Solutions Exercise sheet 8

1. Recall that a normal closure of an extention $L : K$ is the smallest extention of L which is normal over K. Let $L : K$ be a finite extention. Show that there exists a normal closure N of $L : K$ which is a finite extention of K and that if M is another normal closure than the extentions $M : K$ and $N : K$ are isomorphic.

Hint: Let $\alpha_1, \dots \alpha_n$ be a basis of L over K with minimal polynomials $m_i = m_{\alpha_i,K}$ and consider the splitting field of the polynomial $m_1 m_2 \dots m_n$.

Solution:

Let $\alpha_1, \dots, \alpha_r$ be a basis for L over K, and let m_j be the minimal polynomial of α_j over K. Let N be the splitting field for $f = m_1 m_2 \dots m_r$ over L. Then N is also the splitting field for f over K, so $N : K$ is normal and finite by Theorem 2.24 from the lectures. Suppose that $L \subseteq P \subseteq N$ where $P : K$ is normal. Each polynomial m_j has a zero $\alpha_j \in P$, so by normality f splits in P. Since N is the splitting field for f, we have $P = N$. Therefore N is a normal closure.

Now suppose that M and N are both normal closures. The above polynomial f splits in M and in N, so each of M and N contain the splitting field for f over K. This splitting field contains L and is normal over K, so it must be equal to both M and N.

2. Let $L : K$ be a finite extention. Show that the following are equivalent

(a) $L : K$ is normal

(b) For every finite extention M of K containing L, every K-monomorphism $\varphi : L \to M$ is a K-automorphism of L.

(c) There exists a finite normal extention N of K containing L such that every every K-monomorphism $\varphi : L \to N$ is a K-automorphism of L.

Solution:

We show that **2**.$a \Rightarrow$ **2**.$b \Rightarrow$ **2**.$c \Rightarrow$ **2**.a.

(**2**.$a \Rightarrow$ **2**.b) If $L : K$ is normal then L is the normal closure of $L : K$.

Claim. We have $\varphi(L) \subseteq L$.

Let $a \in L$. Let m be the minimal polynomial of a over K. Then $m(a) = 0$, so $\varphi(m(a)) = 0$. But $\varphi(m(a)) = m(\varphi(a))$, since φ is a K-monomorphism, so $m(\varphi(a)) = 0$ and $\varphi(a)$ is a zero of m. Therefore $\varphi(a)$ lies in L since $L : K$ is normal and we obtain our claim.

But φ is a K-linear map defined on the finite-dimensional vector space L over K, and it is a monomorphism. Therefore $\varphi(L)$ has the same dimension as L, whence $\varphi(L) = L$ and φ is a K-automorphism of L.

(**2**.$b \Rightarrow$ **2**.c) Let N be the normal closure for $L : K$. Then N exists by Exercise **1**., and has the requisite properties by **2**.b.

(**2**.$c \Rightarrow$ **2**.a) Suppose that f is any irreducible polynomial over K with a zero $\alpha \in L$. Then f splits over N by normality, and if β is any zero of f in N, then by Lemma 3.2 from the lectures, there exists an automorphism σ of N such that $\sigma(\alpha) = \beta$. By hypothesis, σ is a K-automorphism of L, so $\beta = \sigma(\alpha) \in \sigma(L) = L$. Therefore f splits over L and $L : K$ is normal.

3. Let $L : K$ be a separable, finite extention of degree n. Show that there are exactly n K-monomorphisms of L into a normal closure N.

Solution:

Use induction on $[L : K]$. If $[L : K] = 1$, then the result is clear. Suppose that $[L : K] = k > 1$. Let $\alpha \in L \backslash K$ with minimal polynomial m over K. Then

$$\deg m = [K(\alpha) : K] = r > 1$$

Now m is an irreducible polynomial over a subfield of $\mathbb{C}$ with one zero in the normal extension N, so m splits in N and its zeros $\alpha_1, \dots, \alpha_r$ are distinct. By induction there are precisely s distinct $K(\alpha)$-monomorphisms $\rho_1, \dots, \rho_s : L \to N$, where $s = [L : K(\alpha)] = k/r$. By Lemma 3.2 from the lectures, there are r distinct K-automorphisms $\tau_1, \dots, \tau_r$ of N such that $\tau_i(\alpha) = \alpha_i$. The maps

$$\varphi_{ij} = \tau_i \rho_j \quad (1 \leqslant i \leqslant r, 1 \leqslant j \leqslant s)$$

are K-monomorphisms $L \to N$.

We claim they are distinct. Suppose $\varphi_{ij} = \varphi_{kl}$. Then $\tau_k^{-1}\tau_i = \rho_l \rho_j^{-1}$. The ρ_j fix $K(\alpha)$, so they map α to itself. But ρ_j is defined by its action on α, so $\rho_l \rho_j^{-1}$ is the identity. That is, $\rho_l = \rho_j$. So $\tau_k^{-1}\tau_i$ is the identity, and $\tau_k = \tau_i$. Therefore $i = k, j = l$, so the φ_{ij} are distinct. They therefore provide $rs = k$ distinct K-monomorphisms $L \to N$.

Finally, we show that these are all of the K-monomorphisms $L \to N$. Let $\tau : L \to N$ be a K-monomorphism. Then $\tau(\alpha)$ is a zero of m in N, so $\tau(\alpha) = \alpha_i$ for some i. The map $\varphi = \tau_i^{-1}\tau$ is a $K(\alpha)$-monomorphism $L \to N$, so by induction $\varphi = \rho_j$ for some j. Hence $\tau = \tau_i \rho_j = \varphi_{ij}$ and we are done.

4. Show that $x^4 + 1$ is irreducible in $\mathbb{Z}[x]$ but reducible in $\mathbb{F}_p[x]$ for every prime p.

Solution:

As we have already seen in class that

$$(x + 1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2$$

is irreducible by Eisenstein Criteria, and hence $x^4 + 1$ is irreducible in $\mathbb{Z}[x]$.

Consider the polynomial $x^4 + 1$ over $\mathbb{F}_p[x]$. If $p = 2$ then $x^4 + 1 = (x + 1)^4$, hence clearly reducible.

If p is an odd prime, then $p^2 - 1$ is divisible by 8, since p is congruent to $1, 3, 5$ or $7 \mod 8$ and all of these are squares $\mod 8$. Hence x^{p^2-1} is divisible by $x^8 - 1$.

This gives the divisibilities

$$x^4 + 1 \mid x^8 - 1 \mid x^{p^2-1} - 1 \mid x^{p^2} - x.$$

Therefore all the roots of $x^4 + 1$ are roots of $x^{p^2} - x$. Since the roots of $x^{p^2} - x$ are the elements of the field $\mathbb{F}_{p^2}$, it follows that the field extention generated by any root of $x^4 + 1$ is at most degree 2 over $\mathbb{F}_p$, which means $x^4 + 1$ cannot be irreducible over $\mathbb{F}_p$.

5. Let L be the splitting field of the polynomial $x^4 + 1$ over $\mathbb{Q}$ and let $G = \mathrm{Gal}(L : \mathbb{Q})$ be its Galois group. Determine G and the fixed fields corresponding to each of its subgroups.

Solution: We will start by determinining the splitting field of the polynomial $x^4 + 1$ over $\mathbb{Q}$. Let $\zeta := e^{\pi i/4} = \frac{i+1}{\sqrt{2}} \in \mathbb{C}$ be the primitive 8-th root of unity. Then the polynomial $x^4 + 1$ has the four zeros $\zeta^{\pm 1}, \zeta^{\pm 3}$, and thus the splitting field $L = \mathbb{Q}(\zeta)$. Since $\zeta^2 = i$, we have $L = \mathbb{Q}(i, \sqrt{2})$. Since $\mathbb{Q}(\sqrt{2})$ is contained in $\mathbb{R}$, we have $[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}(\sqrt{2})] = 2$, and together with $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ we obtain $[L : \mathbb{Q}] = [\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$.

Next, we will determine the Galois group. Since $L = \mathbb{Q}(\zeta)$, each element of the Galois group is determined by the image of ζ. Hence $G = \mathrm{Gal}(L : \mathbb{Q})$ operates transitively on the set of zeros $\{\zeta^{\pm 1}, \zeta^{\pm 3}\}$. Let $\sigma, \varphi \in G$ be such that $\sigma(\zeta) = \zeta^{-1}$ and $\varphi(\zeta) = \zeta^{-3}$. Since $(-1)^2 \equiv (-3)^2 \equiv 1 \pmod 8$, we have

$$\sigma^2(\zeta) = \varphi^2(\zeta) = \zeta,$$

and thus $\sigma^2 = \varphi^2 = 1$. Hence there are two distinct cyclic subgroups of order 2 in G, and since $|G| = 4$, we have that G is a product of two cyclic groups of order 2, so isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. It has subgroups $\langle\sigma\rangle$, $\langle\varphi\rangle$, $\langle\sigma\varphi\rangle$ of order 2 together with the trivial subgroup.

Now we can determine the fixed fields corresponding to each of the subgroups. From the lectures we know that $L^{\langle \mathrm{id} \rangle} = L$ and $L^G = \mathbb{Q}$.

Since $\varphi(i) = \varphi(\zeta^2) = \zeta^{10} = \zeta^2 = i$, we have that φ operates trivially on the intermediate field $\mathbb{Q}(i)$. Hence $\mathbb{Q}(i) \subset L^{\langle\varphi\rangle}$, so $[L^{\langle\varphi\rangle} : \mathbb{Q}] \geqslant 2$. Since $L^{\langle\varphi\rangle} \subsetneq L$ as $\varphi(\zeta) \neq \zeta$, we have that $[L^{\langle\varphi\rangle} : \mathbb{Q}] < 4$, so $\mathbb{Q}(i) = L^{\langle\varphi\rangle}$.

From $\zeta^{-1} = \frac{1-i}{\sqrt{2}}$ we obtain $\zeta + \zeta^{-1} = \sqrt{2}$, which implies $\sigma(\sqrt{2}) = \sigma(\zeta) + \sigma(\zeta^{-1}) = \zeta^{-1} + \zeta = \sqrt{2}$. Hence $\mathbb{Q}(\sqrt{2}) \subset L^{\langle\sigma\rangle}$. Similarly as above, we can use a degree argument to conclude that $L^{\langle\sigma\rangle} = \mathbb{Q}(\sqrt{2})$.

From $\sigma\varphi(\zeta) = \zeta^{-5} = \zeta^3$ and $(\zeta^3)^3 = \zeta^9 = \zeta$, we obtain that $\sigma\varphi$ interchanges the two zeros ζ and ζ^3. Hence $\zeta + \zeta^3$ is invariant under $\sigma\varphi$. From $\zeta^3 = \frac{-1+i}{\sqrt{2}}$ we obtain that $\zeta + \zeta^3 = i\sqrt{2}$, so that $\mathbb{Q}(i\sqrt{2}) \subseteq L^{\langle\sigma\varphi\rangle} \subsetneq L$. Note that $[\mathbb{Q}(i\sqrt{2}) : \mathbb{Q}] = 2$, so a similar degree argument as above implies that $L^{\langle\sigma\varphi\rangle} = \mathbb{Q}(i\sqrt{2})$.

Overall, this results in the following list of subgroups of G and their corresponding intermediate fields: