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. $S_{n-1} \lneq H \lneq S_n$

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

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

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

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 want $Gal(L/L') = \{1\}$

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

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

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

Then by definition of splitting field

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

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

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

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 $1 \leq b \leq n-1$

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

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

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,

one can show $Aut(L/\mathbb{Q})$ is nonabelian, contradict

with $Gal(L/\mathbb{Q})$ 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 $L = \mathbb{Q}(\alpha)$, where $\alpha^n \in \mathbb{Q}$ 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.) Suppose $L = \mathbb{Q}(\alpha)$

some $n \in \mathbb{N}$. (Note: This implies ... α
larger field than L.)

pf: Suppose $L = \mathbb{Q}(\alpha)$

$[L : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}]$

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

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

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

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

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

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

$\Rightarrow L'$ is Galois over $\mathbb{Q}$ and

$\mathbb{Q} \subseteq L \subseteq L'$

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

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

$[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = 3$

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

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

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

$\alpha_1, \alpha_2 \in \mathbb{Q}(\alpha_1, \alpha_2)$

$\Rightarrow \alpha_3 \in \mathbb{Q}(\alpha_1, \alpha_2)$

---

35. Construct a finite field of 16 elements.

Consider $\mathbb{F}_2[x]$ and x^4+x+1

x^4+x+1 is irreducible in $\mathbb{F}_2[x]$

By x^4+x+1 has no roots in $\mathbb{F}_2$

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

$\mathbb{F}_2[x]/(x^4+x+1) \cong \underbrace{\mathbb{F}_2(\alpha)}$

is a field with basis
$\{1, \alpha, \alpha^2, \alpha^3\}$ over field $\mathbb{F}_2$

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)

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

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

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

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

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

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

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

$- \quad 5$

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

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

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

$\Rightarrow \exists t$ 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 need 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 $\mathbb{Z}[\sqrt{2}]/(5) \ni \bar{a}+\bar{b}\sqrt{2}$, then 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 $a \in \mathbb{F}_p$ s.t. each subfield of $\mathbb{F}_{p^n}$ is of the form $\mathbb{F}_p(a^l)$ for one natural number l.

What we have: $\mathbb{F}_{p^n}$ is the splitting field of $x^{p^n} - x$

And $\mathbb{F}_{p^n}$ is Galois over $\mathbb{F}_p$

And $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$

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

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

Then consider $ev_\gamma : \mathbb{F}_p[x] \to \mathbb{F}_{p^n}$

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 $ev_\gamma : \mathbb{F}_p[x] \to \mathbb{F}_{p^n}$ is onto

And $\mathbb{F}_p[x]/\ker ev_\gamma \cong \mathbb{F}_{p^n}$

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

And $\mathbb{F}_p(x)$ is a P.I.D

$\Rightarrow$ ker ev_γ is a maximal ideal

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

$\Rightarrow$ ker ev_γ 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 any 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 $\langle\beta\rangle = (F_{p^d})^\times$

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

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

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

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

Question: How to get l?

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

---

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

Call splitting field L, if $f(x)$ is irreducible, consider α be a root,

then $[F_p(\alpha) : F_p] = 6$

Then one can show α is the solution of $x^{p^6} - x$

Indeed, all elements in $F_p(\alpha)$ are the solutions of $x^{p^6} - x$

And, we know that $f(x) \mid x^{p^6} - x$ by $f(x)$ can be treated as minimal polynomial

And $x^{p^6} - x$ splits in $F_p(\alpha)$

$\Rightarrow$ $f(x)$ is splits in $F_p(\alpha)$

Then by definition, $L \subseteq F_p(\alpha)$

Also, by definition, $L = F_p(\alpha, \alpha_2, \cdots, \alpha_6)$

$\Rightarrow F_p(\alpha) \subseteq F_p(\alpha, \alpha_2, \cdots, \alpha_6)$

$\Rightarrow$ $L = F_p(\alpha) \Rightarrow [L : F_p] = 6$ is the splitting field of
($F_p(\alpha)$ is just the splitting field of $f(x)$ over F_p)

Then suppose $f(x)$ is reducible: $f(x) = 5+1$ in the form of irreducibles

$f(x) = 4+1+1$

$f(x) = 3+1+1+1$

$f(x) = 2+1+1+1$

$f(x) = 1+1+1+1+1$

This can be show that the degree of splitting field are $5, 4, 3, 2, 1$

$$\begin{cases} f(x) = 4+2 \\ f(x) = 3+3 \\ f(x) = 3+2 \\ f(x) = 2+2+2 \\ f(x) = 2+2 \end{cases}$$

Case 1: $f(x) = 4+2$, then $f(x) = \overset{4}{g_1(x)}\overset{2}{g_2(x)}$ s.t. $g_1(x), g_2(x)$ are irreducibles

Then since $g_1(x), g_2(x)$ don't have the same root.

(Otherwise it contradicts with the uniqueness of minimal polynomial)

Let's say L_1 be the splitting field of $g_1(x)$,

L_2 be the splitting field of $g_2(x)$,

Then $L_1 \cong F_{p^4}$

$L_2 \cong F_{p^2}$

$\Rightarrow L_2 \subseteq L_1$ by $2|4$

$\Rightarrow g_2(x)$ splits in F_{p^4}

$\Rightarrow$ Splitting field is F_{p^4}

Case 2: $f(x) = 3+3$, if $g_1(x) = g_2(x)$, then $L = F_{p^3}$

Otherwise, by similar method, one can show that $L = F_{p^3}$ still.

Case 3: $3+2$

Notice F_{p^2} is not a subfield of F_{p^3} since $2 \nmid 3$

$\Rightarrow$ The splitting field has degree 6

Case 4: $2+2+2$,

Then still F_{p^2}

Case 5: $2+2$, F_{p^2}

b) Compute the number of elements in the set $\{\beta \in F_{p^6} \mid F_p(\beta) = F_{p^6}\}$. (Hint: It will be useful to compute the number of distinct monic irreducible polynomials of degree 6 in $F_p[x]$).

From 39, one can show that the generator of $(F_{p^6})^\times$ can be β

$\Rightarrow$ There are at least $\varphi(p^6) = p^6 - p^5$.

From part a) we can see that, if $f(x)$ is a irreducible polynomial with degree 6, then the root α of of $f(x)$

$F_p(\alpha) \cong F_{p^6}$

So We need to know the irreducible number of distinct monic irreducible polynomial of degree 6 in $F_p[x]$.

$x^6 + a_5x^5 + a_4x^4 + \cdots + a_1x + a_0$

It's not the end of this question, see Field exercise 3, this answer maybe incorrect