Field Exercise

Wednesday, March 21, 2018 3:15 PM

2. Let L be an extension of a field K. Prove that if $a \in L$ is nonzero, then a is algebraic over K if and only if there exists a nonzero $f(x) \in K[x]$ such that $f(a) = a^{-1}$

($\Leftarrow$): Suppose $\exists f(x)$ s.t. $f(a) = a^{-1}$. Then $g(x) = f(x) - a^{-1}$

$g(a) = f(a) - a^{-1} = 0 \Rightarrow a$ is algebraic over K.

($\Rightarrow$): Suppose a is algebraic over K, then $\exists g(x)$ s.t. $g(a) = 0$

Then $f(x) = g(x) + a^{-1}$

$\Rightarrow f(a) = g(a) + a^{-1} = a^{-1}$

---

3. Prove or disprove that $x^4 - 21x + b$ is irreducible over $\mathbb{Q}(\sqrt[3]{5})$.

pf: $x^4 - 21x + b$, then let $p(x) = (x - a)$

Then $a \in \mathbb{Q}(\sqrt[3]{5})$

Then $(\frac{p}{q})^4 + 21(\frac{p}{q}) + b = 0$

$p^4 + 21pq^3 + bq^4 = 0$

$\Rightarrow q \mid p$

$\Rightarrow (\frac{p}{q}) \in \mathbb{Z}$

$x^4 - 21x + b$ is irreducible by Eisenstein's Criterion

primitive, $21, b \in (3)$, $b \notin (9)$

Then if $p(x) = (x^2 + ax + b)$

Then $q(x) = x^2 + cx + d$

$(x^2 + ax + b)(x^2 + cx + d)$

$= x^4 + ax^3 + bx^2 + cx^3 + acx^2 + bcx + dx^2 + adx + bd$

$= x^4 + (a+c)x^3 + (b + ac + d)x^2 + (bc + ad)x + bd$

$\Rightarrow a + c = 0$

$b + ac + d = 0$

$bc + ad = -21$

$bd = 6$

$b - a^2 + d = 0$

$b + d = a^2$

$a(d - b) = -21$

$a(b - d) = 21$

$bd = 6$

$(b+d)(b-d)^2 = 21^2$

$bd = 6$

$b + d = a^2$

$b - d = \frac{21}{a}$

$\Rightarrow b = \frac{\frac{21}{a} + a^2}{2}$

$d = \frac{a^2 - \frac{21}{a}}{2}$

$(a^2 - \frac{21}{a})(a^2 + \frac{21}{a}) = 24$

$(a^3 - 21)(a^3 + 21) = 24a^2$

$a^6 - 24a^2 - 441 = 0$

---

4. Let L be an algebraic extension of a field K. Let $f(x) \in L[x]$ be nonconstant. Let M be a splitting field of $f(x)$ over L. Write $f(x) = \beta(x - a_1) \cdots (x - a_n)$, $\beta \in L^\times$, $a_1, \ldots, a_n \in M$.

a) Prove that a_j is algebraic over K for $1 \le j \le n$. (Notice: it may be the case that $[L : K] = \infty$)

b) Prove that there exists a nonzero $g(x) \in L[x]$ such that $f \circ g \in K[x]$. (Hint: One approach is to work in the ring $M[x]$ and then reduce to $L[x]$).

a) pf: We want to show $\exists g(x) \in K[x]$ s.t. $g(a_i) = 0$ (Notice a_i may not in K)

$M = L(a_1, \ldots, a_n)$ By definition of splitting field and definition of $L(a_1, \ldots, a_n)$

Consider $f(x) = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_0$

Since $f(x) \in L[x]$

$\Rightarrow b_i \in L$

$\Rightarrow b_i$ is algebraic over k (By L is algebraic extension over K)

$\Rightarrow [K(b_0, b_1, b_2, \ldots, b_n) : K] < \infty$

Now, Consider $K(b_0, b_1, \ldots, b_n)(a_1, \ldots, a_n)$

This is a splitting field of $f(x)$ over $K(b_0, \ldots, b_n)$

Then since $f(x) \in K(b_0, b_1, \ldots, b_n)[x]$

and $f(a_i) = 0$, $m_{K(b_0, \ldots, b_n), a_i(x)} \mid f(x)$

$\Rightarrow [K(b_0, b_1, \ldots, b_n)(a_1) : K(b_0, \ldots, b_n)] < n$

$\Rightarrow [K(b_0, b_1, \ldots, b_n)(a_1, a_2) : K(b_0, \ldots, b_n)(a_1)] < n$

$\Rightarrow [K(b_0, b_1, \ldots, b_n)(a_1, \ldots, a_n) : K(b_0 \cdots b_n)] < \infty$

$\Rightarrow [K(b_0, \ldots, b_n)(a_1, \ldots, a_n) : K] < \infty$

By $K(a_i) \subseteq K(b_0, \ldots, b_n)(a_1, \ldots, a_n)$

$\Rightarrow [K(a_i) : K] < \infty$

$\Rightarrow a_i$ is algebraic over K.

b) Prove that there exists a nonzero $g(x) \in L[x]$ such that $f(x)g(x) \in K[x]$. (Hint: One approach is to work in the ring $M[x]$ and then reduce to $L[x]$.)

pf: $f(x) \in L[x]$, first let's show $\exists\, g(x) \in M[x]$ s.t. $f(x)g(x) \in K[x]$

$M = L(a_1, \cdots, a_n)$

$f(x) = p(x-a_1)\cdots(x-a_n)$

a_i is algebraic over K

$\Rightarrow \exists\, h_i(x) \in K[x]$ s.t. $h_i(a_i) = 0$

Also, $h_i(x) \in K[x] \subseteq L[x]$

Then let $f(x) = f_1(x)f_2(x)\cdots f_L(x)$ s.t. $f_j(x)$ is irreducible in $L[x]$

Then by U.F.D., $\forall f_j(x), \exists a_j$ s.t. $f_j(a_j) = 0$

And $f_j(x)$ is irreducible in $L[x]$ + $f_j(a_j) = 0$ and $h_j(a_j) = 0$ for same a_j

$\Rightarrow f_j(x) \mid h_i(x)$ in $L[x]$

$\Rightarrow \exists\, g_j(x) \in L[x]$ s.t. $f_j(x)g_j(x) = h_j(x)$

$\Rightarrow f_1(x)g_1(x)\cdots f_L(x)g_L(x) = \underbrace{h_1(x)\cdots h_L(x)}_{\in K[x]}$

$\underbrace{f_1(x)\cdots f_L(x)}_{=f(x)}\ \underbrace{g_1(x)\cdots g_L(x)}_{=g(x)\in L}$

$\Rightarrow \exists\, g(x) \in L$ s.t. $f(x)g(x) \in K[x]$

Method 2: Write $f(x) = \prod_{\text{for some } i} m_{a_i,L}(x)$ (it is possible that $m_{a_i,L}(x) = m_{a_j,L}(x)$, this one only multiply once)

By $f(a_i) = 0$

$\Rightarrow m_{a_i,L}(x)q(x) = f(x)$ where $q(x) \in L[x]$

Then since we know $f(x)$ splits $\Rightarrow q(x)$ splits $\Rightarrow$ keep doing $\cdots$

Until we done

$\Rightarrow f(x) = \prod_{\text{for some } i} m_{a_i,L}(x)$

$m_{a_i,L}(x) \mid h_i(x)$ By $K \subseteq L$

$\Rightarrow h_i(x) \in K[x] \subseteq L[x]$

$\Rightarrow \exists\, g(x) \in L[x]$ $\cdots$

(You can see that it is the same proof almost, except $\cdots$)

---

6. (Skip 5, check assignment) Let $L \subseteq \mathbb{C}$ be a splitting field of an irreducible polynomial $f(x) \in \mathbb{Q}[x]$. Suppose that $f(x)$ has at least one real root and at least one nonreal root (deg ≥ 3). Prove that $|\mathrm{Aut}(L/\mathbb{Q})|$ is even and $\mathrm{Aut}(L/\mathbb{Q})$ is nonabelian. (Hint: Complex conjugation is useful here.)

pf: L is a splitting field of a irreducible polynomial $f(x) \in \mathbb{Q}[x]$

Suppose $\deg f(x) = 3$

Then $L = \mathbb{Q}(a_1, a_2, \overline{a_2})$

Some attempt, solution is below

$[\mathbb{Q}(a) : \mathbb{Q}] = 3$

By irreducible $f(x)$ and $\deg f(x) = 3$

$\mathbb{Q}(a_2, \overline{a_2}) = \mathbb{Q}(a_2)$ by $a_2 \in \mathbb{Q}(a_2)$

$\Rightarrow a_2 = a+bi$

$\Rightarrow \frac{1}{a_2} = \frac{a-bi}{a^2+b^2}$

$\Rightarrow \overline{a_2} \in \mathbb{Q}(a_2)$

Then we need to show that $[\mathbb{Q}(a_1, a_2) : \mathbb{Q}(a_1)] = 2$

By $\deg f(x) = 3$ and $f(a_2) = 0$

Consider $f(x) = (x-a_1)f_1(x) + r_1(x)$

By assumption $\deg r_1(x) < \deg(x-a_1)$

$\Rightarrow r_1(x)$ is constant

$f(a_1) = 0 \Rightarrow r_1(x) = 0$

$\Rightarrow f(x) = (x-a_1)f_1(x)$

Then since $f_1(x) = (x-a_2)(x-\overline{a_2})$

$\Rightarrow$ if $[\mathbb{Q}(a_1, a_2) : \mathbb{Q}(a_1)] = 1$

$\Rightarrow x - a_2 \in \mathbb{Q}(a_1)$

$\Rightarrow a_2 \in \mathbb{Q}(a_1)$

Since a_2 is nonreal

Contradict

$\Rightarrow [\mathbb{Q}(a_1, a_2) : \mathbb{Q}(a_1)] = 2$

$x^3 - 2$

$x_1 = 2^{\frac{1}{3}}$

$x_2 = 2^{\frac{1}{3}}e^{\frac{2\pi}{3}i} = 2^{\frac{1}{3}}(\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3})$

$= 2^{\frac{1}{3}}(\frac{\sqrt{3}}{2} + \frac{1}{2}i)$

$x_3 = 2^{\frac{1}{3}}e^{\frac{3\pi}{3}i} = 2^{\frac{1}{3}}$

Solution is here:

Generally, Since $f(x)$ has at least one nonreal root $\Rightarrow$ $\deg f(x)$ can be odd,

Since $f(x)$ has at least one nonreal root $\Rightarrow$ $i \in L$ (By $a+bi \in L \Rightarrow a-bi \in L \Rightarrow 2bi \in L \Rightarrow i \in L$)

$a_i \in L$

Generally, Since $f(x)$ has at least one nonreal root $\Rightarrow$ deg $f(x)$ can be odd,

Since $f(x)$ has at least one nonreal root $\Rightarrow$ $i \in L$ (By $a+bi \in L \Rightarrow a-bi \in L \Rightarrow 2bi \in L \Rightarrow i \in L$)

$Q(i) \subseteq L$

$\Rightarrow$ Consider $[L:Q] = [L:Q(i)][Q(i):Q]$

$\Rightarrow$ $[L:Q]$ is even

$\Rightarrow$ $|Aut(L/Q)|$ is even by L is Galois over Q

To show $Aut(L/Q)$ is nonabelian, first choose conjugate σ s.t. $\sigma(i) = -i$

Then since f has at least one nonreal root

By simple extension Lemma, $i: Q \to Q$

$f(x)$ is the irreducible polynomial

$\exists \tau$ s.t. $\tau \in Aut(L/Q)$

and $\tau(\alpha) = \beta$

α is real root of $f(x)$

β is nonreal ------

$\Rightarrow$ $\tau\sigma(\alpha) = \tau(\alpha) = \beta$

$\sigma\tau(\alpha) = \sigma(\beta) = \bar{\beta}$

$\beta \neq \bar{\beta}$ by β is nonreal

$\Rightarrow$ Nonabelian

---

7. Let L be an algebraic extension of a field K, let F be an algebraically closed field (that is, a field having the property that every element of $F[x]$ splits over F). Let $i: K \to F$ be a nonzero homomorphism. Prove that i extends to a homomorphism $j: L \to F$. In addition show that, given $\alpha \in L$, if $\beta \in F$ is a root of $i(m_{\alpha,K})(x)$, then there exists an extension j with that $j(\alpha) = \beta$. (Hint: for $f(x) \in K[x]$, $i(f)(x) \in F[x]$ is obtained by applying i to the coefficients of $f(x)$.)

(Hint: Use Zorn's Lemma).

Pf: (The reason we need Zorn's Lemma is that L might not be a finite extension)

Definition: A finite extension L of a field K is said to be normal over K (or a normal extension of K) if L is the splitting field of some $f(x) \in K[x]$ over K.

8. Let $L \subseteq R$ be a finite normal extension of Q. Prove that if p is prime and $\ell \neq 3$, then $\sqrt[\ell]{p} \notin L$

Pf: We need L be finite, normal extension of R.

$L = Q(\alpha_1, \dots, \alpha_n)$

And L is normal over Q

L is the splitting field of some $f(x)$ over Q

$f(x) \in Q[x]$

If $\sqrt[\ell]{p} \in L$,

$m_{\sqrt[\ell]{p}, Q}(x) = x^\ell - p$

Then by splitting Lemma, we will have $m_{\sqrt[\ell]{p}, Q}(x)$ splits in L

$\Rightarrow$ We will get some complex number $\in L$

Which contradict that L is a subfield of R.

---

9. Let L be a finite normal extension of field K.

a) Let $g(x) \in K[x]$ be irreducible and monic. Prove that if $g(x) = \prod_{j=1}^{m} g_j(x)$ where each $g_j(x) \in L[x]$ is irreducible and monic, then the group $Aut(L/K)$ permutes the $g_j(x)$'s transitively. (Hint: Think about the proof of the Splitting Theorem)

b) Prove that if α belongs to a finite extension of L. Then $[L(\alpha):L]$ divides $[K(\alpha):K]$.

c) Find an example showing that a) and b) can fail when L is not normal over K.

a) Pf: $g(x)$ is irreducible and monic in $K[x]$

Then let $L(\alpha_1, \alpha_2, \dots, \alpha_n)$ be the splitting field of $g(x)$ over L (α_i is the root of $g(x)$)

Special Case: Now, Suppose $\alpha_i \in L$, by splitting theorem, $g(x)$ is irreducible in $K[x]$, $g(\alpha_i) = 0$, $\alpha_i \in L$

$\Rightarrow$ $g(x)$ splits in L

$K \subseteq L \subseteq L(\alpha_1, \dots, \alpha_n)$

$g(x)$ is irreducible over K, $g(x) \in K[x]$

$\Rightarrow$ $\forall \alpha_i, \alpha_j$, since by assumption, $g(\alpha_i) = g(\alpha_j) = 0$

$\exists j: K(\alpha_i) \to K(\alpha_j)$

s.t. $j|_K = id$ and $j(\alpha_i) = \alpha_j$

$L(\alpha_i)$ is a splitting field of $f(x)$ over $K(\alpha_i)$

$L(\alpha_j)$ is a splitting field of $f(x)$ over $K(\alpha_j)$

$\Rightarrow$ $\exists j': L(\alpha_i) \to L(\alpha_j)$ s.t.

s.t. $j|_K = id$ and $j(\alpha_i) = \alpha_j$

$L(\alpha_i)$ is a splitting field of $f(x)$ over $K(\alpha_i)$

$L(\alpha_j)$ is a splitting field of $f(x)$ over $K(\alpha_j)$

$\Rightarrow \exists\ j' : L(\alpha_i) \to L(\alpha_j)$ s.t.

$j'|_{K(\alpha_i)} = j \Rightarrow j'|_K = id$ and $j'(\alpha_i) = \alpha_j$

We need to show $j'|_L \in Aut(L/K)$

By $j'(\alpha_i) = \alpha_j$

and $j'(\alpha_i) \in L$ iff $\alpha_j \in L$

$\Rightarrow j'|_L \in Aut(L/K)$ (This is not complete, we only show $j'(L(\alpha_i)) \setminus L) \cap L = \emptyset$

We still need to show $j'(L) \subseteq L$ and They have the same degree
So we can show they are equal

True Solution: Consider $K(\alpha_i)$, $K(\alpha_j)$, $L(\alpha_i)$, $L(\alpha_j)$

Consider $i : K \to K$, $g(x)$ is irreducible and $g(\alpha_i) = g(\alpha_j) = 0$

$\Rightarrow g(x) = m_{\alpha_i,K}(x) = m_{\alpha_j,K}(x)$

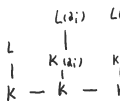
Also, $g(x) \in K[x]$

$\Rightarrow i(g)(x) = g(x)$

Therefore $\exists\ j : K(\alpha_i) \to K(\alpha_j)$

s.t. $j(\alpha_i) = \alpha_j$

And $j|_K = i$



Then $L(\alpha_i)$ is a splitting field of some $f(x)$ over $K(\alpha_i)$ $f(x) \in K[x]$

$L(\alpha_j)$ is a splitting field of some $f(x)$ over $K(\alpha_j)$

And $j : K(\alpha_i) \to K(\alpha_j)$ is a homophism

Then $\exists\ j' : L(\alpha_i) \to L(\alpha_j)$ s.t. $j'|_{K(\alpha_i)} = j$ and $j'|_K = i|_K = i$

Wrong proof, can't show all elements in $Aut(L/K)$ permutes $g_i(x)$ and $g_j(x)$

$\Rightarrow j'(\alpha_i) = \alpha_j \Rightarrow j'(\alpha_i) \in L$ iff $\alpha_j \in L$

$\Rightarrow j'|_L \in Aut(L/K)$

This proof only shows $\forall\ g_i(x), g_j(x)$

$\exists\ \sigma \in Aut(L/K)$ s.t.

$\sigma(g_i(x)) = g_j(x)$

But it doesn't show

$\forall\ \sigma \in Aut(L/K)$, ----

(So I think this proof is either incorrect or need to be justified)

Then consider $m_{\alpha_i,L}(x)$

$j'(m_{\alpha_i,L})(x)$ is irreducible

and $j'(m_{\alpha_i,L})(\alpha_j) = 0$

$\Rightarrow j'(m_{\alpha_i,L})(x) = m_{\alpha_j,L}(x)$

Some mind polynomial are unique, and $g_i(x)$ are monic irreducible in $L[x]$

$\Rightarrow$ Let $m_{\alpha_i,L}(x) = g_i(x) \in L$

$m_{\alpha_j,L}(x) = g_j(x) \in L$

$\Rightarrow j'|_L(g_i(x)) = g_j(x)$

Can we show $\forall\ \sigma \in Aut(L/K)$, σ extends to some homophism to $L(\alpha_i)$ and $L(\alpha_j)$? (Finally, we come back to the original idea)

So, we need a Larger field M such that $g(x)$ splits in M

Notice, don't say M is a splitting field of $g(x)$ over L (We cannot show in this case M is normal over K)

Don't choose M is a splitting field of $g(x)$ over K (This case cannot show $M \supseteq L$)

Let's choose M is a splitting field of $f(x)g(x)$ over $K \Rightarrow M \supseteq L \supseteq K$

And Since M is normal over K

One can show that $\forall\ \alpha, \beta$, s.t. $g(\alpha) = g(\beta) = 0$ and

some $g(x)$ is irreducible in $K[x]$

$\exists\ \sigma \in Aut(M/K)$ s.t. $\sigma(\alpha) = \beta$ (By splitting Theorem)

And one can also show $\sigma(L) = L \Rightarrow \sigma|_L \in Aut(L/K)$

By L is normal over K and if

$\gamma \in L$, since $[L:K] < \infty$

$\Rightarrow \gamma$ is algebraic over K

Don't read purple part, useless

$|Aut(L(\alpha)/K)| \leq [L(\alpha):L][L:K]$

By L is normal over K, $[\text{homophism } i \mid i : L \to L(\alpha)] \in Aut(L/K)$

Notice: Don't confuse with $Aut(L(\alpha)/K)$ and $\{j|_L \mid j : L(\alpha) \to L(\beta), j \text{ is homophism}\}$

The latter one $j|_L \notin Aut(L/K)$

For the former one, consider $Aut(L(\alpha)/K)|_L$,

Since $Aut(L(\alpha)/K)|_L = Aut(L/K)$

$\Rightarrow \sigma \in Aut(L(\alpha)/K)$ s.t.

$\sigma|_L(m_{\alpha,L})(x) = m_{\beta,L}(x)$

$\Rightarrow \sigma(m_{\alpha,L})(x) = m_{\beta,L}(x)$

$\Rightarrow \sigma(\alpha)$ is a root of $m_{\beta,L}(x)$

consider $m_{\gamma,K}(x)$,

$\sigma(m_{\gamma,K})(\sigma(\gamma)) = 0$

And $\sigma(m_{\gamma,K})(x) = m_{\gamma,K}(x)$

$\Rightarrow \sigma(\gamma)$ is a root of $m_{\gamma,K}(x)$

And by L is normal over $K \Rightarrow m_{\gamma,K}(x)$ splits in L

$\Rightarrow \sigma(\gamma) \in L$

Therefore, $\sigma(L) \subseteq L$

And σ is isomorphism from $M \to M$ fix K

$[L:K] = [\sigma(L):\sigma(K)] = [\sigma(L):K]$

$\Rightarrow \sigma(L) = L$

$\sigma \in Aut(L(\alpha)/K)$

$\sigma|_L \in Aut(L/K) \Rightarrow \sigma|_L \in Aut(L/K)$

Also, By the proof from Galois and intuitively (Notice L is normal over K)

we can see that $Aut(M/K)|_L = Aut(L/K)$

$\sigma|_L(m_{\alpha,L}(x)) = m_{\beta,L}(x)$

$\Rightarrow \sigma(m_{\alpha,L})(x) = m_{\beta,L}(x)$

$\Rightarrow \sigma(\alpha)$ is a root of $m_{\beta,L}(x)$

$\Rightarrow \sigma(\alpha) = \beta$

$\Rightarrow \beta \in L(\alpha)$

$\Rightarrow Aut(L(\alpha)/K)|_L \neq Aut(L/K)$ if $L(\alpha) \neq L(\beta)$

Also, By the proof from Galois and intuitively (Notice L is normal over K)

we can see that $Aut(M/K)|_L = Aut(L/K)$

Now, since $\sigma(\alpha) = \beta$, consider

$m_{\alpha,L}(x)$, $\sigma(m_{\alpha,L})(\sigma(\alpha)) = 0$

And $\sigma(m_{\alpha,L})(x)$ is irreducible and monic

implies $\sigma(m_{\alpha,L})(x) = m_{\beta,L}(x)$

And $g_\alpha(x)$ and $g_\beta(x)$ are also

monic and irreducible in $L[x]$

$\Rightarrow$ $g_\alpha(x) = m_{\alpha,L}(x)$

$g_\beta(x) = m_{\beta,L}(x)$

$\Rightarrow \sigma(g_\alpha(x)) = g_\beta(x)$

However, when we do

$|Aut(L(\alpha)/K)|$

Why we say it $\leq [L(\alpha):L][L:K]$

And Suppose L is Galois over K

Did we just do

$|Aut(L(\alpha)/K)| = \#$ distinct roots of $m_{\alpha,L}(x)$ in $K(\alpha) \cdot [L:K]$

If this is the case, doesn't this imply $Aut(L(\alpha)/K)|_L = Aut(L/K)$? (X) This is not true, from the proposition we could just find the upper bound but not usually the actual value.

To show: $Aut(L(\alpha)/K)|_L \subseteq Aut(L/K)$

$\forall \sigma \in Aut(L(\alpha)/K)|_L$

We want to show $\sigma(L) = L$

By the $\gamma \in L$, and γ is algebraic over K

$\Rightarrow m_{\gamma,K}(x)$ exists, and By splitting theorem

$\Rightarrow m_{\gamma,K}(x)$ splits in L

Also, by $m_{\gamma,K}(x) \in K[x]$

$\Rightarrow \sigma(m_{\gamma,K})(x) = m_{\gamma,K}(x)$

$\Rightarrow$ $\sigma(\gamma)$ is a root of $m_{\gamma,K}(x)$

$\Rightarrow \sigma(\gamma) \in L$

$\Rightarrow \sigma(L) \subseteq L$

$|Aut(L(\alpha)/K)| = \#\{i : L(\alpha) \to L(\alpha)$ s.t. $i|_L = i$ where $i: L \to L\}$

$\cdot \#\{i : L \to L$ s.t. $i|_K = id\}$ $\longrightarrow$ equal $[L:K]$ X

$= \#$ distinct roots of $m_{\alpha,L}(x)$ in $L(\alpha) \cdot [L:K]$?

$\Rightarrow |Aut(L(\alpha)/K)|_L| = [L:K] = |Aut(L/K)|$ X

$\Rightarrow Aut(L(\alpha)/K)|_L = Aut(L/K)$ Contradict! So either we screw up when guessing $L(\alpha) \neq L(\beta)$ Or we screwed up when calculating $|Aut(L(\alpha)/K)|$

Now, let's take an example: Consider $L = Q(i)$, $g(x) = x^6 + 1$, $g(x)$ is irreducible in $Q[x]$

$g(x) = (x^3 + i)(x^3 - i)$ in $L[x]$

Now, the solution: $g(x) = (x^3 + e^{\frac{\pi i}{2}})(x^3 - e^{\frac{\pi i}{2}})$

$\Rightarrow x^3 + e^{\frac{\pi i}{2}} = 0$

$x^3 = -e^{\frac{\pi i}{2}}$

$= e^{-\frac{\pi i}{2}}$

$x = e^{-\frac{\pi i}{6}}, e^{\frac{3\pi i}{6}}, e^{\frac{7\pi i}{6}}$

$x^3 - e^{\frac{\pi i}{2}} = 0$

$x^3 = e^{\frac{\pi i}{2}}$

$x = e^{\frac{\pi i}{6}}, e^{\frac{5\pi i}{6}}, e^{\frac{9\pi i}{6}}$

$x = e^{\frac{\pi i}{6}}, e^{\frac{3\pi i}{6}}, e^{\frac{5\pi i}{6}}, e^{\frac{7\pi i}{6}}, e^{\frac{9\pi i}{6}}, e^{\frac{11\pi i}{6}}$

Suppose L' is the splitting field of $g(x)$ over K

$\Rightarrow L' = Q(e^{\frac{\pi i}{6}})$

Consider $Aut(Q(e^{\frac{\pi i}{6}})/Q)$

$\exists \sigma$ s.t. $\sigma(e^{\frac{\pi i}{6}}) = e^{\frac{2\pi i}{6}}$

$\Rightarrow \sigma(e^{\frac{3\pi i}{6}}) = \sigma(e^{\frac{\pi i}{6}})^3$

$= (e^{\frac{3\pi i}{6}})^3$

$= e^{\frac{9\pi i}{6}} = e^{\frac{3\pi i}{2}} = -i$

$\Rightarrow \sigma(i) = -i \in Q(i)$

$Aut(Q(e^{\frac{\pi i}{6}})/Q)|_{Q(i)} = Aut(Q(i)/Q)$

True, because we have $L(\alpha) = L(\beta)$

So we don't have the problem.

General Version of this question:

Suppose α is the root of $g_1(x)$ and β is the root of $g_2(x)$ and $L(\alpha) \neq L(\beta)$ (i.e. $\beta \notin L(\alpha)$)

Then let's consider $Aut(L(\alpha)/K)|_L \subseteq Aut(L/K)$

If $Aut(L(\alpha)/K)|_L = Aut(L/K)$

$\Rightarrow \exists \sigma \in Aut(L(\alpha)/K)$ s.t. $\sigma|_L(m_{\alpha,L})(x) = m_{\beta,L}(x)$

By the conclusion from Q9. a) ($Aut(L/K)$ permutes $g_i(x)$ transitively)

$m_{\alpha,L}(\alpha) = 0$

$\Rightarrow \sigma|_L(m_{\alpha,L})(\sigma(\alpha)) = 0$

$\Rightarrow m_{\beta,L}(\sigma(\alpha)) = 0$

$\Rightarrow \sigma(\alpha) = \beta$, however, $\beta \notin L(\alpha)$ By assumption

$\Rightarrow Aut(L(\alpha)/K)|_L \neq Aut(L/K)$

Now, change to another way to think of this question, forget the conclusion from above:

Notice $Aut(L(\alpha)/K)|_L : L \to L$

Thus $|Aut(L(\alpha)/K)| = \#\{$homomorphism $j: L(\alpha) \to L(\alpha)$ s.t. $j|_L = i$ where i is homomorphism $L \to L\}$

$\cdot \#\{$homomorphism $i: L \to L$ s.t. $i|_K =$ identity $\}$

Now, we can show that $|Aut(L(\alpha)/K)|_L| = \#\{$homomorphism $i: L \to L$ s.t. $i|_K =$ identity $\}$

Now, what is the $\{$homomorphism $i: L \to L$ s.t. $i|_K =$ identity $\}$?

Is this equal to $Aut(L/K)$?

If yes, this will be a contradiction,

If no, this will be no contradiction.

Now, consider $Q(\sqrt{2}) = L$, $Q(2^{\frac{1}{4}})$ or $L(2^{\frac{1}{4}})$, also, $Q(\sqrt{2})$ is normal over Q

Also $x^4 - 2 = (x^2 - \sqrt{2})(x^2 + \sqrt{2})$ in $L[x]$

Now, let's talk about $L(2^{\frac{1}{4}})$ and $Aut(L(2^{\frac{1}{4}})/Q) = Aut(Q(2^{\frac{1}{4}})/Q)$

By this example, one can see that $|Aut(L(\alpha)/K)| = \#\{j: L(\alpha) \to L(\alpha)$ s.t. $j|_L = i$ when $i: L \to L\}$

$\cdot \#\{i: L \to L$ s.t. $i|_K =$ identity $\}$

✡✡ This formula is incorrect.

$|Aut(Q(2^{\frac{1}{4}})/Q)| = 2$ By $Q(2^{\frac{1}{4}}) = 2^{\frac{1}{4}}$ or $Q(2^{\frac{1}{4}}) = -2^{\frac{1}{4}}$

$j: Q(\sqrt[4]{2}) \to Q(\sqrt[4]{2})$ s.t. $j|_{Q(\sqrt{2})} = i$, $i: Q(\sqrt{2}) \to Q(\sqrt{2})$ s.t. $i|_Q =$ identity

$m_{2^{\frac{1}{4}}, Q(\sqrt{2})}(x) = x^2 - \sqrt{2}$

Number of such j is 2

Then consider $i: Q(\sqrt{2}) \to Q(\sqrt{2})$ s.t. $i|_Q =$ identity

number of such i is 2

$2 \times 2 = 4$

However $|Aut(Q(2^{\frac{1}{4}})/Q)| = 2 \neq 4$ As one can show

The problem is if we fix (let's say $\sigma(2^{\frac{1}{4}}) = 2^{\frac{1}{4}}$

Then $\Rightarrow \sigma(2^{\frac{1}{2}}) = 2^{\frac{1}{2}}$

Or $\sigma(2^{\frac{1}{4}}) = 2^{-\frac{1}{4}}$

$\Rightarrow \sigma(2^{\frac{1}{2}}) = 2^{\frac{1}{2}}$

Thus such i have only two !

---

b) Prove that if α belongs to a finite extension of L, then $[L(\alpha): L]$ divides $[K(\alpha): K]$

b) Prove that if α belongs to a finite extension of L, then $[L(\alpha):L]$ divides $[K(\alpha):K]$

Notice $[L(\alpha):L] = \deg g_1(x)$ by a)

$[K(\alpha):K] = \deg g(x)$

By conclusion from a), $Aut(L/K)$ permutes them transitively

$\Rightarrow \deg g_1(x) \mid \deg g(x)$

c) Find an example showing that a) and b) can fail when L is not normal over K

Consider $L = \mathbb{Q}(\sqrt[4]{3})$, it is not normal over K by 8.

$x^4 - 3 = (x - \sqrt[4]{3})(x^3 + \sqrt[4]{3}x^2 + \sqrt[2]{3}x + \sqrt[4]{3^3})$ in $\mathbb{Q}(\sqrt[4]{3})$

But there is no map $\sigma \in Aut(L/K)$ s.t.

$\sigma(x - \sqrt[4]{3}) = x^3 + \sqrt[4]{3}x^2 + \sqrt[2]{3}x + \sqrt[4]{3^3}$

The order is different

$[L(\alpha):L] = \cdots 3$

$[K(\alpha):K] = \cdots 4$

Definition: Let L be a finite extension of a field K. An extension M of L is a normal closure of L over K if M is normal over K and has the additional property that there is no proper subfield of M that is normal over K and contains L.

10. Let L be a finite extension of a field K.

a) Prove that there exists a normal closure of L over K.

Consider $L = K(\alpha_1, \cdots \alpha_n)$

Then choose M be the splitting field of $f(x) = m_{\alpha_1,K}(x) \cdots m_{\alpha_n,K}(x)$

$\Rightarrow M \supseteq L \supseteq K$

Now, we want to show such M is the closure of L

Suppose $\exists M'$ s.t. $K \subseteq L \subseteq M' \subsetneq M$

Since M' is normal over K

By Splitting theorem, $m_{\alpha_1,K}(x)$ splits in M' (by $\alpha_i \in L \subseteq M' \Rightarrow \cdots$)

$\vdots$

$m_{\alpha_n,K}(x)$ splits in M'

$\Rightarrow f(x)$ splits in M'

Contradict with M is the splitting field of $f(x)$ over K.

$\Rightarrow M$ is the normal closure of L over K. (Thanks to L is finite extension otherwise L have no idea)

b) Prove that any two normal closures of L over K are K-isomorphic (that is, there exists an isomorphism between two such closures that fixes K pointwise))

Suppose M' is a normal closure of L over K (from a)

Then we can see $f(x)$ splits in M'

Then if M' is not a splitting field of $f(x)$ over K

$\Rightarrow \exists M'' \subseteq M'$ s.t. M'' is a splitting field of $f(x)$ over K

and M'' by a) we can see that contains L

$\Rightarrow M'$ have to be a splitting field of $f(x)$ over K

Then let $i : K \to K$

and by M and M' are both splitting fields of $f(x)$ over $K \Rightarrow \exists$ isomorphism $j : M \to M'$ s.t. $j|_K = i$

c) Prove that if M is normal over K and $L \subseteq M$, then M contains a unique normal closure of L over K.

Pf: Suppose M is normal over K, consider if it contains to normal closure N and N'

N and $N' \supseteq L$ and $\exists$ isomorphism $i : N \to N'$ s.t. $i|_K$ = identity

By a), we can see that N and N' are both splitting field of $f(x) = m_{\alpha_1,K}(x) \cdots m_{\alpha_n,K}(x)$ over K

Then, $f(x) = (x - a_1^1)(x - a_1^2) \cdots (x - a_1^{m_1})(x - a_2^1) \cdots (x - a_2^{m_2}) \cdots \cdots (x - a_n^1) \cdots (x - a_n^{m_n})$ in N

$f(x) = (x - a_1^{1\prime}) \cdots (x - a_1^{m_1\prime}) \cdots \cdots (x - a_n^{1\prime}) \cdots (x - a_n^{m_n\prime})$ in N'

By N and N' both in M and M is a U.F.D

$\Rightarrow a_i^i = a_i^{i\prime} \Rightarrow N' = K(a_1^{1\prime}, \cdots a_1^{m_1\prime}, \cdots \cdots a_n^{1\prime}, \cdots a_n^{m_n\prime})$

$= K(a_1^1, \cdots \cdots a_n^{m_n}) = N$

---

11. Find the normal closure of $\mathbb{Q}(2^{\frac{1}{4}}, 5^{\frac{1}{3}})$ over $\mathbb{Q}$

By 10, we know normal close is the splitting field of $m_{2^{\frac{1}{4}},\mathbb{Q}}(x)\, m_{5^{\frac{1}{3}},\mathbb{Q}}(x)$

$= (x^4 - 2)(x^3 - 5)$

$\pm \sqrt[4]{2}e^{\frac{\pi i}{2}}, \sqrt[4]{2}e^{\pi i}, \sqrt[4]{2}e^{\frac{3\pi i}{2}},$

By 10, we know normal closure is the splitting field of $m_{2^{\frac{1}{4}},\mathbb{Q}}(x)\, m_{5^{\frac{1}{3}},\mathbb{Q}}(x)$

$= (x^4-2)(x^3-5)$

$2^{\frac{1}{4}},\ 2^{\frac{1}{4}}e^{\frac{\pi i}{2}},\ 2^{\frac{1}{4}}e^{\pi i},\ 2^{\frac{1}{4}}e^{\frac{3\pi i}{2}},$

$5^{\frac{1}{3}},\ 5^{\frac{1}{3}}e^{\frac{2\pi i}{3}},\ 5^{\frac{1}{3}}e^{\frac{4\pi i}{3}}$

$\Rightarrow \quad e^{\frac{\pi i}{2}} = i,\ e^{\frac{3\pi i}{2}} = -i$

$e^{\frac{2\pi i}{3}} = \left(-\frac{1}{2}+\frac{\sqrt{3}}{2}i\right),\ e^{\frac{4\pi i}{3}} = -\frac{1}{2}-\frac{\sqrt{3}}{2}i$

$\mathbb{Q}(2^{\frac{1}{4}}, 5^{\frac{1}{3}}, \sqrt{3}, i)$ is the splitting field of $f(x) = m_{2^{\frac{1}{4}},\mathbb{Q}}(x)\, m_{5^{\frac{1}{3}},\mathbb{Q}}(x)$ over $\mathbb{Q}$, $\Rightarrow \mathbb{Q}(2^{\frac{1}{4}}, 5^{\frac{1}{3}}, \sqrt{3}, i)$ is the normal closure of L over $\mathbb{Q}$

---

12. Let p be a prime and let $L \subseteq \mathbb{C}$ be a splitting field of x^p-2 over $\mathbb{Q}$. Prove that $\mathrm{Aut}(L/\mathbb{Q})$ is isomorphic to the group of matrices $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$, $a,b \in \mathbb{F}_p$, and $a \neq 0$, explain why L is a Galois extension of $\mathbb{Q}$

pf: Let L be a splitting field of x^p-2 over $\mathbb{Q}$.

$L = \mathbb{Q}(2^{\frac{1}{p}},\ 2^{\frac{1}{p}}e^{\frac{2\pi i}{p}},\ 2^{\frac{1}{p}}e^{\frac{4\pi i}{p}},\ \cdots\cdots\cdots\ 2^{\frac{1}{p}}e^{\frac{(2p-2)\pi i}{p}})$

L is Galois over $\mathbb{Q}$ by

L is normal over $\mathbb{Q}$ and

L is separable over $\mathbb{Q}$ by $\mathrm{char}(\mathbb{Q})=0$

$\Rightarrow L$ is Galois over $\mathbb{Q}$ by F.T.G.T.

$\Rightarrow L = \mathbb{Q}(2^{\frac{1}{p}}, e^{\frac{2\pi i}{p}})$

And By conclusion from cyclotomic extension

$\Rightarrow [\mathbb{Q}(e^{\frac{2\pi i}{p}}) : \mathbb{Q}] = \varphi(p) = p-1$

$[\mathbb{Q}(2^{\frac{1}{p}}, e^{\frac{2\pi i}{p}}) : \mathbb{Q}(e^{\frac{2\pi i}{p}})] = p$

$\Rightarrow |\mathrm{Aut}(L/\mathbb{Q})| = p(p-1)$ We can do this because L is Galois over $\mathbb{Q}$

$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a^2 & ab+b \\ 0 & 1 \end{pmatrix}$

$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a^2 & ab+b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a^3 & a^2b+ab+b \\ 0 & 1 \end{pmatrix}$

$\begin{pmatrix} a^4 & a^3b+a^2b+ab+b \\ 0 & 1 \end{pmatrix}$

$\begin{pmatrix} a^5 & a^4b+a^3b+a^2b+ab+b \\ 0 & 1 \end{pmatrix}$

Answer from Stacks Overflow:

Consider, let's call them $\sqrt[p]{2}, \sqrt[p]{2}\zeta, \sqrt[p]{2}\zeta^2, \cdots\cdots \sqrt[p]{2}\zeta^{p-1}$

Let $\varphi \in \mathrm{Aut}(L/\mathbb{Q})$

$\varphi(\zeta) = \zeta^a$ for one $1 \le a \le p-1$

(Notice all such ζ^a are primitive root by p is prime, also, since ζ is primitive a constant be 0 it's easy to show)

$\varphi(\sqrt[p]{2}) = \sqrt[p]{2}\zeta^b$ for one $1 \le b \le p-1$

Once can check that is a nice isomorphism

$\chi : G \to G' : \left\{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in \mathbb{F}_p^{\times},\ b \in \mathbb{F}_p\right\}$

And btw, more general version can change to x^p-q for one prime q.

---

13. Let K be a field of prime characteristic p. Prove that if α belongs to an extension of K and α is algebraic over K. Then α is separable over K if and only if $K(\alpha) = K(\alpha^p)$. (Hint: Remember that an element of $K(\alpha^p)$ is of the form $f(\alpha^p)$ for some $f \in K[x]$.)

pf: ($\Rightarrow$):

already have $K(\alpha^p) \subseteq K(\alpha)$, we also need $K(\alpha) \subseteq K(\alpha^p)$

$\mathrm{char}(K) = p$

$x^p - \alpha^p = (x-\alpha)^p$

If $\alpha \notin K(\alpha^p)$

$x^p-\alpha^p$ is irreducible in $K(\alpha^p)$

Otherwise, suppose it is reducible

By U.F.D of $K(\alpha)$, we will get

$x^p-\alpha^p = f(x)g(x) \Rightarrow f(x) = (x-\alpha)^r$, s.t. $r < p$

Then $\Rightarrow f(x) \in K(\alpha^p)$

$\Rightarrow \alpha^r \in K(\alpha^p)$

Then by Euclidean Algorithm

$(r,p)=1$, $\exists x,y$ s.t.

$\Rightarrow xp+yr=1$

$\Rightarrow (\alpha^p)^x \cdot (\alpha^r)^y = (\alpha)^{px+ry} = \alpha$

$\Rightarrow \alpha \in K(\alpha^p)$ contradict

Then $x^p-\alpha^r$ is irreducible in $K(\alpha^p)[x]$

Then consider the following: Since $x^p - \alpha^p = m_{\alpha, K(\alpha^p)}(x)$

$\Rightarrow x^p-\alpha^p \mid m_{\alpha,K}(x)$

$\Rightarrow (x-\alpha)^p \mid m_{\alpha,K}(x)$

(,) $m_{\alpha,K}(x)$ is reducible .

it is show $\alpha \in K(\alpha^p)$

$\alpha = f(\alpha^p)$ for one $f(x) \in K[x]$

$f(\alpha^p) - \alpha = 0$

$\Rightarrow f(x^p) - x = 0$

α is a root of this

$\Rightarrow \quad x^p - a^p \mid m_{a,K}(x)$

$\Rightarrow (x-a)^p \mid m_{a,K}(x)$

Contradict with $m_{a,K}(x)$ is reducible .

$\Leftarrow$ Suppose $K(a) = K(a^p)$

$a = f(a^p)$

$\Rightarrow f(x^p) - x = 0$

Then $m_{a,K}(x) \mid f(x^p) - x$

$(f(x^p) - x)' = -1 \neq 0$

$\Rightarrow \forall$ root x_0 of $f(x^p) - x$

$(f(x^p) - x)'_{x_0} = -1 \neq 0$

$\Rightarrow$ multiplicity of $x_0 = 1$

$\Rightarrow m_{a,K}(x)$ is reducible

---

15. Let L be a finite Galois extension of K and $H \leq G = Gal(L/K)$. Prove that $\sigma(L^H) = L^{\sigma H \sigma^{-1}}$.

$H \leq G = Gal(L/K)$

$\Rightarrow \quad L^H = \{a \in L \mid h(a) = a \ \forall h \in H\}$

$\sigma(L^H) = \{\sigma(a) \mid a \in L \text{ and } h(a) = a \ \forall h \in H\}$

$L^{\sigma H \sigma^{-1}} = \{a \in L \mid \sigma h \sigma^{-1}(a) = a \ \forall h \in H\}$

Suppose $\sigma(a) \in \sigma(L^H)$, then $h(a) = a \ \forall h \in H$

Then $\sigma h \sigma^{-1}(\sigma(a)) = \sigma h(a) = \sigma(a) \ \forall h \in H$

$\Rightarrow \quad \sigma h \sigma^{-1}(\sigma(a)) = \sigma(a) \ \forall h \in H$

$\Rightarrow \quad \sigma(L^H) \subseteq L^{\sigma H \sigma^{-1}}$

Let $a \in L^{\sigma H \sigma^{-1}}$

Then $\sigma h \sigma^{-1}(a) = a \ \forall h \in H \Rightarrow h\sigma^{-1}(a) = \sigma^{-1}(a) \ \forall h \in H$

$\sigma\sigma^{-1}(a) = a$

$\sigma(\sigma^{-1}(a)) = a$

$h(\sigma^{-1}(a)) = h\sigma^{-1}(a) = \sigma^{-1}(a) \ \forall h \in H$

$\Rightarrow \sigma(\sigma^{-1}(a)) \in \sigma(L^H)$

$\Rightarrow a \in \sigma(L^H)$

$\sigma \in Gal(L/K)$

Proof from notes: $L^{\sigma H \sigma^{-1}} = \{a \in L \mid \sigma\tau\sigma^{-1}(a) = a \ \forall \tau \in H\}$

$= \{a \mid \tau\sigma^{-1}(a) = \sigma^{-1}(a) \ \forall \tau \in H\}$

$= \{a \mid \sigma^{-1}(a) \in L^H\}$

$= L \cap \sigma(L^H)$ and $\sigma : L \to L$ fix K

$= \sigma(L^H)$ Where do we use Galois ?

---

16. Let L be a finite Galois extension of and $G = Gal(L/K)$. For $a \in L$, define $H_a = \{\sigma \in G \mid \sigma(a) = a\}$.

a) Prove that $H_a \leq G$ and $K(a) = L^{H_a}$.

b) Prove that $H_a \trianglelefteq G$ if and only if $m_{a,K}(x)$ splits over $K(a)$ if and only if $\sigma(a) \in K(a)$ for all $\sigma \in G$.

a) $\sigma_1, \sigma_2 \in G$, then $\sigma_1\sigma_2^{-1}(a) = \sigma_1(a) = a$

By $\sigma_2(a) = a$

$\Rightarrow a = \sigma_2^{-1}(a)$

$\Rightarrow \sigma_1\sigma_2^{-1} \in G$.

Therefore, $H_a \leq G = Gal(L/K)$

And It is obvious that $K(a) \leq L^{H_a}$ since H_a fix H and a

To show $L^{H_a} \leq K(a)$

Since L is Galois over K

$\Rightarrow L$ is Galois over L^{H_a}

$Gal(L/L^{H_a}) = H_a$

$\Rightarrow [L : L^{H_a}] = |H_a|$

Then consider $[L : K(a)] = Gal(L/K(a))$

$\Rightarrow H_a \leq Gal(L/K(a))$

Then Let $\tau \in Gal(L/K(a))$

$\tau(a) = a, \ \tau \in Gal(L/K)$

$\Rightarrow \tau \in H_a$

$\Rightarrow H_a = Gal(L/K(a))$ By $K(a) \leq L^{H_a}$

To show $L^{H_a} \leq K(a)$

$\Rightarrow L^{H_a} = K(a)$

By Suppose $\beta \notin K(a)$

$\Rightarrow \exists \ \sigma \in Gal(L/K(a))$ s.t.

$\sigma(\beta) \neq \beta$

$\Rightarrow \beta \notin L^{H_a}$

$\Rightarrow L^{H_a} = K(a)$

$\Rightarrow \exists\ \sigma \in Gal(L/K(\alpha))$ s.t.

$\sigma(\beta) \neq \beta$

$\Rightarrow \beta \notin L^{H_\alpha}$

$\Rightarrow L^{H_\alpha} = K(\alpha)$

b) Prove that $H_\alpha \trianglelefteq G$ if and only if $m_{\alpha,K(\alpha)}$ splits over $K(\alpha)$ if and only if $\sigma(\alpha) \in K(\alpha)$ for all $\sigma \in G$

If $H_\alpha \trianglelefteq G \iff L^{H_\alpha} = K(\alpha)$ is Galois over $K \iff K(\alpha)$ is normal and separable over K (By Fundamental Theorem of Galois Theory)

$\iff m_{\alpha,K(\alpha)}$ splits over $K(\alpha)$ (By Splitting Theorem)

By σ send α to another root of $m_{\alpha,K}(x)$ and $m_{\alpha,K}(x)$ splits over $K(\alpha)$

$\iff \sigma(\alpha) \in K(\alpha)\ \forall \sigma \in G$

---

18. Let L be a cyclotomic extension of a field K of characteristic zero.

a) Prove that for every $\alpha \in L$, $m_{\alpha,K}(x)$ splits over $K(\alpha)$

This is by $Gal(L/K)$ is cyclic

$\Rightarrow Gal(L/K(\alpha)) \trianglelefteq Gal(L/K)$

$\Rightarrow$ $K(\alpha)$ is Galois over K

$\Rightarrow$ $K(\alpha)$ is normal and separable over K, ...

b) For this part, assume that $K = \mathbb{Q}$. Prove that $\sqrt[3]{p} \notin L$ for any prime p.

pf: Suppose $\sqrt[3]{p} \in L$, then $m_{\sqrt[3]{p},\mathbb{Q}}(x)$ splits over $\mathbb{Q}(\sqrt[3]{p})$ by a)

However, we can see that this is impossible

Also, this demonstrates why we are so confident that in (3)

$2^{\frac{1}{p}} \notin \mathbb{Q}(\zeta_p)$

Here $\mathbb{Q}(\zeta)$ is the L

---

20. Let L be a finite Galois extension of K such that $G = Gal(L/K) = D_{2n}$, where $n \geq 3$ is odd.

a) Determine the number of degree n extensions of K that are contained in L.

b) Determine the number of Galois extensions of K that are properly contained in L.

pf: a) $[M:K] = n$

$[L:K] = 2n$

$\Rightarrow [L:M] = 2$

Then $[L:M] = Gal(L/M) \leq G$,

Then $\langle s \rangle, \langle sr^d \rangle, \langle r^{\frac{n}{2}} \rangle$ if n is even

b) Determine the normal subset of D_{2n}

---

21. Let K be a field whose characteristic is not 2.

a) Prove that if K' is an extension of K and $[K':K] = 2$, then $K' = K(\alpha)$ for some $\alpha \in K'$ s.t. $\alpha^2 \in K^\times \setminus (K^\times)^2$

So $[K':K] = 2 \times 1$

$\Rightarrow$ It is going to be one extension

$\Rightarrow K' = K(\beta)$ for some $\beta \in K' \setminus K$

and also, the $m_{\beta,K}(x) = x^2 + bx + c$.

And since $char(K) \neq 2$

$\Rightarrow m_{\beta,K}(x)' \neq 0 \Rightarrow$ There is no root of $m_{\beta,K}(x)$ has multiplicity greater than one.

$\Rightarrow b^2 - 4ac \neq 0$

Since $\sqrt{b^2-4ac}$ may be undefined, so let's call it α s.t. $\alpha \in K'$ and $\alpha^2 = b^2 - 4ac$, $\alpha \notin K$ (otherwise can the $\beta \in K$)

And $x = \frac{-b \pm \alpha}{2}$

$\Rightarrow K(\beta) = K(\alpha)$

And α is the solution of polynomial $x^2 - \alpha^2 = 0$

$\alpha^2 = b^2 - 4ac \neq 0 \Rightarrow \alpha^2 \in K^\times$

And if $\alpha^2 = \gamma^2$ for some $\gamma \in K^\times$

Then $\Rightarrow 2\gamma = -\alpha^2$

$\Rightarrow \alpha \in K^\times$

Contradict

$\Rightarrow \alpha \in K^\times \setminus (K^\times)^2$

$\Rightarrow K(\beta) = K(\alpha)$ and $\alpha^2 \in K^\times \setminus (K^\times)^2$

b) Suppose that K_1 and K_2 are degree two extensions inside some normal extension of K with $K_j = K(\alpha_j)$ and $\alpha_j^2 \in K$ $j = 1, 2$. Prove that $K_1 = K_2$ if and only if α_1^2 and α_2^2 belong to the same coset of $(K^\times)^2$ in $K^\times$.

pf: $[K_1 : K] = 2$, $[K_2 : K] = 2$ $\quad$ since $\mathrm{char}(K) \neq 2 \Rightarrow K_1 = K(\alpha_1)$, $K_2 = K(\alpha_2)$, $\alpha_1, \alpha_2 \in K^\times \setminus (K^\times)^2$

By a)

Then $K_1 = K_2 \Leftrightarrow K(\alpha_1) = K(\alpha_2) \Leftrightarrow \alpha_2 = k\alpha_1$ s.t. $k \in K^\times, k \neq 0 \Leftrightarrow \alpha_1^2(\alpha_2^{-1})^2 = \frac{1}{k^2} = (\frac{1}{k})^2 \in (K^\times)^2$

$\Leftrightarrow \alpha_1^2(K^\times)^2 = \alpha_2^2(K^\times)^2$

Notice we are talking about $(K^\times)^2$

So we are talking about the

operation under $\cdot$,

Show $(K^\times)^2 \leq K^\times$

By $a^2(b^{-1})^2 = (ab^{-1})^2 \in (K^\times)^2$

by abelian

$\Rightarrow$ subgroup

No need to check normal since we are talking about cosets.

$\alpha_1^2 \in \alpha_1^2(K^\times)^2$

$\alpha_2^2 \in \alpha_2^2(K^\times)^2$ $\qquad \alpha_1^2(K^\times)^2 = \alpha_2^2(K^\times)^2$

$\Leftrightarrow \alpha_1^2(\alpha_2^{-1})^2 \in (K^\times)^2$

Then $\alpha_2 = k_0 + k_1\alpha_1$ s.t. $k_1 \neq 0$ by $\alpha_2 \notin K^\times$

show $k_0 = 0$

By $\alpha_2^2 \in K^\times$, $\alpha_1^2 \in K^\times$

$\Rightarrow \alpha_2^2 = k_0^2 + k_1^2\alpha_1^2 + 2k_0k_1\alpha_1$

$\Rightarrow 2k_0k_1\alpha_1 \in K^\times$

$\Rightarrow k_0 = 0$

c) Suppose that L is a Galois extension of K such that $[L:K] = 3$. Let M be an extension of L that is Galois over K and such that $\mathrm{Gal}(M/K) \cong A_4$. Describe the intermediate extensions between L and M. Which of them are Galois over K?

pf: $\mathrm{Gal}(L/K) = 3$. $\quad |A_4| = \frac{4!}{2} = 12$

$$|\mathrm{Gal}(M/K)| = [M:K] = [M:L]\underbrace{[L:K]}_{3} = 12$$

$$\Rightarrow [M:L] = 4$$

Consider $L \subsetneq L' \subsetneq M$

Then M is Galois over L', M is Galois over L and M is Galois over K

And L' is Galois over K

If and only if $\mathrm{Gal}(L'/K) \cong \mathrm{Gal}(M/K)/\mathrm{Gal}(M/L')$

$\mathrm{Gal}(M/L') \trianglelefteq \mathrm{Gal}(M/K)$

and $|\mathrm{Gal}(L'/K)| = [L':K] > [L:K] = 3$

$\Rightarrow \mathrm{Gal}(M/L') < 4$

$[M:L] = 4 \Rightarrow M = L(\alpha, \beta)$ or $M = L(\alpha)$

If $M = L(\alpha, \beta)$, then $[M:L] = 2 \times 2$

If $M = L(\alpha)$, then $[M:L] = 4$

Consider $|\mathrm{Gal}(M/L)| = 4$

And $\mathrm{Gal}(M/L) \leq A_4$

$|A_4| = 12 = 3 \times 2^2$

Does A_4 has subgroup of order 6?

If $H \leq A_4$ and $|H| = 6$, $|A_4 : H| = 2 \Rightarrow H \trianglelefteq A_4$

Then consider

A_4/H, By the prop that A_n is generated by 3-cycles

choose the 3 cycles not in H. Then since $|A_4/H| = 2$

A_4/H. By the prop that A_n is generated by 3-cycles

choose the 3 cycles not in H. Then since $|A_4/H| = 2$

$\Rightarrow H, xH, x^2H$ must 2 of them are equal

One can show it is impossible

$\Rightarrow$ There is no subgrp of order 6

Then consider $|n_2| = |(\text{cyl } 2)$ (subgroup with order $2^2 = 4$)

$n_2 \mid 3 \Rightarrow n_2 = 1$ or $n_2 = 3$

$|n_3| = |(\text{cyl } 3)$

$n_3 \mid 4 \Rightarrow n_3 = 1$ or $n_3 = 4$

Since we know there are not only one subgrp with order 3

$\Rightarrow n_3 \neq 1 \Rightarrow$ no normal subgroup with order 3

Consider subgroup with order 2.

$\{e, (1\ 2)(3\ 4)\}$

$\{e, (1\ 3)(2\ 4)\}$

$\{e, (1\ 4)(2\ 3)\}$

Therefore, A_4 only has normal subgrp of order 4.

So there is an intermediate field L' s.t. $L \subsetneq L' \subsetneq M$ and L' is Galois over K.

Then $M = L(\alpha, \beta)$
or $M = L(2)$ $\quad |Gal(M/L)| = [M:L] = 4$

if $M = L(\alpha, \beta)$, then

$[L(\alpha,\beta) : L(\alpha)][L(\alpha) : L] = 2 \times 2$

$[L(\alpha) : L] = 4$

but $L(\alpha)$ is Galois over 4

$\Rightarrow$

---

22. Let L be a finite Galois extension of a field K. Suppose that $[L:K] = n \geq 2$, $Gal(L/K)$ is cyclic and $L = K(\alpha)$ for some $\alpha \in L$ that satisfies $\alpha^n \in K$.

If $\exists\, d$ s.t. $d \leq n$, and $\alpha^d \in K$

Then $x^d - \alpha^d$ has a root α

$\Rightarrow$ Contradict with $[L:K] = n$

$\Rightarrow x^n - \alpha^n$ has root of α, and $x^n - \alpha^n \in K(x)$

and $m_{\alpha,K}(x) \mid x^n - \alpha^n$

By $[L:K] = n \Rightarrow m_{\alpha,K}(x) = x^n - \alpha^n$

a) Prove that the set of intermediate subfields extension L of K are $\{K(\alpha^d) \mid 1 \leq d \leq n, d \mid n\}$.

Since L is Galois over K

We can show that if $K \subseteq M \subseteq L$

L is Galois over M

$\Rightarrow Gal(L/M) \leq Gal(L/K)$ by cyclic

$\Rightarrow M$ is Galois over K

Let $|Gal(L/M)| = d$

Now, consider $K(\alpha^d)$

By $m_{\alpha^d,K}(x) \mid x^{\frac{n}{d}} - \alpha^n$

$\Rightarrow \deg m_{\alpha^d,K}(x) \leq \frac{n}{d}$

$[K(\alpha^d) : K] \leq \frac{n}{d}$

$m_{\alpha, K(\alpha^d)}(x) \mid x^d - \alpha^d$

$\Rightarrow [K(\alpha) : K(\alpha^d)] \leq d$

Since $[K(\alpha) : K] \leq n$

$\Rightarrow [K(\alpha^d) : K] = \frac{n}{d}$

$[K(\alpha) : K(\alpha^d)] = d$

$\Rightarrow K(\alpha)$ is Galois over K

and $Gal(K(\alpha)/K(\alpha^d)) = d$

Since $Gal(K(\alpha)/K)$ is cyclic

$\Rightarrow$ any subgroup is unique

and $Gal(K(2)/K(2^d)) = d$

Since $Gal(K(2)/K)$ is cyclic

$\Rightarrow$ any subgroup is unique

$\Rightarrow Gal(K(2)/M) = Gal(K(2)/K(2^d))$

And $L^{Gal(K(2)/M)} = L^{Gal(K(2)/K(2^d))}$

$L^{Gal(K(2)/M)} = M$

$L^{Gal(K(2)/K(2^d))} = K(2^d)$

$\Rightarrow M = K(2^d)$

b) Prove that $x^n - 1$ has n distinct roots in L.

Pf: $x^n - 2^n$ has n distinct roots by $K(2)$ is Galois over K and $[K(2):K] = n$

$x^n - 2^n = 0$ has n distinct roots in L

Show: $(\frac{x}{2})^n - 1 = 0$ has n distinct roots

By $2_1 \neq 2_2$ and $2_1^n - 2^n = 2_2^n - 2^n = 0$

$\Rightarrow (\frac{2_1}{2})^n - 1 = (\frac{2_2}{2})^n - 1 = 0$

And $2_1 2^{-1} \neq 2_2 2^{-1}$ (otherwise $2_1 = 2_2$)

$\Rightarrow$ $x^n - 1$ has n distinct solutions $2_i 2^{-1}$, and $2_i \in L$, $2^{-1} \in L$

$\Rightarrow$ They are all in L and distinct.

---

24. Let L be the splitting field of a nonconstant $f(x) \in K[x]$. Suppose that $|Aut(L/K)| < [L:K]$. Let $M = L^{Aut(L/K)}$.

Prove that there exists a prime p and a natural number l such that $[M:K] = p^l$

By proposition, L is Galois over M and

$[L:M] = |Gal(L/M)| = |Aut(L/K)| < [L:K]$

$K \subseteq M \subseteq L$

$[L:K] = [L:M][M:K]$

Thus, $[M:K] = \frac{[L:K]}{[L:M]} = \frac{[L:K]}{|Gal(L/M)|}$

L is a splitting field of $f(x)$ over K

$char(K) \neq 0$ Otherwise L is separable and normal over $K \Rightarrow L$ is Galois over K, contradict,

$\Rightarrow char(K) = p$.

$2 \in M \subseteq L$

L is normal over K. For $2 \in M$, $m_{2,K}(x) \in K[x]$ has only one root.

If $m_{2,K}(x)$ has another root, since L is normal, $\beta \in L$, $\beta \neq 2$

Then there exists $\sigma \in Aut(L/K)$ s.t. $\sigma(2) = \beta$ by splitting theorem

Then since $2 \in M = L^{Aut(L/K)}$, $\sigma(2) \neq \beta$, contradict, thus, $m_{2,K}(x)$ is of the form $(x-2)^n$, thus $m_{2,K}(x)' = 0$ (By $m_{2,K}(x)$ is irreducible and $m_{2,K}(x)$ has multiplicity greater than 1)

$\Rightarrow m_{2,K}(x) = g(x^p)$ for some $g(x) \in K[x]$ (By proposition from worksheet)

$\Rightarrow$ ----- (Stuck, will be back)

---

25. Let L be a finite Galois extension of K and Let H be a subgroup of G and $G = Gal(L/K)$. Prove that $Aut(L^H/K)$ is isomorphic to $N_G(H)/H$. (Here, $N_G(H)$ is the normalizer of H in G).

Pf: $H \trianglelefteq N_G(H)$ by $\forall g \in N_G(H)$ $gHg^{-1} = H$ (definition)

And $N_G(H) \leq Gal(L/K)$

Consider $\sigma \in N_G(H)$

From previous question, we have $L^{\sigma H \sigma^{-1}} = \sigma(L^H)$ (check Q15)

And since $\sigma H \sigma^{-1} = H$

$\Rightarrow L^H = \sigma(L^H)$ and $\sigma \in Aut(L/K)$

$\Rightarrow \sigma|_{L^H} \in Aut(L^H/K)$

$\Rightarrow$ Consider the map $N_G(H)/H \to Aut(L^H/K)$

$\sigma H \mapsto \sigma|_{L^H}$, we need to show this map is homomorphic and bijective

Then to show it is well-defined by

Suppose $\sigma_1 H = \sigma_2 H$

Then $\sigma_1^{-1}\sigma_2 \in H = Aut(L/L^H)$

$\Rightarrow \sigma_1^{-1}\sigma_2$ fixes L^H

$\Rightarrow \sigma_1|_{L^H} = \sigma_2|_{L^H}$

$\varphi(\sigma_1 H \sigma_2 H) = \varphi(\sigma_1\sigma_2 H)$

$= \sigma_1\sigma_2|_{L^H}$

$= \sigma_1|_{L^H} \circ \sigma_2|_{L^H}$

$= \varphi(\sigma_1 H)\varphi(\sigma_2 H)$

By $\sigma_1(L^H) = L^H$, $\sigma_2(L^H) = L^H$

Suppose $\sigma_1 H = \sigma_2 H$

Then $\sigma_1^{-1}\sigma_2 \in H = Aut(L/L^H)$

$\Rightarrow \sigma_1^{-1}\sigma_2$ fixes L^H

$\Rightarrow \sigma_1|_{L^H} = \sigma_2|_{L^H}$

So it is well-defined

To show injective

$\sigma_1|_{L^H} = \sigma_2|_{L^H}$

$\sigma_1^{-1}\sigma_2$ fixes L^H

$\sigma_1^{-1}\sigma_2 \in Aut(L/L^H)$

$\sigma_1^{-1}\sigma_2 \in H$

$\Rightarrow \sigma_1 H = \sigma_2 H$

$= \sigma_1\sigma_2|_{L^H}$ By $\sigma_1(L^H) = L^H$, $\sigma_2(L^H) = L^H$

$= \sigma_1|_{L^H} \circ \sigma_2|_{L^H}$

$= \varphi(\sigma_1 H)\varphi(\sigma_2 H)$

Thus φ is homomorphic

To show surjective, consider $\tau \in Aut(L^H/K)$

Extends τ to the $\sigma \in Aut(L/K)$

(i.e. $\sigma|_{L^H} = \tau$, check

the arguments for extending $Hom_K(M,L)$ to $Gal(L/K)$)

Now, suppose $\sigma \in Aut(L/K)$ s.t. $\sigma|_{L^H} = \tau$

Still use previous question's conclusion

$L^{\sigma H \sigma^{-1}} = \sigma(L^H)$

$= \tau(L^H) = L^H$

By $\sigma H \sigma^{-1} = Aut(L/L^{\sigma H \sigma^{-1}})$

$H = Aut(L/L^H)$

$\Rightarrow \sigma H \sigma^{-1} = H$

$\Rightarrow \sigma \in N_G(H)$

$\Rightarrow$ surjective

$\Rightarrow$ Isomorphism exists.

---

27. Suppose that L is a Galois extension of K and H is a minimal nontrivial subgroup of $Gal(L/K)$. Prove that if L^H is not Galois over K, then L is a normal closure of L^H over K.

pf: Suppose L is not the normal closure of L^H over K

$\exists L'$ s.t. $K \subsetneq L^H \subsetneq L' \subsetneq L$ s.t. L' is normal over K and $L' \supseteq L^H$

Then L is Galois over L' and $L' = L^{Gal(L/L')}$

$\Rightarrow L^{Gal(L/L')} \supseteq L^H$

$\Rightarrow Gal(L/L') \subsetneq H$ contradict with H is minimal nontrivial subgroup

Then the only possibilities is that L^H is the normal closure of L^H over K

Then L^H is normal over K

Since L is separable $\Rightarrow L^H$ is separable over K

$\Rightarrow L^H$ is Galois over K

Contradict with L^H is not Galois over K.

---

28. Let L be a finite Galois extension of K and $G = Gal(L/K)$. Let $K \subseteq M \subseteq L$ and $H = Gal(L/M)$. Prove that L is a normal closure of M over K if and only if $\bigcap_{\sigma \in G} \sigma H \sigma^{-1} = 1$

pf: ($\Rightarrow$):

Suppose L is normal closure of M over K $\Rightarrow M$ is not Galois over K

$H = Gal(L/M) \subsetneq Gal(L/K)$

And Then is no L' s.t. $M \subseteq L' \subsetneq L$

s.t. L' is Galois over K

$\Rightarrow 1 \neq Gal(L/L') \subsetneq Gal(L/K)$

$1 \neq Gal(L/L') \subseteq H \subseteq Gal(L/K)$ $\Rightarrow$ $\forall$ nontrivial subgroup of H it is not a normal subgroup of G, otherwise L is not the normal closure of M over K.

$\sigma_1 H \sigma_1^{-1} \neq \sigma_2 H \sigma_2^{-1}$ $\forall h \neq 1$, $h \in H$

$L^{\bigcap_{\sigma \in G} \sigma H \sigma^{-1}} \supseteq L^{\sigma_1 H \sigma_1^{-1}} = \sigma_1(L^H)$

Want to show this: $\bigcap_{\sigma \in G} \sigma H \sigma^{-1} = 1 \Rightarrow \bigcap_{\sigma \in G} \sigma H \sigma^{-1} \subseteq 1$

$\Rightarrow L^{\bigcap_{\sigma \in G} \sigma H \sigma^{-1}} \supseteq L^1 = L$

Then need to show: $L^{\bigcap_{\sigma \in G} \sigma H \sigma^{-1}} \supseteq \bigcup_{\sigma \in G} \sigma(L^H) = L$

Okay, this is not that useful

From Frank Exchange: Lemma: Intersection of conjugate closures is normal in G.

$H \leq G$, $K = \bigcap_{g \in G} gHg^{-1}$, then $K \trianglelefteq G$

pf: Let $\sigma \in G$

$\sigma K \sigma^{-1} = \sigma(\bigcap_{g \in G} gHg^{-1})\sigma^{-1}$

$= \bigcap_{g \in G} (\sigma g H g^{-1} \sigma^{-1})$ σ acts on G, it's just a reparametrize

$= \bigcap_{g \in G} (gHg^{-1})$

$= K$

$\Rightarrow K \trianglelefteq G$

Therefore, in this question $\bigcap_{\sigma \in G} \sigma H \sigma^{-1}$ normal in G

is also a subgroup of H

$\Rightarrow$ $K \trianglelefteq G$

Therefore, in this question $\bigcap_{\sigma \in G} \sigma H \sigma^{-1}$ normal in G

and it's also a subgroup of H

by if $\sigma \in H$, then $\sigma H \sigma^{-1} = H$

$\Rightarrow$ By conclusion we get above

$\Rightarrow$ $\bigcap_{\sigma \in G} \sigma H \sigma^{-1} = 1$

($\Leftarrow$): Suppose $\bigcap_{\sigma \in G} \sigma H \sigma^{-1} = 1$, Suppose L is not the normal closure of M over K, but L is still normal and separable over K

Then $\exists L'$, s.t. $M \subseteq L' \subsetneq L$ and L' is normal closure of M over K

Therefore L' is normal and separable over K

$\Rightarrow$ L' is Galois over K

$\Rightarrow$ $Gal(L'/K) \trianglelefteq G$

and $L' \supseteq M$

$\Rightarrow$ $Gal(L'/K) \leq Gal(L/M) = H$

And since $Gal(L'/K)$ is nontrivial

(otherwise $|Gal(L'/K)| = 1 \Rightarrow [L : L'] = 1$

Contradict $L \neq L'$)

$\Rightarrow$ $\bigcap_{\sigma \in G} \sigma Gal(L'/K) \sigma^{-1} \neq 1$

$\Rightarrow$ $\bigcap_{\sigma \in G} \sigma H \sigma^{-1} \neq 1$

Contradict

---

29. Let L be a finite Galois extension of K. Let $G = Gal(L/K)$. Suppose that $f(x) \in L[x]$ is monic and the coefficients of $f(x)$ generate L over K. Let $g(x) = \prod_{\sigma \in G} \sigma(f)(x)$.

a) Show that $g(x) \in K[x]$

L is Galois over K.

$g(x) = \prod_{\sigma \in G} \sigma(f)(x)$

Consider $\forall \tau \in G$,

$\tau(g)(x) = \prod_{\sigma \in G} \tau\sigma(f)(x)$

$= \prod_{\sigma \in G} \sigma(f)(x)$ just a permutation

$= g(x)$

$\Rightarrow \tau(g)(x) = g(x) \quad \forall \tau \in G$

If $g(x) \notin K[x]$, say coefficient $a_i \notin K$

By Galois theory, $\exists \tau$ s.t. $\tau(a_i) \neq a_i$

$\Rightarrow \tau(g) \neq g(x)$

Contradict

$\Rightarrow g(x) \in K[x]$

---

b) Show that if $f(x)$ is separable and irreducible in $L[x]$, then $g(x)$ is separable and irreducible in $K[x]$.

pf: Suppose $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$

$f(x)$ is separable, and irreducible $\Rightarrow f'(x) \neq 0$

$L = K(a_{n-1}, a_{n-2}, \cdots, a_1, a_0)$

$\Rightarrow f(x) \notin K[x]$

$g(x) = \prod_{\sigma \in G} \sigma(f)(x)$

Since $\sigma_1(f)(x) \neq \sigma_2(f)(x)$ if $\sigma_1 \neq \sigma_2$

(otherwise $\sigma_1(a_i) = \sigma_2(a_i)$

and since $L = K(a_{n-1}, \cdots, a_0)$

$\Rightarrow \sigma_1 = \sigma_2$)

First, let's show $\sigma(f)(x)$ is separable:

by $f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$

Then $\sigma(f)(x) = (x - \beta_1)(x - \beta_2) \cdots (x - \beta_n)$

Consider the splitting field L' of $f(x)\sigma(f)(x)$ over L

Then σ extends to one $\sigma' \in Aut(L'/K)$

s.t. $\sigma'|_L = \sigma$

Then $\sigma'(\alpha)$ is the root of $\sigma(f)(x) = \sigma(f)(x)$

Then $\sigma(f)(x)$ is separable.

Or if $\sigma(f)'(x) \neq 0$, then $\sigma(f)(x)$ is separable since $\sigma(f)$ is irreducible.

Then $\sigma(f)(x)$ is separable.

Or if $\sigma(f)'(x) \neq 0$, then $\sigma(f)(x)$ is separable since $\sigma(f)$ is irreducible.

Then $\sigma(f)(x)' = nx^{n-1} + (n-1)\sigma(a_{n-1})x^{n-2} + \cdots + \sigma(a_1)$

$\neq 0$

$\Rightarrow$ $\sigma(f)(x)$ is separable.

We also want to show $\sigma(f)(x)$ and $\sigma'(f)(x)$ no same root.

Suppose they have the same root, let's say α

$\sigma(f)(\alpha) = 0$

$\sigma'(f)(\alpha) = 0$ Then $\sigma(f)$ and $\sigma'(f)$ are both monic and irreducible

but $\sigma(f) \neq \sigma'(f)$

This contradicts with the uniqueness of minimal polynomial.

Thus, one can show that $g(x)$ is seperable.

To show $g(x)$ is irreducible.

Suppose $g(x) = g_1(x)g_2(x)$ s.t. $g_1(x)$ is irreducible on $K[x]$

Now, we want to show $\exists\ \sigma$ s.t. $\sigma(g_1(x)) \neq g_1(x)$

$g_1(x) = \sigma_1^1(f)(x)\,\sigma_1^2(f)(x) \cdots \sigma_1^m(f)(x)$

$g_2(x) = \sigma_2^1(f)(x)\,\sigma_2^2(f)(x) \cdots \sigma_2^m(f)(x)$

Then consider $\tau \in Aut(\frac{M}{K})$

Then since $\tau\sigma_1^i(f)(x) = \sigma_2^j(f)(x)$ for some j

And $\sigma(f)(x)$ and $\sigma(f)(x)$ don't have same root $\forall\ \sigma$ and σ'

$\Rightarrow$ $\tau(g_1(x)) \neq g_1(x)$

Then contradict with $g_1(x) \in K[x]$

---

c) Let α be a root of $f(x)$ in an extension of L. Show that a splitting field of $g(x)$ over K is a Galois closure of $L(\alpha)$.

pf: First, let's show that the splitting field of $g(x)$ over K. Call it M, we want to show

M is Galois over K

By M is splitting field of a <u>separable</u> function $g(x)$ over K $\Rightarrow$ $|Aut(\frac{M}{K})| = [M:K]$ (Check "Solvable Galois section")

Then M is Galois over K

And since $f(x)$ splits on M

Then coefficients of $f(x) \subseteq M$

Thus L and α are contained in M

$\Rightarrow$ $K \subseteq L \subseteq L(\alpha) \subseteq M$

Now, we want to show that M is the Galois closure <u>over K</u> of $L(\alpha)$

i.i.e. $\nexists M'$ s.t. $K \subseteq L \subseteq L(\alpha) \subseteq M' \subsetneq M$ s.t. M' is Galois over K and $L(\alpha) \subseteq M' \subsetneq M$)

Suppose there exists such M', since M' is Galois over K and $g(x)$ is irreducible in $K[x]$ and $g(\alpha) = 0$, and $\alpha \in L(\alpha) \subseteq M'$, then $g(x)$ splits in M' which contradict M is the splitting field of $g(x)$ over K.
