Solutions Exercise sheet 6

1. Let K be a field of characteristic 0 and $L : K$ a finite algebraic extention. Show that $L : K$ is simple if and only if there are only finitely many intermediate fields.

Solution: ($\Leftarrow$) Since the extention $L : K$ is finite, there exists $n \in \mathbb{Z}_{\geqslant 0}$ such that we can write $L = K(\alpha_1, \dots, \alpha_n)$, with $\alpha_i \in L$. We will prove this direction by induction over n.

For $n = 1$ this is clear.

Set $M = K(\alpha_1, \dots, \alpha_{n-1})$. Then $K \subseteq M \subseteq L$ is an intermediate field, and by our induction hypothesis we have $M = K(\beta)$ for some $\beta \in L$.

Then $L = K(\alpha_n, \beta) = K(\alpha_1, \dots, \alpha_n)$. For each $a \in K$ define $M_a := K(\alpha_n + a\beta)$. Then $K \subseteq M_a \subseteq L$ is an intermediate field.

By assumption, there exist only finitely many intermediate fields, but since K is infinite, there exist $a, b \in K$ with $a \neq b$ and $M_a = M_b$. Then

$$\beta = \frac{(\alpha_n + b\beta) - (\alpha_n + a\beta)}{b - a} \in M_b.$$

We have further that $\alpha_n = (\alpha_n + b\beta) - b\beta \in M_b$, since $(\alpha_n + b\beta) \in M_b$ and $b\beta \in M_b$. Hence $L = K(\alpha_n, \beta) = M_b = K(\alpha_n + b\beta)$, so that $L : K$ is simple.

($\Rightarrow$) Assume that $L = K(\alpha)$, for some $\alpha \in L$ and let M be an intermediate field $K \subseteq M \subseteq L$.

Then $L = M(\alpha)$. Let f be the minimal polynomial of α over K and let g be the minimal polynomial of α over M. Then $g \mid f$.

Write $g = a_0 + a_1 X + \dots + X^r$ and let $M_0 := K(a_0, \dots, a_{r-1}) \subseteq M$. Then $g \in M_0[X]$. For $\tilde{g}$ the minimal polynomial of α over M_0 we have $\tilde{g} \mid g$. Then

$$\begin{aligned}[L : M] &= \deg(g) \geqslant \deg(\tilde{g}) \\ &= [L : M_0] = [L : M][M : M_0],\end{aligned}$$

so that $[M : M_0] = 1$. Hence $M = M_0$ and M is determined by g (with $g \mid f$), and since f only has finitely many normed divisors (in a splitting field of f), there exist only finitely many intermediate fields.

2. (a) Prove that if $[K : k] = 2$, then $k \subseteq K$ is a normal extention.

(b) Show that $\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}$ is normal.

(c) Show that $\mathbb{Q}(\sqrt[4]{2}(1 + i)) : \mathbb{Q}$ is not normal over $\mathbb{Q}$.

(d) Deduce that given a tower $L : K : k$ of field extentions, $L : k$ needs not to be normal even if $L : K$ and $K : k$ are normal.

Solution:

(a) Since $[K : k] = 2$, there is an element $\xi \in K \backslash k$. Then $k(\xi) : k$ is a proper intermediate extension of $K : k$, and the only possibility is that $K = k(\xi)$, so that ξ has a degree-2 minimal polynomial $f(X) = X^2 - sX + t \in k[X]$. Then $s - \xi \in k(\xi) = K$ and

$$f(s-\xi) = s^2 - 2s\xi + \xi^2 - s^2 + s\xi + t = -s\xi + \xi^2 + t = f(\xi) = 0.$$

Hence K is the splitting field of f, implying that $K : k$ is a normal extension.

(b) Let us prove that $\mathbb{Q}(\sqrt[4]{2}, i)$ is the splitting field of the polynomial $X^4 - 2 \in \mathbb{Q}[X]$ (which is irreducible by Eisenstein's criterion). This is quite straightforward: this splitting field must contain all the roots of the polynomials, i.e. $\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}$, implying that it must contain $i\sqrt[4]{2}/\sqrt[4]{2} = i$, so that it must contain $\mathbb{Q}(\sqrt[4]{2}, i)$. Clearly all the roots of $X^4 - 2$ lie $\mathbb{Q}(\sqrt[4]{2}, i)$ which is then the splitting field of $X^4 - 2$, so that it is a normal extension of $\mathbb{Q}$.

(c) Since $i \notin \mathbb{R} \supseteq \mathbb{Q}(\sqrt[4]{2})$ satisfies the polynomial $X^2 + 1 \in \mathbb{Q}(\sqrt[4]{2})$, we have $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] = 2$. Moreover, $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ (as $X^4 - 2$ is irreducible by Eisenstein's criterion), so that

$$[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = 8.$$

Let $\gamma = \sqrt[4]{2}(1 + i)$. It is enough to prove that the minimal polynomial of γ over $\mathbb{Q}$ does not split in $\mathbb{Q}(\gamma)$ to conclude that $\mathbb{Q}(\gamma) : \mathbb{Q}$ is not a normal extension.

Notice that $\gamma^2 = \sqrt{2}(1 - 1 + 2i)$, so that $\gamma^4 = -8$, and γ satisfies the polynomial $g(X) = X^4 + 8 \in \mathbb{Q}[X]$. Hence $[\mathbb{Q}(\gamma) : \mathbb{Q}] \leqslant 4$. On the other hand,

$$\mathbb{Q}(\sqrt[4]{2}, i) = \mathbb{Q}(\sqrt[4]{2}(1+i), i) = \mathbb{Q}(\gamma)(i),$$

with $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\gamma)] \leqslant 2$ since i satisfies $X^2 + 1 \in \mathbb{Q}(\gamma)[X]$. Then

$$8 = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\gamma)(i) : \mathbb{Q}(\gamma)][\mathbb{Q}(\gamma) : \mathbb{Q}],$$

and the only possibility is that $[\mathbb{Q}(\gamma)(i) : \mathbb{Q}(\gamma)] = 2$ and $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 4$. In particular, $g(X)$ is the minimal polynomial of γ over $\mathbb{Q}$, and $i \notin \mathbb{Q}(\gamma)$. But the roots of $g(X)$ are easily seen to be $u\gamma$, for $u \in \{\pm 1, \pm i\}$, so that the root $i\gamma$ of g does not lie in $\mathbb{Q}(\gamma)$ (as $i \notin \mathbb{Q}(\gamma)$).

(d) Let $k = \mathbb{Q}$, $L = \mathbb{Q}(\gamma)$ and $K = \mathbb{Q}(\gamma^2)$. Then $\gamma^2 = 2\sqrt{2}i \notin \mathbb{Q}$ satisfies the degree-2 polynomial $Y^2 + 8 \in \mathbb{Q}[Y]$, so that $[K : k] = 2$. Since $[L : k] = 4$, we have $[L : K] = 2$. Then by point 1 the extensions $L : K$ and $K : k$ are normal, while $L : k$ is not by previous point.

3. (a) Let K be field containing $\mathbb{Q}$. Show that any automorphism of K is a $\mathbb{Q}$-automorphism.

(b) From now on, let $\sigma : \mathbb{R} \to \mathbb{R}$ be a field automorphism. Show that σ is increasing:

$$x \leqslant y \Longrightarrow \sigma(x) \leqslant \sigma(y).$$

(c) Deduce that σ is continuous.

(d) Deduce that $\sigma = \mathrm{Id}_{\mathbb{R}}$.

Solution:

(a) Let $\sigma : K \to K$ be a field automorphism, and suppose that $\mathbb{Q} \subseteq K$. Then $\mathbb{Z} \subseteq K$, and for every $n \in \mathbb{Z}$ one has $\sigma(n) = \sigma(n \cdot 1) = n\sigma(1)$, by writing n as a sum of 1's or -1's and using additivity of σ. Hence $\sigma|_{\mathbb{Z}} = \mathrm{Id}_{\mathbb{Z}}$. Now suppose $f \in \mathbb{Q}$, and write $f = mn^{-1}$ with $n \in \mathbb{Z}$. Then by multiplicativity of σ we obtain $\sigma(f) = \sigma(m)\sigma(n^{-1}) = mn^{-1} = f$, so that $\sigma|_{\mathbb{Q}} = \mathrm{Id}_{\mathbb{Q}}$ and σ is a $\mathbb{Q}$-isomorphism.

(b) Let $x, y \in \mathbb{R}$ such that $x \leqslant y$. Then $y - x \geqslant 0$, so that there exist $z \in \mathbb{R}$ such that $y - x = z^2$. Then

$$\sigma(y) - \sigma(x) = \sigma(y - x) = \sigma(z^2) = \sigma(z)^2 \geqslant 0,$$

so that $\sigma(y) \geqslant \sigma(x)$ and σ is increasing.

(c) To prove continuity, it is enough to check that inverse images of intervals are open. For $I = (a, b) \subseteq \mathbb{R}$ an interval with $a \neq b$, by surjectivity of σ there exist $\alpha, \beta \in \mathbb{R}$ such that $\sigma(\alpha) = a$ and $\sigma(\beta) = b$, and since σ is injective and increasing we need $\alpha < \beta$. Then $\sigma^{-1}(I) = \{x \in \mathbb{R} : a < \sigma(x) < b\} = \{x \in \mathbb{R} : \sigma(\alpha) < \sigma(x) < \sigma(\beta)\} = (\alpha, \beta)$, which is an open interval in $\mathbb{R}$. Hence σ is continuous.

(d) Now σ is continuous and so is $\mathrm{Id}_{\mathbb{R}}$. By part (a), those two maps coincide on $\mathbb{Q}$, which is a dense subset of $\mathbb{R}$. Then they must coincide on the whole $\mathbb{R}$, so that $\sigma = \mathrm{Id}_{\mathbb{R}}$.

4. (a) Show that every finite field is isomorphic to $\mathbb{F}_p[x]/(f(x))$ for some prime p and some monic irreducinle polynomial $f(x)$ in $\mathbb{F}_p[x]$.

(b) Show that each irreducible polynomial $f(x)$ in $\mathbb{F}_p[x]$ of degree n divides $x^{p^n} - x$ and is separable.

(c) Factor $x^8 - x$ and $x^{16} - x$ in $\mathbb{F}_2[x]$

Solution: (a) Let F be a finite field. We have seen in class that F has order p^n for some p and positive integer n.We have also seen that $F^\times$ is cyclic. Let α be a generator and consider the evaluation at α homomorphism $E_\alpha : \mathbb{F}_p[x] \to F$ which sends $g(x) \in \mathbb{F}_p[x]$ to $g(\alpha)$ and fixes $\mathbb{F}_p$.

Since every element of F is either zero or a power of α, and $E_\alpha(x^r) = \alpha^r$, E_α is surjective.

Therefore $F \simeq \mathbb{F}_p[x]/\ker E_\alpha$.

Since F is a field, the kernel of E_α is a maximal ideal in $\mathbb{F}_p[x]$ and hence $\ker E_\alpha = (f(x))$ for some monic irreducible polynomial $f(x)$.

(b) The field $\mathbb{F}_p[x]/(f(x))$ has order p^n, hence for all $t \in \mathbb{F}_p[x]/(f(x))$ we have $t^{p^n} = t$. In particular $x^{p^n} \equiv x \mod (f(x))$. Therefore $f(x)|(x^{p^n} - x)$ in $\mathbb{F}_p[x]$. Since $x^{p^n} - x$ is separable so is its factor $f(x)$

(c) $x^8 - x = x(x-1)(x^3 + x + 1)(x^3 + x^2 + 1)$

Note that $8 = 2^3$ and all irreducible polynomials of degree 1, namely x and $x - 1$ as well as degree 3 irreducible polynomials in $\mathbb{F}_2[x]$, namely $x^3 + x + 1$ and $x^3 + x^2 + 1$, appear in the factorization $x^8 - 3$.

Similarly we have

$$x^{16} - x = x(x-1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)$$

and the polynomials appearing on the right are all of the irreducible polynomials in $\mathbb{F}_2[x]$ of degree 1,2 and 4.

5. (a) Show that $(x^d - 1)|(x^n - 1)$ if and only if $d|n$

(b) Prove that a subfield F of $\mathbb{F}_{p^n}$ has order p^d where $d|n$.

(c) Show that for each $d|n$ there is one subfield F of $\mathbb{F}_{p^n}$ of order p^d.

Solution:

(a) Assume $(x^d - 1) \mid (x^n - 1)$. By Euclidean division, we can write $n = qd + r$, for $q, r \in \mathbb{Z}_{\geqslant 0}$ with $0 \leqslant r < d$. Note that

$$(x^d - 1) \mid (x^d - 1)(x^{n-d} + x^{n-2d} + \cdots + x^{n-qd} + 1)$$

Since $(x^d - 1)(x^{n-d} + x^{n-2d} + \cdots + x^{n-qd} + 1) = x^n + x^d - x^{n-qd} - 1$, we have $x^d - 1 \mid x^n - 1 + x^d - x^r$. Together with $(x^d - 1) \mid (x^n - 1)$, this implies

$$(x^d - 1) \mid (x^d - x^r) = (x^d - 1) + (1 - x^r),$$

which gives $(x^d - 1) \mid (x^r - 1)$. Hence $r = 0$, which implies $d \mid n$.
The other direction follows from the identity

$$x^n - 1 = (x^d)^{\frac{n}{d}} - 1 = (x^d - 1)((x^d)^{\frac{n}{d}-1} + (x^d)^{\frac{n}{d}-2} + \cdots + (x^d) + 1).$$

(b) Let F be a subfield of $\mathbb{F}_{p^n}$. Then $|F| = p^d$ for $d = [F : \mathbb{F}_p]$.
Note that the group of units F^* is a finite abelian group. Then by the main theorem on finitely generated abelian groups,

$$F^* \cong \mathbb{Z}/e_1\mathbb{Z} \times \ldots \mathbb{Z}/e_r\mathbb{Z}, \tag{1}$$

for $e_1, \ldots, e_r \in \mathbb{Z}_{\geqslant 1}$ with $e_1 \mid e_2 \mid \cdots \mid e_r$. Then we have for each $a \in \mathbb{F}^*$ that $a^{e_r} = 1$. Thus a is a zero of $X^{e_r} - 1$ and $|F^*| \leqslant e_r$. From (1) it also follows that $e_1 \cdots e_r = |F^*|$. Hence $e_1 = \cdots = e_{r-1} = 1$ and thus $r = 1$ and $|F^*|$ is cyclic of order $p^d - 1$.
Since $0^{p^d} = 0$, we have that each $a \in F$ is a zero of the polynomial $X^{p^d} - X$, so F is a splitting field of the polynomial $X^{p^d} - X$ over $\mathbb{F}_p$.
Similarly, $\mathbb{F}_{p^n}$ is the splitting field of the polynomial $X^{p^n} - X$, and since F is a subfield of $\mathbb{F}_{p^n}$, we have $(X^{p^d} - X) \mid (X^{p^n} - X)$, so by part (a), $p^d - 1$ divides $p^n - 1$. Replacing x by p in the proof of part (a), we obtain $d \mid n$.

(c) Let d be a positive integer such that $d \mid n$. Let F be the splitting field of the polynomial $X^{p^d} - X$ over $\mathbb{F}_p$. Then by the solution of part (b), F is a field of order p^d. Note that $\mathbb{F}_{p^n}$ is a splitting field of the polynomial $X^{p^n} - X$ over $\mathbb{F}_p$. Since $d \mid n$ implies $p^d - 1 \mid p^n - 1$, by part (a) we have that $X^{p^d} - X$ divides $X^{p^n} - X$. Hence F is an intermediate field $\mathbb{F}_p \subseteq F \subseteq \mathbb{F}_{p^n}$.