

Math323-Final Paper

Ahmet Kasım Erbay-2017205108

Proof of Q1:

We have that E is finite extension over K . This gives us there are finitely many intermediate fields F_i 's exist, since the intermediate fields are in one to one correspondence with the subrings of the galois extension, E/K such that $K \subseteq F_i \subseteq E$. Also E is seperable since all the given $\epsilon_i \in E$ are seperable.

Hence by the Primitive Element Theorem such α exists.

Proof of Q2:

(i)

Let E/K be a finite extension and G be the group of all K -automorphisms of E . Also let K' be the fixed field of G . Then, $K \subseteq K' \subseteq E$ and $|G| = [E : K]$. We have the followings,

- E/K is finite $\implies E/K'$ is finite.
- E/K is seperable and normal. $\implies E/K'$ is seperable and normal.

Therefore, there are exactly $n = [E : K']$ K automorphisms. Since we have $K' = K$. K is the fixed field of G . Hence E/K is Galois.

(ii) Could not prove.

(iii)

Let L be a minimal splitting field of $P(x)$ over E . Then $L = K(\text{zeros of } f \text{ in an extenson of } E) = K(\alpha_1, \alpha_2, \dots, \alpha_n, \text{ zeros of } f \text{ other than } \alpha_i \text{'s in an extension of } E) \implies K \subseteq E \subseteq L, \text{ thus } p_i \in K[x] \implies L/K \text{ is seperable. Thus } E = \text{Split}_K(p(x)) \text{ of seperable polynomial } p(x) \in K[x] \text{ over } K.$

Proof of Q3:

We have the chain of field extensions $K \subseteq F \subseteq E$. Assume E/K is finite Galois extension. Then E/F is already a finite extension. It is also a normal extension since E/K is algebraic extension.

I could not prove the seperability of E/F . If this is the case.

We have E/F is finite, normal and separable, which is Galois.

Proof of Q4:

(1) Let $f_1, f_2 \in \text{Aut}(E/K) \implies f_1(k) = k$ and $f_2(k) = k \forall k \in K$.

$f_1 \circ f_2$ is isomorphism of E and $f_1 \circ f_2(k) = f_1(f_2(k)) = k \implies f_1 \circ f_2 \in \text{Aut}(E/K)$.

(2) Let $f_1 \in \text{Aut}(E/K) \implies f_1$ is isomorphism and $f_1(k) = k \forall k \in K$
 $\implies f_1^{-1}$ is isomorphism and $f_1^{-1}(k) = k, \forall k \in K. \implies f_1^{-1} \in \text{Aut}(E/K)$.

(3) The identity isomorphism $I : E \rightarrow E$, defined as $I(k) = k, \forall k \in K$.

(4) The associativity is trivial.

Hence $\text{Aut}(E/K)$ is a group under composition of functions.

Proof of Q6:

(i)

For any $\alpha \in E$, we have that $m_{\alpha,F}(x) | m_{\alpha,K}(x)$. Hence all the zeros of $m_{\alpha,F}(x)$ are in E and all of them are distinct. Hence E/K is a normal separable extension
 $\implies E/F$ is Galois.

We have,

$$(j \circ i)(F) = j_{E/F}(\text{Gal}(E/F)) = F,$$

and

$$(i \circ j)(H) = \text{Gal}(E/j_{E/F}(H)) = H,$$

This proves that i and j are inverses of each other.

(ii)

By the primitive element theorem, we can write $L = K[\alpha]$. Let $f(X) \in K[X]$ be the minimal polynomial of α over K . Then, we have $\deg(f) = d$. Therefore, the splitting field E over L of f is of degree at most $d!$ over K . Therefore, $G = \text{Gal}(E/K) = [E : K] \leq d!$ So, G has at most $2^{d!}$ subsets, and therefore, at most $2^{d!}$ subgroups. By the fundamental theorem of Galois theory, this means that there are at most $2^{d!}$ intermediate fields. So there are finitely many fields.

(iii)

proof: Let's prove this by induction on $[E:K]$, it is clearly holds for $E=K$. Assume the result holds for extensions of smaller degree than $n=[E:K]$. Let $\alpha \in E/K$ and $f(x)$ be the minimal polynomial of degree m . Then $[K(\alpha):K]=m \implies [E:K(\alpha)]=n/m$. Also, since K is a Galois extension of $K(\alpha)$, we have $|\text{Aut}(E/K)|=n/m$.

Now $\text{Aut}(E/K)$ acts on the set σ , where σ denotes the roots of $f(x)$ in E since the coefficients of the polynomial lies in K .

The stabiliser of α fixes every element of $K(\alpha)$, and so is the Galois group of E over $K(\alpha)$. By induction, $|\text{Aut}(E/K)_\alpha| = n/m$.

Also we have the roots of f are all distinct and lie in E since $\text{Aut}(E/K)$ is Galois $|\sigma|=m$. By the Orbit–Stabiliser Theorem 7.2 (Cameron), we have,

$$|\text{Aut}(E : K)| = |\sigma| \cdot |\text{Aut}(E : K)_\alpha| = m \cdot (n/m) = n,$$

and that finalize the proof.

Note: I am so sorry that this is my all attention for this term. It was really hard to be focused at home. Also the materials are fully computer based(pdf's, exams, books etc.) which was hard to work on on a daily basis. Thanks for all your effort to make the lecture more easier for everyone. I hope things will be better for future semesters.