Solutions Exercise sheet 4

1. Let $F \subset K \subset L$ be fields. Show that $L : F$ is an algebraic extention if and only if $L : K$ and $K : F$ are algebraic.

Solution: ($\Leftarrow$) Assume $L : K$ and $K : F$ are algebraic. Let $l \in L$. Since $L : K$ is algebraic, l is a root of a non-zero polynomial over K. We will show that it is also the root of a non-zero polynomial with coefficients in F.

Let

$$f(x) := a_n x^n + \cdots + a_0$$

be a polynomial in $K[x]$ with root l. Since we also assume that the extention $K : F$ is algebraic, the degree $[F(a_0, \ldots, a_n) : F]$ is finite. Then also the degree $[F(a_0, \ldots, a_n, l) : F]$ is finite.

($\Rightarrow$) Assume that $L : F$ is an algebraic extention. Then since $K \subset L$, we have that $K : F$ is algebraic as well.

If $l \in L$, then since $L : F$ is algebraic, there exists a non-zero polynomial f with coefficients in F such that $f(l) = 0$. Since $F \subset K$, then $f \in K[x]$, so that l is algebraic over K and thus $L : K$ is algebraic as well.

2. Let $L : K$ be an algebraic field extention. Prove that every subring R of L which contains K is a field. Give a counter example in the case that the extention is not algebraic.

Solution: Let R be a subring as above. We need to prove that each element of R has a multiplicative inverse.

Let $0 \neq r \in R$. Then also $r \in L$ and since $L : K$ is algebraic, there exists a minimal polynomial $f(x) := x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, with $a_i \in K$ and $f(r) = 0$. By minimality, the coefficient a_0 has to be non-zero, and since K is a field, it has an inverse a_0^{-1} in K. Then

$$r \cdot (-a_0^{-1}) \cdot (r^{n-1} + a_{n-1}r^{n-2} + \cdots + a_1) = 1,$$

and since $r, a_i \in R$, for each i, r is invertible in R. Thus R is a field.

3. (a) Let F be a field and $a \in \overline{\mathbb{Q}}$ that generates a field extention of F of degree 7. Prove that a^2 generated the same extention.

(b) Prove that part **3**.a holds for 7 replaced by any odd integer.

Solution: (a) we have that a generates $F(a)$ with $[F(a) : F] = 7$. Note that $a^2 \in F(a)$, so that $F(a^2) \subset F(a)$. Because of the multiplicativity of the field degree, we have that $[F(a) : F(a^2)]$ must divide $[F(a) : F]$. Since $a \notin F$, we have $F(a^2) = F(a)$.

(b) If $[F(a) : F(a^2)]$ divides an odd integer, then it must be odd itself. Note that the minimal polynomial of a over $F(a^2)$ also divides the polynomial $x^2 - a$. Hence the degree is an odd integer less or equal $\deg(x^2 - a) = 2$, and we obtain $F(a^2) = F(a)$.

4. Let p and q are two distinct primes. Prove that $\mathbb{Q}(\sqrt{p})$ and $\mathbb{Q}(\sqrt{q})$ are isomorphic as vector spaces over $\mathbb{Q}$ but not as fields.

Solution: The minimal polynomials of $\sqrt{p}$ and $\sqrt{q}$ over $\mathbb{Q}$ are $x^2 - p$ and $x^2 - q$ respectfully. Both have degree two, so the elements $\sqrt{p}$ and $\sqrt{q}$ are algebraic over $\mathbb{Q}$. Thus $\mathbb{Q}(\sqrt{p})$ and $\mathbb{Q}(\sqrt{q})$ are both $\mathbb{Q}$-vector spaces of dimension 2 and thus isomorphic.

Claim. Prove that $\mathbb{Q}(\sqrt{p})$ and $\mathbb{Q}(\sqrt{q})$ are not isomorphic as fields.

Assume that there is a field isomorphism

$$\varphi : \mathbb{Q}(\sqrt{p}) \to \mathbb{Q}(\sqrt{q})$$

Since φ is a homomorphism, we have $\varphi(1) = 1$. Then we have

$$\varphi(\sqrt{p})^2 = \varphi(\sqrt{p}^2) = \varphi(p) = p \cdot \varphi(1) = p.$$

That means, that there exists $x \in \mathbb{Q}(\sqrt{q})$ with $x^2 = p$. We can write $x = a + b\sqrt{q}$ for some $a, b \in \mathbb{Q}$, which translates to

$$a^2 + qb^2 + 2ab\sqrt{q} = p.$$

If $a = 0$, we would have to solve $qb^2 = p$ for $b \in \mathbb{Q}$, which is not possible for prime numbers $p \neq q$. If $b = 0$ then we would have to solve $a^2 = p$ in $\mathbb{Q}$, which again is not possible. Hence we obtain our claim by contradiction.

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

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

(b) Compute the minimal polynomial of x over $\mathbb{Q}(\sqrt{2})$. [*Hint:* $[\mathbb{Q}(x) : \mathbb{Q}(\sqrt{2})] = ?$]

(c) Compute the minimal polynomial of x over $\mathbb{Q}$.

Solution:

(a) 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

$$\sqrt{2} = \frac{x^3 + 6x - 3}{3x^2 + 2} \in \mathbb{Q}(x).$$

(b) 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 $\mathbb{Q}(\sqrt{2})$.

(c) 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 $\mathbb{Q}$.