapsto \mathrm{Tr}(m_x) \end{aligned} \qquad \text{(trace map)}$$

and

$$\begin{aligned} \mathrm{N}_{L/K} : L &\to K \\ x &\mapsto \det(m_x). \end{aligned} \qquad \text{(norm map)}$$

Prove:

- $\mathrm{Tr}_{L/K}$ is K-linear
- $\mathrm{N}_{L/K}(xy) = \mathrm{N}_{L/K}(x)\mathrm{N}_{L/K}(y)$ for every $x, y \in L$, and $\mathrm{N}_{L/K}(x) = 0$ if and only if $x = 0$.

4. Given a tower of finite extensions $L_1/L_2/K$, show that

$$\mathrm{Tr}_{L_1/K} = \mathrm{Tr}_{L_2/K} \circ \mathrm{Tr}_{L_1/L_2}.$$

[*Hint:* Get a K-basis for L_1 starting from a K-basis for L_2 and an L_2-basis for L_1, then evaluate the right hand side on $\alpha \in L_1$].

5. Prove that if $x \in L$ is such that $L = K(x)$, and

$$\mathrm{Irr}(x, K)(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_1 X + a_0 \in K[X],$$

then $\mathrm{Tr}_{L/K}(x) = -a_{d-1}$ and $\mathrm{N}_{L/K}(x) = (-1)^d a_0$. [*Hint:* $(1, x, \ldots, x^{d-1})$ is a K-basis of L.]

Please turn over!

6. Let p be an odd prime number, $\zeta_p = e^{\frac{2\pi i}{p}}$ and $K_p = \mathbb{Q}(\zeta_p)$. Find $\mathrm{Irr}(\zeta_p, \mathbb{Q})$, $\mathrm{Tr}_{K_p/\mathbb{Q}}(\zeta_p)$, $\mathrm{N}_{K_p/\mathbb{Q}}(\zeta_p)$ and $\mathrm{N}_{K_p/\mathbb{Q}}(\zeta_p - 1)$. [*Hint:* Look at Exercise 2.4 from Exercise sheet 9. Use previous point, and notice that $\mathbb{Q}(\zeta_p) = \mathbb{Q}(\zeta_p - 1)$.]

Solution:

1. It is immediate to check K-linearity of each map m_x. Indeed, m_x is additive by distributivity of the multiplication with respect to addition, and it respect scalar multiplication by commutativity of the multiplication in L.

   For $K = \mathbb{R}$, $L = \mathbb{C}$ and $\alpha = a+ib \in \mathbb{C}$ (with $a, b \in \mathbb{R}$), we have $m_\alpha(1) = \alpha = a+ib$, while $m_\alpha(i) = -b + ia$, so that m_α is represented by the matrix

$$M_\alpha = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

2. We immediately notice that $m_0 = 0$ and $m_1 = \mathrm{id}_L$. For $x, y, z \in L$, we have $m_{x+y}(z) = (x+y)z = xz + yz = m_x(z) + m_y(z)$ and $m_{xy}(z) = (xy)z = x(yz) = m_x(m_y(z)) = (m_x \circ m_y)(z)$. This means that $r_{L/K}$ respects both sum and multiplication, and we can conclude that it is a ring homomorphism. As $r_{L/K}$ is not the zero map (since it sends $1 \mapsto id_L \neq 0$) and L is a field, the kernel is equal to (0), so that $r_{L/K}$ is injective.
3. First, we prove linearity of $\mathrm{Tr}_{L/K}$. Let $n = [L : K]$ and fix a K-basis $\mathcal{B}$ for L. Then by basic linear algebra we have a K-linear ring isomorphism $\varphi : \mathrm{End}_K(L) \to M_n(K)$. Also, the trace map $\mathrm{tr} : M_n(K) \to K$ is easily seen to be K-linear. Then by construction we have that $\mathrm{Tr}_{L/K} = \mathrm{tr} \circ \varphi \circ r_{L/K}$, which is K-linear as it is a composition of K-linear maps.

   As concerns norm, we have $\mathrm{N}_{L/K} = \det \circ \varphi \circ r_{L/K}$. Since all the composed maps respect multiplication, so does $\mathrm{N}_{L/K}$. Moreover, we have $\mathrm{N}_{L/K}(x) = 0$ if and only if $\det(m_x) = 0$, which is equivalent to saying that m_x is not an invertible endomorphism, and this happens precisely when $x = 0$ (since for $x \neq 0$, me have $m_{x^{-1}} = m_x^{-1}$).
4. Let $\mathcal{B}_1 = (e_1, \ldots, e_k)$ be an L_2-basis for L_1, and $\mathcal{B}_2 = (f_1, \ldots, f_l)$ be an K-basis for L_2. As seen in class, $\mathcal{B} := (e_1 f_1, e_1 f_2, \ldots, e_1 f_l, e_2 f_1, \ldots, e_2 f_l, \ldots, e_k f_1, \ldots, e_k f_l)$ is a K-basis for L_1.

   For $\alpha \in L_1$, we can find coefficients $\lambda_{ij} \in L_2$, with $1 \leq i, j \leq k$, so that for each i one has

$$\alpha \cdot e_i = \sum_{j=1}^{k} \lambda_{ij} e_j.$$

   Then for each i, j as above and $1 \leq s, t \leq l$ we can find coefficients $\mu_{ijst} \in L_2$ such that for each i, j and s one has

$$\lambda_{ij} \cdot f_s = \sum_{t=1}^{l} \mu_{ijst} f_t.$$

See next page!

Putting those two equalities together we get, for each i and t as above,

$$\alpha \cdot e_i f_s = \sum_{j=1}^{k} \sum_{t=1}^{l} \mu_{ijst} e_j f_t$$

Then the matrix correspondent to m_α as a L_2-linear map of L_1, with respect to the basis $\mathcal{B}_1$, is

$$[m_\alpha]_{L_1/L_2} = {}^T(\lambda_{ij})_{i,j},$$

so that $\mathrm{Tr}_{L_1/L_2}(\alpha) = \sum_{i=1}^{k} \lambda_{ii}$. Moreover, the matrix correspondent to m_α as a K-linear map of L_1, with respect to the basis $\mathcal{B}$, is

$$[m_\alpha]_{L_1/K} = {}^T(\mu_{ijst})_{(i,s),(j,t)},$$

where the row index is the couple (i, s) and the column index is the couple (j, t), and row (column) indexes are ordered with lexicographical order, so that $\mathrm{Tr}_{L_1/K}(\alpha) = \sum_{i=1}^{k} \sum_{s=1}^{l} \mu_{iiss}$.
Furthermore, for each i, j as before, the matrix correspondent to $m_{\lambda_{i,j}}$ as a K-linear map of L_2, with respect to the basis $\mathcal{B}_2$, is

$$[m_{\lambda_{i,j}}]_{L_2/K} = {}^T(\mu_{ijst})_{s,t},$$

so that $\mathrm{Tr}_{L_2/K}(\lambda_{ij}) = \sum_{s=1}^{l} \mu_{ijss}$.
In conclusion, we have

$$\mathrm{Tr}_{L_2/K}(\mathrm{Tr}_{L_1/L_2}(\alpha)) = \mathrm{Tr}_{L_2/K}(\sum_{i=1}^{k} \lambda_{ii}) = \sum_{i=1}^{k} \mathrm{Tr}_{L_2/K}(\lambda_{ii}) = \sum_{i=1}^{k} \sum_{s=1}^{l} \mu_{iiss} = \mathrm{Tr}_{L_1/K}(\alpha).$$

5. We have that $L \cong K[X]/(P(X))$ as field extensions of K, and that $(1, x, \ldots, x^{d-1})$ is a K-basis for L. Then we are interested in the matrix $M_x = (\lambda_{ij})_{0 \le i,j \le d-1}$ associated to m_x. For $j = 0, \ldots, d-2$, we have $x \cdot x^j = x^{j+1}$ so that we have

$$\lambda_{ij} = \begin{cases} 1 & \text{if } i = j+1 \\ 0 & \text{else.} \end{cases}, \text{ for } j = 0, \ldots, d-2.$$

Moreover, $x \cdot x^{d-1} = x^d = -a_0 - a_1 x - \cdots - a_{d-1} x^{d-1}$, so that

$$\lambda_{i,(d-1)} = -a_i.$$

What we have found is

$$M_x = \begin{pmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{d-2} \\ 0 & \ldots & 0 & 1 & -a_{d-1} \end{pmatrix}.$$

Then we get $\mathrm{Tr}_{L/K}(x) = \mathrm{tr}(M_x) = -a_{d-1}$, and using Legendre form for the determinant on the first row we also obtain $\mathrm{N}_{L/K}(x) = \det(M_x) = (-1)^d a_0$.

Please turn over!

6. Using the solution of Exercise 2.4 from Exercise sheet 9, ζ_p satisfies the cyclotomic polynomial $\varphi_p(X) = X^{p-1} + \cdots + X + 1 \in \mathbb{Z}[X]$, which is irreducible in $\mathbb{Z}[X]$. Since φ_p is a primitive polynomial, it is also irreducible in $\mathbb{Q}[X]$ by Gauss Lemma, so that $\mathrm{Irr}(\zeta_p, \mathbb{Q}) = \varphi_p$. Then by previous point we have $\mathrm{Tr}_{K_p/\mathbb{Q}}(\zeta_p) = -1$ and $\mathrm{N}_{K_p/\mathbb{Q}}(\zeta_p) = 1$ as p is odd.
   Notice that we have $\mathbb{Q}(\zeta_p) = \mathbb{Q}(\zeta_p - 1)$, so that $\mathrm{Irr}(\zeta_p - 1, \mathbb{Q}$ has degree $p - 1$. Since $\zeta_p - 1$ satisfies $G(X) := \varphi_p(X + 1)$ which is irreducible of degree $p - 1$, we get
   $$\mathrm{Irr}(\zeta_p - 1, \mathbb{Q}) = \varphi_p(X + 1) = \frac{(X + 1)^p - 1}{X},$$
   whose constant coefficient is easily seen to be equal to p, so that $N_{L/K}(\zeta_p - 1) = p$.

4. Prove that for every algebraic field extension $K/\mathbb{R}$ we have that K is isomorphic either to $\mathbb{R}$ or to $\mathbb{C}$.

Solution:

Given a field k and an algebraic closure $\bar{k}$ of k, we have that for every algebraic extension K/k, the field K is isomorphic (with an isomorphism fixing k) to a field $K' \subseteq \bar{k}$. Indeed, fixing an algebraic closure $\bar{K}$ of K, we have that $\bar{K}$ is an algebraic closure of k.

Then by uniqueness of the algebraic closure there exists an isomorphism $\varphi : \bar{K} \to \bar{k}$ fixing k, so that $K \cong K' := \varphi(K) \subseteq \bar{k}$.

Applying this with $k = \mathbb{R}$ and K as in the exercise, we have that K is isomorphic over $\mathbb{R}$ to a field K' such that $\mathbb{R} \subseteq K' \subseteq \mathbb{C}$. As $\mathbb{C} = \mathbb{R} \oplus i\mathbb{R}$, we have $[\mathbb{C} : \mathbb{R}] = 2$, and the field extensions $K'/\mathbb{R}$ and $\mathbb{C}/K'$ are finite. By multiplicativity of the degree in towers of extensions, we have $[\mathbb{C} : K'][K' : \mathbb{R}] = [\mathbb{C} : \mathbb{R}] = 2$ and there are only 2 possibilities, in both of which the thesis is immediate:

- $[\mathbb{C} : K'] = 1$ and $[K' : \mathbb{R}] = 2$. Then $\mathbb{C} \cong K' \cong K$;
- $[\mathbb{C} : K'] = 2$ and $[K' : \mathbb{R}] = 1$. Then $\mathbb{R} \cong K' \cong K$.