Solutions of exercise sheet 1

1. Let K be a field. For each of the following statements, indicate whether it is true (with a proof) or false (by giving and explaining a counterexample):

1. Every algebraic extension L of K is a finite extension.
2. The field $\mathbb{C}$ is an algebraic closure of $\mathbb{Q}$.
3. Let L/K be a finite extension and $x \in L$; if P is the minimal polynomial of x, then we have $[L : K] = \deg(P)$.
4. The separable degree of the extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is 4.
5. There exists a finite field of order 243.
6. The extension $\mathbb{Q}(\exp(2i\pi/123))/\mathbb{Q}$ is algebraic.
7. If K_2/K_1 and K_1/K are algebraic extensions, then K_2/K is algebraic.
8. Let $L = \mathbb{Q}(\sqrt{2}, \exp(2i\pi/127), \sqrt{3+\sqrt[4]{12}})$; there exists $x \in \mathbb{C}$ such that $L = \mathbb{Q}(x)$.
9. Let L/K be a separable field extension and $n \geq 1$ an integer such that $[K(x) : K] \leq n$ for all $x \in L$; then $[L : K] \leq n$.

Solution:

1. False. For instance, the algebraic closure $\bar{\mathbb{F}}_p$ of the finite field $\mathbb{F}_p$ is infinite (as seen in the first semester, one can embed for n a positive integer each field $\mathbb{F}_{p^n}$ inside $\bar{\mathbb{F}}_p$. Since a finite extension of a finite field is finite, $\bar{\mathbb{F}}_p$ is not a finite extension of $\mathbb{F}_p$. But an algebraic closure is an algebraic extension by definition, so that this is indeed a counterexample.
2. False. $\mathbb{C}$ is not an algebraic extension of $\mathbb{Q}$, so by definition of algebraic closure it cannot be an algebraic closure of $\mathbb{Q}$. The fact that this is a transcendental extension can be stated by proving, for instance, that e or π are not algebraic. However the proof is not trivial (this is done more in general by the Lindemann-Weierstrass Theorem).
3. False. For instance, let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt[4]{2})$. We have $[L : K] = 4$, but for the element $x = \sqrt{2}$ has minimal polynomial $P(X) = X^2 - 2$ of degree 2.
4. True. Indeed, there are precisely 4 embedding of $\mathbb{Q}(\sqrt[4]{2}) \cong \mathbb{Q}[X]/(X^4 - 2)$ inside $\bar{\mathbb{Q}}$ which fix $\mathbb{Q}$. Indeed, such an embedding is determined by choosing an image of $\sqrt[4]{2}$, which simply needs to be a root of $X^4 - 2$, which is separable (it has 4 distinct roots $\sqrt[4]{2}i^k$, where $k = 0, 1, 2, 3$).
5. True, because $243 = 3^5$ and we can build $\mathbb{F}_{243}$ as a particular degree-5 extension of $\mathbb{F}_3$.

Please turn over!

6. True, because $\xi_{123} = \exp(2i\pi/123)$ is algebraic over $\mathbb{Q}$, and algebraic elements generate algebraic extensions. Indeed, ξ_{123} is a root of the polynomial $X^{123} - 1 \in \mathbb{Q}[X]$. The minimal polynomial is the 123-th cyclotomic polynomial

$$\Phi_{123}(X) = \prod_{\substack{1 \leq k \leq 122 \\ (k,123)=1}} (X - \xi_{123}^k).$$

7. True. Take $x \in K_2$ and let $P = X^n + a_1 X^{n-1} + \cdots + a_{n-1}X + a_n \in K_1[X]$ be its minimal polynomial. Denote $K_0 = K(a_1, \ldots, a_n)$. The extension K_0/K is finite (since it is finitely generated and algebraic). Also the extension $K_0(x)/K_0$ is finite, because x is algebraic over K_0 by construction. Since finiteness is preserved in towers, the extension $K_0(x)/K$ is finite, and so is the subextension $K(x)/K$. In particular, $K(x)/K$ is algebraic, and x is algebraic over K.
8. True. Let $\alpha = \sqrt{2}$, $\beta = \exp(2i\pi/127)$ and $\gamma = \sqrt{3 + \sqrt[4]{12}}$. Those three elements of $\mathbb{C}$ are algebraic over $\mathbb{Q}$:
   - α is a root of $X^2 - 2$;
   - β is a root of $X^{127} - 1$;
   - γ is a root of $(X^2 - 3)^4 - 12$.

   Then L is a finitely generated algebraic extension of $\mathbb{Q}$, so that it is finite. We also know that finite extensions of $\mathbb{Q}$ are always separable, so that we can apply the primitive element theorem and get that there exists $x \in L \subseteq \mathbb{C}$ such that $L = \mathbb{Q}(x)$.
9. True. Without loss of generality we can assume that n is minimal, so that there exists $x \in L$ such that $[K(x) : K] = n$. Suppose by contradiction that $[L : K] > n$. Then $K(x) \neq L$ and we can take $y \in L \setminus K(x)$. Then, for $L_0 := K(x, y)$, we get that L_0/K is a finitely generated algebraic separable extension, so that it is finite and separable and we can apply the primitive element theorem, obtaining $z \in L_0$ such that $L_0 = K(z)$. Then

$$[K(z) : K] = [K(x, y) : K] = [K(x, y) : K(x)][K(x) : K] > [K(x) : K] = n,$$

   contradiction.

2. Let $x = \sqrt{2} + \sqrt[3]{3}$.

1. Prove that $\mathbb{Q}(x) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$. [*Hint:* Find the minimal polynomial of $x - \sqrt{2}$ and expand]
2. Compute the minimal polynomial of x over $\mathbb{Q}(\sqrt{2})$. [*Hint:* $[\mathbb{Q}(x) : \mathbb{Q}(\sqrt{2})] = ?$]
3. Compute the minimal polynomial of x over $\mathbb{Q}$.

Solution:

See next page!

1. Clearly, $\mathbb{Q}(x) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$. For the other inclusion, it is enough to prove that $\sqrt{2} \in \mathbb{Q}(x)$, since this also implies that $\sqrt[3]{3} = x - \sqrt{2} \in \mathbb{Q}(x)$. This can be done by trying to solve Point (2): from $(x-\sqrt{2})^3 = 3$ we deduce $x^3 + 6x - 3 = \sqrt{2}(3x^2+2)$, so that
$$\sqrt{2} = \frac{x^3 + 6x - 3}{3x^2 + 2} \in \mathbb{Q}(x).$$
2. From the previous point, we have that x satisfies the polynomial
$$Q(X) = X^3 - 3\sqrt{2}X^2 + 6X - 2\sqrt{2} - 3 \in \mathbb{Q}(\sqrt{2})[X].$$
To prove that this is the minimal polynomial, it is enough to prove that $\mathbb{Q}(x) = \mathbb{Q}(\sqrt{2})(\sqrt[3]{3})$ is a degree-3 extension of $\mathbb{Q}(\sqrt{2})$, which is equivalent to saying that $\sqrt[3]{3}$ has degree 3 over $\mathbb{Q}(\sqrt{2})$. To prove this last equivalent statement, notice that $\sqrt[3]{3}$ is a root of the polynomial $f = X^3 - 3 \in \mathbb{Q}(\sqrt{2})[X]$, which can be easily checked to be irreducible. Indeed $\deg(f) = 3$, so that it is enough to check that f has no root in $\mathbb{Q}(\sqrt{2})$. For every element $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, with $a, b \in \mathbb{Q}$, we have (as 1 and $\sqrt{2}$ are linear independent over $\mathbb{Q}$):
$$(a + b\sqrt{2})^3 = 3 \iff \begin{cases} a^3 + 6ab^2 = 3 \\ 3a^2b + 2b^3 = 0. \end{cases}$$
The second equation holds for $b = 0$ or $3a^2 + 2b^2 = 0$, which both give $b = 0$, so that $a^3 = 3$, impossible in $\mathbb{Q}$. Hence $[\mathbb{Q}(x) : \mathbb{Q}] = 3$ and x has minimal polynomial Q over $\mathbb{Q}(\sqrt{2})$.
3. We have that $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, so that from what we found in the previous point we get
$$[\mathbb{Q}(x) : \mathbb{Q}] = [\mathbb{Q}(x) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 6.$$
Then the minimal polynomial of x over $\mathbb{Q}$ has degree 6.
Now, continuing the computations from Point (1) we get
$$x^6 + 36x^2 + 9 + 12x^4 - 6x^3 - 36x = 2(9x^4 + 12x^2 + 4),$$
so that x is a root of $P(X) = X^6 - 6X^4 - 6X^3 + 12X^2 - 36X + 1$, which by our previous discussion is the minimal polynomial of x over $\mathbb{Q}$.

3. Let p be a prime number and K a field of characteristic p. Let $\phi : K \to K$ be the Frobenius morphism given by $\phi(x) = x^p$.

1. Give an example of field K where ϕ is surjective, and an example where it is not.

We assume that ϕ is surjective.

2. Let $P \in K[X]$ be a polynomial such that $P' = 0$. Prove that there exists $Q \in K[X]$ such that $P = Q^p$.
3. Deduce that any irreducible polynomial $P \in K[X]$ is separable.

Please turn over!

4. Deduce that any algebraic extension L/K is separable.

Solution:

1. ϕ is always injective (as $\ker(\phi) = 0$), so that it is surjective when K is finite (e.g., $K = \mathbb{F}_p$). On the other hand, for $K = \mathbb{F}_p(T)$ we have $\phi(K) = \mathbb{F}_p(T^p)$ (indeed, $\phi(\mathbb{F}_p[X]) = \mathbb{F}_p[X]$ by surjectivity of ϕ on $\mathbb{F}_p$ and the fact that ϕ is additive, so that the isomorphism $\phi : \mathbb{F}_p[T] \longrightarrow \mathbb{F}_p[T^p]$ extends to the corresponding fraction fields). In particular, ϕ is not surjective for $K = \mathbb{F}_p(T)$.
2. Write $P = \sum_{i=0}^n a_i X^i$. Then $P' = \sum_{i=0}^n i a_i X^{i-1} = 0$ gives ia_i for each i which implies that $a_i = 0$ for $p \nmid i$, so that $P \in K[X^p] = \phi(K[X])$ as in the previous point (because we are now assuming that ϕ is surjective), meaning that there is a polynomial $Q \in K[X]$ such that $Q^p = P$.
3. Suppose that P is irreducible. As seen in class, P is then separable if and only if $P' \neq 0$. But if by contradiction $P' = 0$, then by previous point $P = Q^p$, contradiction with P irreducible.
4. It is enough to prove that every $x \in L$ is separable over K, that is, it has separable minimal polynomial. This is immediate from the previous point together with the irreducibility of the minimal polynomial.

4. Find an element $x \in K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ such that $K = \mathbb{Q}(x)$.

Solution:

We claim that $x = \sqrt{2} + \sqrt{3}$ is such an element. Of course, $K \supseteq \mathbb{Q}(x)$. On the other hand, $x(\sqrt{3} - \sqrt{2}) = 3 - 2 = 1$, so that $\sqrt{3} - \sqrt{2} = x^{-1} \in K$. Then

$$\frac{1}{2}(x + \sqrt{3} - \sqrt{2}) = \sqrt{3} \in K,$$

and it follows that $\sqrt{2} \in \mathbb{Q}(x)$ as well. This implies $K = \mathbb{Q}(x)$.

5. Let K be a field and let E_1 and E_2 be two algebraically closed extensions of K. Let $\bar{K}_1$ and $\bar{K}_2$ denote the algebraic closure of K in E_1 and E_2 respectively.

Let L be an algebraic extension of K.

1. Show that for any field homomorphism $\sigma : L \to E_1$ such that $\sigma|_K = \mathrm{Id}_K$, the image $\sigma(L)$ is contained in $\bar{K}_1$.
2. Show that the number of field homomorphisms $\sigma : L \to E_1$ such that $\sigma|_K = \mathrm{Id}_K$ is equal to the number of field homomorphisms $\sigma : L \to E_2$ such that $\sigma|_K = \mathrm{Id}_K$.

Solution:

See next page!

1. Let $x \in L$, $i \in \{1,2\}$ and $\sigma : L \to E_i$ such that $\sigma|_K = \mathrm{Id}_K$. Being L an algebraic extension of K, there exist a minimal polynomial P of x, so that $P(x) = 0$. Then

$$P(\sigma(x)) = \sigma(P(x)) = \sigma(0) = 0,$$

which implies that $\sigma(x)$ is algebraic over K, so that $\sigma(x) \in \bar{K}_i$. Then $\sigma(L) = \bar{K}_i$.

2. Given two field extensions N_1, N_2 of K, denote

$$\mathrm{Hom}_{K,\mathrm{m}}(N_1, N_2) := \{\psi : N_1 \longrightarrow N_2 | \phi \text{ is a field homomorphism and } \psi|_K = \mathrm{Id}_K\}.$$

From the previous point we get that for $i = 1, 2$ the field homomorphisms $L \longrightarrow E_i$ which fix K can be identified with those $L \longrightarrow \bar{K}_i$ simply by restricting the codomain. So there is a bijection $\gamma_i : \mathrm{Hom}_{K,\mathrm{m}}(L, E_i) \xrightarrow{\sim} \mathrm{Hom}_{K,\mathrm{m}}(L, \bar{K}_i)$. By unicity of the algebraic closure, there exists an isomorphism $\phi : \bar{K}_1 \to \bar{K}_2$, which (similarly as in Exercise 4 from Exercise Sheet 7 from Algebra I) induces the map $\phi^* : \mathrm{Hom}_{K,\mathrm{m}}(L, \bar{K}_1) \longrightarrow \mathrm{Hom}_{K,\mathrm{m}}(L, \bar{K}_2)$ sending $\tau \mapsto \phi \circ \tau$, which is easily seen to have inverse $(\phi^{-1})^* : \sigma \mapsto \phi^{-1} \circ \sigma$.
In conclusion,

$$\mathrm{Hom}_{K,\mathrm{m}}(L, E_1) \xrightarrow{\sim} \mathrm{Hom}_{K,\mathrm{m}}(L, \bar{K}_1) \xrightarrow{\sim} \mathrm{Hom}_{K,\mathrm{m}}(L, \bar{K}_2) \xleftarrow{\sim} \mathrm{Hom}_{K,\mathrm{m}}(L, E_2),$$

so that in particular $\mathrm{Hom}_{K,\mathrm{m}}(L, E_1)$ and $\mathrm{Hom}_{K,\mathrm{m}}(L, E_2)$ are in bijection as we were asked to prove.
N.B. The sets $\mathrm{Hom}_K, m(N_1, N_2)$ have a natural structure of K-vector spaces, and all the bijections we wrote are actually isomorphisms of K-vector spaces.