510A HW4 Tempted Solutions

Haosen Wu

Nov. 14 2018

1. Suppose $F := \mathbb{F}_p$ is a finite field of order p. Consider the extension $E := \mathbb{F}_{p^n}/\mathbb{F}_p$. In this problem, we will compute this Galois group (check that the extension is Galois).

   - Show that the map $x \mapsto x^p$ is a field isomorphism fixing $\mathbb{F}_p$ pointwise; we will write Fr_p for the corresponding element of $Gal(E/F)$.
   - Determine the order of $Gal(E/F)$.
   - Show that Fr_p has order at least n in $Gal(E/F)$ and is a cyclic generator of $Gal(E/F)$.
   - Conclude that the subfields of $\mathbb{F}_{p^n}$ have order p^d where $d|n$ and there is 1 such subgroup for each such d.

   Answer. *Define* $\sigma := x \to x^p$.

   Proof of claim (All finite field extensions are Galois): The extension is Galois, followed from normality and separability. Enough to show that from $E = \mathbb{F}_p[x]/(x^{p^n} - x)$. *This polynomial has no repeated roots: formal derivative of* $\delta(x^{p^n} - x) = -1$ *reveals that; Equivalently to say the polynomial splits is that any* $y \in \mathbb{F}_p$, $y \in ker(ev(x^{p^n} - x))$, *henceforth revoking* $\mathbb{F}_{p^n}^*$ *is cyclic thus* $y^{p^n - 1} = 1$. *then* $y^{p^n} - y = y - y = 0$. *Above satisfies the normality and separability.*

   i) *It being a homomorphism follows from freshmen's dream:* $(x + y)^p = x^p + y^p$. *The kernel is trivial since only* 0 *has its power* 0. *Surjectivity follows from that mapping is between finite underlying sets.*
   Consider $x^p = x^{p-1}x$, *we know that* $\mathbb{F}_p^*$ *is cyclic thus for* $x \in \mathbb{F}_p$, $x^p = id_F x = x$. *We thus proved* Fr_p *is an* $\mathbb{F}_p$*-automorphism.*

   ii) $Gal(E/F) = Aut_F E = [E : F]$, *therefore the order is the* n, *as we know that* $\mathbb{F}_{p^n}/\mathbb{F}_p = \bigoplus_n \mathbb{F}_p$ *with* n*-copies (from notes).*
   (If assume iii), $Gal(E/F)$ *is proved to be cyclic generated with element order at least n, then* $Gal(E/F) = n$

   iii) *We have showed* $\mathbb{F}_p \subset \mathbb{F}_{p^n}^{\langle\sigma\rangle}$, *and the element fixed by* σ *has to satisfy* $x^p = x$, *that we have* p *solutions, thus* $\mathbb{F}_p = \mathbb{F}_{p^n}^{\langle\sigma\rangle}$; *that is equivalent to* Fr_p *has order* n. *Since* Fr_p *has order* n *and* $Gal(E/F) = n$, *it can only be the case* Fr_p *generates the group and thus our* $Gal(E/F)$ *is cyclic.*

iv) As subfield $\mathbb{F}_{p^d}$ satisfy $[\mathbb{F}_{p^n} : \mathbb{F}_{p^d}][\mathbb{F}_{p^d} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_p]$ thus $d|n$. The extension is Galois thus the second claim follows (from FToG): each of such p^d-subfield enjoys a corresponding subgroup. Moreover, the uniqueness follows from that element $y \in F_{p^d}$ are exactly the solution to $x^{p^d} - x = 0$, we know the equation has at most p^d elements, that says $F_{p^d} \subset F_{p^n}$ has to be unique.

2. Suppose $F := \mathbb{C}((t))$, i.e., the field of formal power series in 1 variable t over $\mathbb{C}$. For every integer $n \geq 1$, let $\mathbb{C}((t^{1/n}))$ be the field of formal power series in $t^{1/n}$. Show that $\mathbb{C}((t^{1/n}))/\mathbb{C}((t))$ is a Galois extension. If ζ_n is a primitive n-th root of unity, show that sending $t^{1/n} \mapsto \zeta_n t^{1/n}$ defines a cyclic generator of $Gal(\mathbb{C}((t^{1/n}))/\mathbb{C}((t)))$. (The field $\mathbb{C}((t))$ is some-times called a quasi-finite field for this reason).

Answer. *

i) $\mathbb{C}((t^{1/n}))/\mathbb{C}((t))$ is Galois: We try to argue the extension field splits on separable polynomial $p(x) = x^n - t = 0$, the polynomial has $\delta p(x) = nx^{n-1} = 0$ iff $x = 0$, sharing no repeated roots, therefore $p(x)$ is separable. Now we know explicitly roots of $p(x) = x^n - t = 0$ are $\zeta_n t^{1/n}$ where ζ_n is n-th primitive root. This polynomial therefore splits on $\mathbb{C}((t^{1/n}))$ since $t^{1/n}$ is adjoined and ζ_n is already in $\mathbb{C}$. We just need to show $\mathbb{C}((t^{1/n}))$ is the smallest such field: clearly $\mathbb{C}(t^{1/n}) \subset \mathbb{C}((t^{1/n}))$, any formal power series $\sum c_i (t^{1/n})^i$ can be written as linear combination of element $\mathbb{C}(t^{1/n})$. Thus the beginning criterion of Galois extension illustrates our extension is Galois.

ii) $|Gal(\mathbb{C}((t^{1/n}))/\mathbb{C}((t)))| = n$ since $x^n - t$ is minimal polynomial of $\zeta_n t^{1/n}$ and have degree n. We also notice that our automorphism is $(-) \to \zeta_n(-)$, but the power map as ζ_n^k also induces automorphisms of $\mathbb{C}((t^{1/n}))/\mathbb{C}((t))$ since they are new roots of unity. Thus such element has order n, which says $Gal(\mathbb{C}((t^{1/n}))/\mathbb{C}((t)))$ is a cyclic n-th order group.

3. Suppose F is a field and consider the field $F(x_1, \ldots, x_n)$, i.e., the field of rational functions in n variables over F. There is an action of the symmetric group S_n on $F(x_1, \ldots, x_n)$ by means of the formula

$$\sigma(f(x_1, \ldots, x_n)) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

A rational function $f \in K(x_1, \ldots, x_n)$ is called *symmetric* if $\sigma f = f$ for every $\sigma \in S_n$. Observe that constant rational functions are symmetric.

i) Define the functions e_i by the formulas:

$$e_j(x_1, \ldots, x_n) = \sum_{1 \leq i_1 \leq i_2 \leq \cdots \leq i_j \leq n} x_{i_1} x_{i_2} \cdots x_{i_j}.$$

Show that e_i are symmetric rational functions; they will be called elementary symmetric functions.

ii) Show that the map $S_n \to Aut_F(F(x_1, \ldots, x_n))$ sending σ to $\{f \mapsto \sigma f\}$ defines a homomorphism. Let $E = F(x_1, \ldots, x_n)^{S_n}$, which is a subfield of $F(x_1, \ldots, x_n)$ containing F. Show that $F(x_1, \ldots, x_n)/E$ is Galois extension with Galois group S_n.

iii) Show that if G is an arbitrary finite group, then there *exists* a Galois extension with Galois group isomorphic to G (hint: embed G in S_n).

Answer. *i)*

$$e_j(x_1, \ldots, x_n) = \sum_{1 \leq i_1 \leq i_2 \leq \cdots \leq i_j \leq n} x_{i_1} x_{i_2} \cdots x_{i_j}$$

was acted by σ_n, then

$$\sigma(e_j(x_1, \ldots, x_n)) = \sum_{1 \leq i_1 \leq i_2 \leq \cdots \leq i_j \leq n} x_{\sigma(i_1)} x_{\sigma(i_2)} \cdots x_{\sigma(i_j)}$$

So right hand side indeed ranges over all footnotes in {1,2,...,i}, then we realize that the application of σ_i will isomorphically act on the sub-polynomials, i.e., an i-th cycle induces an isomorphism on the i-th cycle subgroup in S_n due to the cyclic. Therefore the polynomial has no change as sum.

ii) For it to be a homomorphism, we want to show $\{f \to \sigma_1\sigma_2(f)\} = \{f \to \sigma_1 \circ \sigma_2(f)\}$ bababa. We also notice that f here is simply index tuple which cycles act on, then the last assertion follows from composition of cycles is their product. One equivalent formulation to say $F(x_1, \ldots, x_n)/E$ is Galois is that $F(x_1, \ldots, x_n)^{Aut(F(x_1,\ldots,x_n)/E)}$ is $E = F(x_1, \ldots, x_n)^{S_n}$, this is immediately to say $Gal(F(x_1, \ldots, x_n))/E) = Aut_E F = S_n$.

Previously we showed S_n can be embedded into the automorphism group of $F(x_1, \ldots, x_n)/F$ as a subgroup, at the meanwhile we already have $F \subset E \subset F(x_1, \ldots, x_n)$, since $F(x_1, \ldots, x_n)/E$ is an intermediate extension of $F(x_1, \ldots, x_n)/F$, thus since the largest extension is finite, we therefore invoke Artin theorem to show extension $F(x_1, \ldots, x_n)/E$ is Galois and then by previous formulation we have $Gal(F(x_1, \ldots, x_n)/E) = S_n$

iii) Embedding G to S_n through Cayley map $\rho : G \to S_n$ such that $\rho(G)$ is a subgroup of S_n; We now by ii) have $F(x_1, \ldots, x_n)/E$ Galois extension with Galois group S_n, now FToG gives an intermediate field extension of Galois (sub)group $\rho(G)$ with $F(x_1, \ldots, x_n) \supset L \supset E$. Now we only need to take $F(x_1, \ldots, x_n)/L$ to be the desired Galois extension.