Field Exercise 2

Thursday, April 12, 2018 5:53 AM

31. Suppose that L is Galois extension of K such that $Gal(L/K) \cong S_n$. (Assume that $n \geq 3$)

a) Prove that there exists a subfield M of L containing K such that $[M:K] = n$ and $M = K(\alpha)$ for every $\alpha \in M \setminus K$.

(Hint: What can you say about properties of the subgroup $Gal(L/M)$?)

Pf: $[L:M] = (n-1)!$

$\Rightarrow |Gal(L/M)| = (n-1)!$

$\Rightarrow$ Consider $L^{S_{n-1}}$, then $|Gal(L/L^{S_{n-1}})| = |S_{n-1}| = n!$

Let $M = L^{S_{n-1}} \Rightarrow [M:K] = n$

To show $M = K(\alpha)$ for every $\alpha \in M \setminus K$,

then consider $m_{\alpha,K}(x)$

Since $\alpha \notin K$, $\exists \sigma \in Aut(L/K) \setminus Aut(L/M)$

s.t. $\sigma(\alpha) \neq \alpha$

We want to $\exists$ a n-cycle σ satisfies this

Then consider the $H \subseteq Gal(L/K)$ s.t. $\forall h \in H$, $h(\alpha) = \alpha$, H is a subgroup by $h_1 h_2^{-1}(\alpha) = \alpha$

Then $Gal(L/M) \leq H \leq S_n$

$S_{n-1} \leq H \leq S_n$

Let's show S_{n-1} is the maximal subgroup of S_n.

Suppose $\exists H$ s.t. $S_{n-1} \subsetneq H \subsetneq S_n$

Then let c be a cycle involving $n+1$

$c = (a, \cdots, b, n) \in H$

Consider S_n acts on c

Let $\sigma \in S_{n-1}$, s.t. $\sigma(a) = b$

$\Rightarrow \sigma c(n) = b$

$\sigma c(b) = n$

$\Rightarrow \sigma c = \sigma'(b\ n)$

s.t. $\sigma'(n) = n$

$\Rightarrow \sigma' \in S_{n-1} \leq H$

$\sigma c \in H$

$\sigma' \in H$

$\Rightarrow (b\ n) \in H$

$\Rightarrow (1\ n) \in H$

And $S_{n-1} \leq H$

$\Rightarrow (1\ i) \in H$ for $1 \leq i \leq n$

But $S_n = \langle (1, i) \rangle$

$\Rightarrow S_n = H$

$\Rightarrow S_{n-1}$ is the maximal subgroup of S_n

b) Take $\alpha \in M \setminus K$, Since L is Galois over K, and $\alpha \in M \setminus K \subseteq L$, $\Rightarrow m_{\alpha,K}(x)$ splits in L.

We want to show L is the normal closure of $M = K(\alpha)$ over K. Then L is the splitting field of $m_{\alpha,K}(x)$. We do this by suppose $\exists L'$ s.t. L' is normal over K, and $K \subseteq M \subseteq L' \subsetneq L$

Then L' is normal and separable over K by L is separable over K

$\Rightarrow L'$ is Galois over K

Then L' is normal and separable over K by L is separable over K

$\Rightarrow L'$ is Galois over K

And since $L' \supseteq M$

$\Rightarrow Gal(L/L') \leq Gal(L/M) = S_{n-1}$

And $Gal(L/L') \trianglelefteq S_n$

So we must $Gal(L/L') = \{1\}$

Suppose $m_{\alpha,K}(x) = (x-\alpha_1)(x-\alpha_2) \cdots (x-\alpha_n)$

Then by definition of splitting field

$L' = K(\alpha_1, \alpha_2, \cdots, \alpha_n)$

Then $Gal(L/L') = Gal(L/K(\alpha_1, \alpha_2, \cdots, \alpha_n)) = \bigcap Gal(L/K(\alpha_i))$

$= \bigcap \{ \rho \in Gal(L/K) \mid \rho(\alpha_i) = \alpha_i \}$

By Q(16)

Okay, let's use the conclusion from 28.

Here $G = Gal(L/K) = S_n$, $H = Gal(L/M) = S_{n-1}$

Then consider $(b \ \ n)$ where $1 \leq b \leq n-1$

$\sigma \underbrace{(\ \ )(\ \ ) \cdots (\ \ )}_{\tau} \sigma^{-1}$

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

Then for each cycle $(a_1, \cdots, a_K)$

$\sigma(a_1, \cdots, a_K)\sigma^{-1}$

$= (\sigma(a_1) \cdots \sigma(a_K))$

$\Rightarrow$ If b is in a cycle of τ

Then $\sigma\tau\sigma^{-1} \in S_n \setminus S_{n-1}$

$\Rightarrow$ One can show that $\bigcap_{\sigma \in S_n} \sigma S_{n-1} \sigma^{-1}$

$= \bigcap_{\sigma \in S_n} (\sigma S_{n-1} \sigma^{-1} \cap S_{n-1})$

$= \{1\}$

$\Rightarrow L$ is the normal closure of M over K

$\Rightarrow L$ is the splitting field of $m_{\alpha,K}(x)$ over K, $M = K(\alpha)$

---

32. Suppose that $f(x) \in \mathbb{Q}[x]$ is irreducible of degree 3 and has cyclic Galois group.

a) Prove that all of the roots of $f(x)$ are real.

pf: Let L be the splitting field of $f(x)$, $f(x)$ is separable by $char(\mathbb{Q}) = 0$

So $Gal_{\mathbb{Q}}(f(x)) = Gal(L/\mathbb{Q})$

Suppose $Gal(L/\mathbb{Q})$ is cyclic, then

Since it is degree 3 then it must have a real root

Suppose it has a nonreal root, then by Q6,

Since it is degree 3 then it must have a real root
Suppose it has a nonreal root, then by Q6,
one can show $Aut(L/Q)$ is nonabelian, contradict
with $Gal(L/Q)$ is cyclic.

$\Rightarrow$ There is no nonreal root

$\Rightarrow$ All roots are real.

b) Let $L \subset \mathbb{R}$ be a splitting field of $f(x)$ over $\mathbb{R}$. Prove that L is not of the form $L = Q(\alpha)$, where $\alpha^n \in Q$ for some $n \in \mathbb{N}$. (Note: This implies that when using radicals to solve for the roots of $f(x)$, it is necessary to work in larger field than L.)

pf: Suppose $L = Q(\alpha)$

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

Then $Gal(L/Q)$ is solvable, we want to show $Gal(Q(\alpha)/Q)$ is not solvable

$Gal(Q(\alpha)/Q) = [Q(\alpha) : Q]$

Let n be the smallest one s.t. $\alpha^n \in Q$

Then $m_{\alpha,Q}(x) \mid x^n - \alpha^n$

$\Rightarrow |Gal(L/Q)| = |Gal(Q(\alpha)/Q)| \mid x^n - \alpha^n$

$f(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$

$[Q(\alpha_1) : Q] = 3$

$[Q(\alpha_2, \alpha_1) : Q(\alpha_1)] = 2$ or 1

$[Q(\alpha_3, \alpha_2, \alpha_1) : Q(\alpha_2, \alpha_1)] = 1$

By $\alpha_1\alpha_2\alpha_3 \in Q \subseteq Q(\alpha_1, \alpha_2)$

$\alpha_1, \alpha_2 \in Q(\alpha_1, \alpha_2)$

$\Rightarrow \alpha_3 \in Q(\alpha_1, \alpha_2)$

Let L' be splitting field of $x^n - \alpha^n$

$\Rightarrow L'$ is Galois over Q and

$Q \subseteq L \subseteq L'$

I have no idea, give up, FYI, check book pg 630.

---

35. Construct a finite field of 16 elements.

Consider $F_2[x]$ and x^4+x+1

x^4+x+1 is irreducible in $F_2[x]$

By x^4+x+1 has no roots in F_2

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

$= x^4 + acx^2 + ax^3 + cx^3 + (bc+ad)x + bd$

$\Rightarrow$ $a = 0$
$c = 0$
But $bc + ad = 0$ contradict

$\Rightarrow x^4+x+1$ is irreducible

Then let α be the root of x^4+x+1, then

$F_2[x]/(x^4+x+1) \cong \underline{F_2(\alpha)}$

is a field with basis

$\{1, \alpha, \alpha^2, \alpha^3\}$ over field F_2

So order is 16.

---

36. Let $R = \mathbb{Z}[\sqrt{2}]/(5)$

a) Prove that R is a finite field (Note: It is okay to use the fact that $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain)

$$(a+b\sqrt{2})(c+d\sqrt{2}) = 1+5k$$

$$c+d\sqrt{2} = \frac{(1+5k)(a-b\sqrt{2})}{a^2-2b^2}$$

$$a^2-2b^2 \mid 1+5k$$

$$\Rightarrow \quad 1+5k = t(a^2-2b^2)$$

$$5k = t(a^2-2b^2)-1$$

$$k = \frac{t(a^2-2b^2)-1}{5}$$

$$a^2 \equiv \pm 1 \pmod 5$$

$$2b^2 \equiv \pm 2 \pmod 5$$

$$a^2-2b^2 \equiv 3, -1, 1, -3 \pmod 5$$

$$\Rightarrow \exists t \text{ s.t. } 5 \mid t(a^2-2b^2)-1$$

$\Rightarrow R$ is a field.

Method 2:

Or since $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain

We want to show 5 is irreducible

suppose $(a+b\sqrt{2})(c+d\sqrt{2}) = 5$

$$\Rightarrow a+b\sqrt{2} \mid 5$$

$$a^2+2b^2 \mid 25$$

$$a^2+2b^2 = 5$$

$$a^2+2b^2 = 1$$

$$\Rightarrow a = 1$$

$$a^2+2b^2 = 25$$

$$\Rightarrow a = 5$$

$\Rightarrow$ 5 is irreducible

$\Rightarrow$ (5) is maximal ideal

$\Rightarrow$ $\mathbb{Z}[\sqrt{2}]/(5)$ is a field

finite be $\mathbb{Z}[\sqrt{2}]/(5) \cong \bar{a}+\bar{b}\sqrt{2}$, thus there are $5 \times 5 = 25$ elements

b) Prove or disprove that R is isomorphic to $\mathbb{F}_5[x]/(x^2-x+1)$

No idea.

---

39. Let p be a prime and $n \in \mathbb{N}$. Prove that there exists $\alpha \in \mathbb{F}_p$ s.t. each subfield of $\mathbb{F}_{p^n}$ is of the form

39. Let p be a prime and $n \in \mathbb{N}$. Prove that there exists $\alpha \in F_p$ s.t. each subfield of F_{p^n} is of the form $F_p(\alpha^l)$ for some natural number l.

What we have: F_{p^n} is the splitting field of $x^{p^n} - x$

And F_{p^n} is Galois over F_p

And $[F_{p^n} : F_p] = n$

Then, consider this, $(F_{p^n})^\times$ is a cyclic group

let's the generator be γ, $(F_{p^n})^\times = \langle \gamma \rangle$

Then consider $ev_\gamma : F_p[x] \to F_{p^n}$

This is onto by if $f(x)$ is a zero polynomial $\Rightarrow f(\gamma) = 0$
if $f(x) = x^k$, $f(\gamma) = \gamma^k$

And cyclic $\Rightarrow$ Onto

So $ev_\gamma : F_p[x] \to F_{p^n}$ is onto

And $F_p[x] / \ker ev_\gamma \cong F$

$\Rightarrow \ker ev_\gamma$ is a maximal ideal

And $F_p(x)$ is a P.I.D

$\Rightarrow \ker ev_\gamma$ is of the form $(\pi(x))$ for some $\pi(x)$ is irreducible in $F_p[x]$

$\Rightarrow \quad F_{p^n} \cong F_p[x] / (\pi(x))$

Then $\exists$ minimal polynomial $\pi(x)$ such that this happens

γ is the root of $\pi(x)$

$\Rightarrow F_{p^n} = F_p(\gamma)$ By definition

And $[F_{p^n} : F_p] = n$, $[F_p(\gamma) : F_p] = n$

$\Rightarrow \forall$ subfield L s.t. $F_p \subseteq L \subseteq F_{p^n}$

Then, by we let's say subfield F_{p^d}

$[F_{p^n} : F_p] = [F_{p^n} : F_{p^d}][F_{p^d} : F_p] = n$

$\Rightarrow d \mid n$

Then $F_{p^d} = F_p(\beta)$ for $\langle \beta \rangle = (F_{p^d})^\times$

$\Rightarrow \quad \beta = \gamma^l$ for some l $\quad |\beta| = p^d - 1$,

$\Rightarrow F_{p^d} = F_p(\beta) = F_p(\gamma^l)$ for some

$$\frac{p^n - 1}{(p^n - 1, l)} = p^d - 1$$

$$(p^n - 1, l) = \frac{p^n - 1}{p^d - 1} = \frac{(p^d)^{\frac{n}{d}} - 1^{\frac{n}{d}}}{p^d - 1}$$

Question: How to get l ?

Or we can just get $(p^n - 1, l) = \frac{p^n - 1}{p^d - 1}$?

40. Let p be prime, suppose that $f(x) \in F_p[x]$ has degree six and has no roots in F_p.

a) What are the possible degrees of the splitting field of $f(x)$ over F_p? Prove that each of degrees you list is actually the degree of a splitting field (over F_p) of some degree six polynomial in F_p