

MATH 7752 Homework 11

James Harbour

April 29, 2022

Problem 1

In this problem you will need the following two definitions.

Definition 1: Let L/F be a finite separable extension and let \overline{F} be an algebraic closure of F containing L . A subfield L' of \overline{F} is called **conjugate to L over F** if $L' = \sigma(L)$ for some F -embedding $\sigma : L \rightarrow \overline{F}$. (Note: L/F is Galois if and only if the only conjugate to L over F is itself.)

Definition 2: A finite extension K/F is called a **p -extension** if K/F is **Galois** and $\text{Gal}(K/F)$ is a p -group.

(a): Let L/F be a separable extension of degree n and let K be the Galois closure of L over F . Prove that K can be written as a compositum $L_1 L_2 \cdots L_n$, where L_1, \dots, L_n are (not necessarily distinct) conjugates of L over F .

Proof. By the primitive element theorem, there exists some $\alpha \in L$ such that $L = F(\alpha)$. Let $\alpha_1, \dots, \alpha_n$ be the roots of $\mu_{\alpha, F}$ (all inside K as K/F is Galois). By the simple extension lemma, for each $i \in \{1, \dots, n\}$ the inclusion $F \subseteq \overline{F}$ extends to an F -embedding $\sigma_i : F(\alpha) \hookrightarrow \overline{F}$ such that $\sigma_i(\alpha) = \alpha_i$. Now set $L_i = \sigma_i(L) = \sigma_i(F(\alpha))$.

Then $L_1 \cdots L_n = F(\alpha_1, \dots, \alpha_n)$ is a splitting field for the separable polynomial $\mu_{\alpha, F}$ over F , whence $L_1 \cdots L_n/F$ is Galois. Thus by minimality of the Galois closure, $K \subseteq L_1 \cdots L_n$. On the other hand, as $\alpha_1, \alpha_n \in K$, it follows that $L_1 \cdots L_n = F(\alpha_1, \dots, \alpha_n) \subseteq K$. Thus $K = L_1 \cdots L_n$. \square

(b): Let K/F and L/F be finite p -extensions. Prove that KL/F is also a p -extension.

Proof. By homework 10 problem 4 part (ii), KL/F is finite Galois and we have an injective group homomorphism $\iota : \text{Gal}(KL/F) \hookrightarrow \text{Gal}(K/F) \times \text{Gal}(L/F)$. As both $\text{Gal}(K/F)$ and $\text{Gal}(L/F)$ are finite p -groups, it follows then that $\text{Gal}(KL/F) \cong \iota(\text{Gal}(KL/F)) \subseteq \text{Gal}(K/F) \times \text{Gal}(L/F)$ is a finite p -group. \square

(c): Suppose that K/L and L/F are both p -extensions, and let M be the Galois closure of K over F (note: we do not know whether K/F is Galois or not). Prove that M/F is also a p -extension.

Proof. By part (a), $M = K_1 \cdots K_n$ for some conjugates K_i of K over F . Then for $i \in \{1, \dots, n\}$, there is some F -embedding $\sigma_i : K \hookrightarrow \overline{F}$ such that $K_i = \sigma_i(K)$. By normality of L/F , $\sigma_i(L) = L$. Thus each extension K_i/L is F -isomorphic to K/L via σ_i and is thus a p -extension. Now by part (b), $M/L = K_1 \cdots K_n/L$ is a p -extension, whence we observe that

$$|\text{Gal}(M/F)| = [M : F] = [M : L][L : F] = |\text{Gal}(M/L)| \cdot |\text{Gal}(L/F)|$$

implies that M/F is also a p -extension. \square

(d): Now assume only that L/F is a separable extension with $[L : F] = p^r$, for some $r \geq 1$. Let M be the Galois closure of L over F . Prove that $[M : F]$ need not be a power of p .

Proof. Consider the example $L/F = \mathbb{Q}(\sqrt[p^r]{2})/\mathbb{Q}$. Then $M = \mathbb{Q}(\sqrt[p^r]{2}, \zeta_{p^r})$ where ζ_{p^r} is a primitive p^r th root of unity. On one hand $[\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}] = \varphi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)/2$ is not a power of p . On the other hand, $p^{r-1}(p-1)/2 = [\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}] \mid [M : \mathbb{Q}]$, so it follows that $[M : \mathbb{Q}]$ is not a power of p . \square

Problem 2

Let $f(x)$ and $g(x)$ be irreducible polynomials in $\mathbb{F}_p[x]$ of the same degree. Let $F = \mathbb{F}_p[x]/(f(x))$. Prove that $g(x)$ splits completely over F .

Proof. By a vector space counting argument, $|F| = p^n$. By uniqueness of splitting fields, F is \mathbb{F}_p -isomorphic to \mathbb{F}_{p^n} which is \mathbb{F}_p -isomorphic to $\mathbb{F}_p[x]/(q(x))$ which contains a root of $q(x)$. Thus, F contains a root of $q(x)$ whence by normality of the extensions F/\mathbb{F}_p , $q(x)$ splits over F . \square

Problem 3

Consider the polynomial $f(x) = x^4 - 2x^2 - 5 \in \mathbb{Q}[x]$.

(a): Determine the Galois group G of the splitting field K of $f(x)$ over \mathbb{Q} .

Proof. Let $\alpha = \sqrt{1 + \sqrt{6}}$ and $\beta = \sqrt{1 - \sqrt{6}}$. Then $f(x) = (x - \alpha)(x + \alpha)(x - \beta)(x + \beta)$ and $K = \mathbb{Q}(\alpha, \beta)$. Noting that $\alpha^2 + \beta^2 = 2$, it follows that $\mu_{\beta, \mathbb{Q}(\alpha)} = x^2 + (\alpha^2 - 2)$ and thus $[K : \mathbb{Q}(\alpha)] = 2$. Note that $f(x)$ is irreducible as none of the choices of pairs of linear factors provide a polynomial in $\mathbb{Q}[x]$ by appealing to Vieta's formulae and the fact that $\alpha^2, \beta^2, \alpha \pm \beta \notin \mathbb{Q}$. Hence, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ and thus $|G| = [K : \mathbb{Q}] = 8$.

Letting $\alpha_1 = \alpha$, $\alpha_2 = -\alpha$, $\alpha_3 = \beta$, $\alpha_4 = -\beta$, it follows that the action of G on $\{\alpha_1, \dots, \alpha_4\}$ induces an injective group homomorphism $\rho : G \hookrightarrow S_4$. Thus $G \cong \rho(G) \subseteq S_4$ is an order 8 subgroup of S_4 , all of which are isomorphic to D_4 so $G \cong D_4$. \square

(b): Find all subgroups of G and their corresponding fixed fields. Which of those are normal extensions of \mathbb{Q} ?

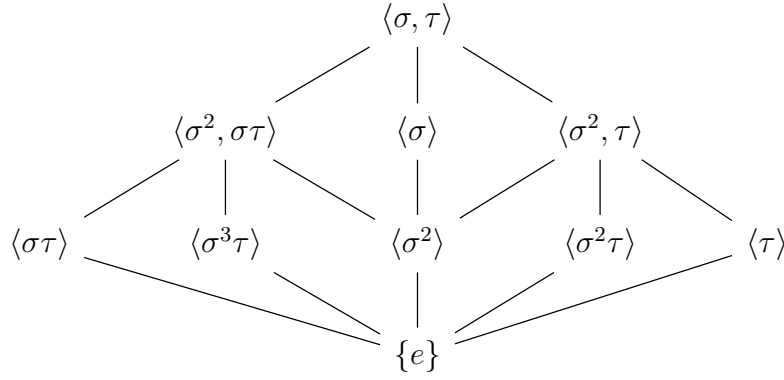
Solution. Let $\alpha_1, \dots, \alpha_4$ and ρ be as in part (a). Set $\gamma = \alpha\beta = \sqrt{-5}$. Note that if $\sigma \in G$, then $\sigma(\alpha), \sigma(\gamma)$ are roots of the minimal polynomials of α and γ respectively, whence $\sigma(\alpha) \in \{\alpha_1, \dots, \alpha_4\}$ and $\sigma(\gamma) \in \{\pm\gamma\}$. Moreover, as $K = \mathbb{Q}(\alpha, \gamma)$, the images of α and γ completely determine the \mathbb{Q} -automorphism σ . Since there are only 8 such choices of images and $|G| = 8$, it follows that G contains automorphisms with all possible images of these elements.

Let $\sigma, \tau \in G$ such that

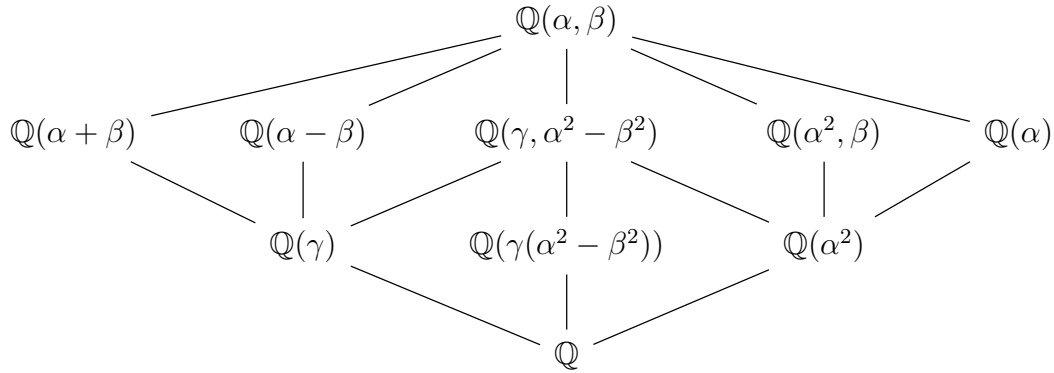
$$\begin{aligned} \sigma(\alpha) &= \beta & \tau(\alpha) &= \alpha \\ \sigma(\gamma) &= -\gamma & \tau(\gamma) &= -\gamma. \end{aligned}$$

Then $\rho(\sigma) = (1324)$ and $\rho(\tau) = (34)$. Moreover, $\rho(\tau\sigma\tau) = \rho(\sigma)^{-1}$. Thus, ρ, σ generate G and satisfy the relations defining D_4 .

For the subgroup diagram, we have



with its corresponding subfield diagram



$\sigma\tau(\alpha + \beta) = \alpha + \beta$, so $\alpha + \beta \in K^{\langle \sigma\tau \rangle}$. As $[K : K^{\langle \sigma\tau \rangle}] = |\langle \sigma\tau \rangle| = 2$, $[K^{\langle \sigma\tau \rangle} : F] = 4$, so $K^{\langle \sigma\tau \rangle} = F(\alpha + \beta)$. Using identical reasoning, we also conclude that $K^{\langle \sigma^3\tau \rangle} = F(\alpha - \beta)$.

$\sigma^2(\alpha\beta) = \alpha\beta$ and $\sigma\tau(\alpha\beta) = \alpha\beta$, so $\gamma \in K^{\langle \sigma^2, \sigma\tau \rangle}$. By degree constraints, $K^{\langle \sigma^2, \sigma\tau \rangle} = F(\gamma)$.

$\tau(\alpha) = \alpha$, so $\alpha \in K^{\langle \tau \rangle}$. By degree constraints, $K^{\langle \tau \rangle} = F(\alpha)$, and likewise $K^{\langle \sigma^2, \tau \rangle} = \mathbb{Q}(\alpha^2)$.

α^2, β are both fixed by $\langle \sigma^2\tau \rangle$, so degree constraints force $K^{\langle \sigma^2\tau \rangle} = F(\alpha^2, \beta)$.

Note that $\sigma(\gamma(\alpha^2 - \beta^2)) = \sigma(\gamma)(\sigma(\alpha^2) - \sigma(\beta^2)) = -\gamma(\beta^2 - \alpha^2) = \gamma(\alpha^2 - \beta^2)$, so $\gamma(\alpha^2 - \beta^2) \in K^{\langle \sigma \rangle}$. We compute that $\gamma(\alpha^2 - \beta^2) = 2\sqrt{-30}$, which is clearly of degree 2 over \mathbb{Q} , so degree constraints give that $K^{\langle \sigma \rangle} = \mathbb{Q}(\gamma(\alpha^2 - \beta^2))$.

Lastly $\sigma^2(\gamma) = \gamma$, $\sigma^2(\alpha^2 - \beta^2) = \alpha^2 - \beta^2$, so $\gamma, \alpha^2 - \beta^2 \in K^{\langle \sigma^2 \rangle}$. Both elements are degree 2 over \mathbb{Q} and only one is complex, so $\gamma \notin \mathbb{Q}(\alpha^2 - \beta^2)$ implies that $[\mathbb{Q}(\gamma, \alpha^2 - \beta^2) : \mathbb{Q}] = 4$. Thus, degree constraints force $K^{\langle \sigma^2 \rangle} = \mathbb{Q}(\gamma, \alpha^2 - \beta^2)$. \square

Problem 4

Let p and q be distinct primes with $q > p$, and let K/F be a Galois extension of degree pq . Prove the following:

(a): There exists a field L with $F \subset L \subset K$ and $[L : F] = q$.

Proof. Let $G = \text{Gal}(K/F)$. Then $|G| = pq$, whence by Sylow's existence theorem there is some subgroup $H \subseteq G$ such that $|H| = p$. Setting $L = K^H$, by the fundamental theorem of Galois theory, $p = |H| = [K : K^H]$ whence $[K^H : F] = q$ as desired. \square

(b): There exists a **unique** field M with $F \subset M \subset K$ and $[M : F] = p$.

Proof. Let $G = \text{Gal}(K/F)$. Let n_q denote the number of Sylow q -subgroups of G . Then as $n_q \mid p$ and $n_q \equiv 1 \pmod{q}$, the restriction that $q > p$ forces $n_q = 1$. Thus there is a unique subgroup of G of order q , whence by the fundamental theorem of Galois theory there is a unique intermediate subfield $M = K^Q$ of K/F with $[K : M] = q$ or equivalently $[M : F] = p$. \square

Problem 5

Prove the following analogue of K ummer's theorem for abelian extensions: Let $n \in \mathbb{N}$ and let F be a field containing a primitive n^{th} root of unity.

(a): Let K/F be a finite Galois extension such that $G = \text{Gal}(K/F)$ is abelian of exponent n . Then there exists $a_1, \dots, a_t \in F$ such that $K = F(\sqrt[n]{a_1}, \dots, \sqrt[n]{a_t})$. More precisely, there exists $\alpha_1, \dots, \alpha_t \in K$ such that $K = F(\alpha_1, \dots, \alpha_t)$ and $\alpha_i^n \in F$ for all i .

Proof. Write $G \cong C_{n_1} \times \dots \times C_{n_t}$ where $n_i \in \mathbb{N}$ and $C_{n_i} = \mathbb{Z}/n_i\mathbb{Z}$. For $j \in \{1, \dots, t\}$, set $G_j = \prod_{i \neq j} C_{n_i}$ and $K_j = K^{G_j}$. As $G_j \triangleleft G$, it follows that K_j/F is Galois and $\text{Gal}(K_j/F) \cong \text{Gal}(K/F)/\text{Gal}(K/K_j) = G/G_j \cong C_{n_j}$. Hence, by K ummer's theorem, there exists some $\alpha_j \in K_j$ such that $K_j = F(\alpha_j)$ and $\alpha_j^{n_j} \in F$, whence $\alpha_j^n = (\alpha_j^{n_j})^{n/n_j} \in F$.

Observe that

$$K = K^{\{e\}} = K^{\bigcap_{i=1}^t G_i} = K_1 K_2 \dots K_t = F(\alpha_1, \alpha_2, \dots, \alpha_t).$$

\square

(b): Conversely, suppose that $K = F(\sqrt[n]{a_1}, \dots, \sqrt[n]{a_t})$ for some $a_1, \dots, a_t \in F$. Prove that K/F is Galois and $G = \text{Gal}(K/F)$ is abelian of exponent n . **Hint:** For part (b) use one of the problems from the previous homework.

Proof. Write $\alpha_i = \sqrt[n]{a_i}$, so $\alpha_i^n = a_i$. As F contains a primitive n^{th} root of unity, K ummer's theorem implies that each $F(\alpha_i)/F$ is Galois with $\text{Gal}(F(\alpha_i)/F) \cong \mathbb{Z}/n_i\mathbb{Z}$ for some $n_i \mid n$. Applying homework 10 problem 4(b) part(ii) iteratively, we obtain an embedding

$$\iota : \text{Gal}(K/F) \hookrightarrow \prod_{i=1}^t \text{Gal}(F(\alpha_i)/F) \cong \prod_{i=1}^t \mathbb{Z}/n_i\mathbb{Z}$$

As the latter group has exponent dividing n , it follows that $\text{Gal}(K/F)$ has exponent dividing n . \square

Problem 6

Let F be a field containing a primitive n^{th} root of unity. Let $a, b \in F$ be such that the polynomials $f(x) = x^n - a$, and $g(x) = x^n - b$ are both irreducible over F . Consider the K ummer extensions $F(\alpha)$, $F(\beta)$, where α is a root of $f(x)$ and β is a root of $g(x)$. Prove that $F(\alpha) = F(\beta)$ if and only if $\beta = c\alpha^r$, for some $c \in F$ and some integer r which is coprime to n (equivalently, if and only if $b = c^n a^r$, for some $c \in F$ and some $(r, n) = 1$).

Proof.

\Leftarrow : Suppose that $\beta = c\alpha^r$, for some $c \in F$ and some integer r which is coprime to n . Note that we immediately have the equality and inclusion $F(\beta) = F(c\alpha^r) = F(\alpha^r) \subseteq F(\alpha)$, thus it suffices to show that $[F(\alpha) : F(\alpha^r)] = |\text{Gal}(F(\alpha)/F(\alpha^r))| = 1$. We will show that the Galois group of this extension is trivial.

Suppose that $\sigma \in \text{Gal}(F(\alpha)/F(\alpha^r))$. Let ζ be a primitive n^{th} root of unity. Noting that $\sigma(\alpha)$ is also a root of $f(x)$ (since $f(x)$ is irreducible), it follows that $\sigma(\alpha) = \zeta^k \alpha$ for some $0 \leq k \leq n-1$. Observe that

$$\alpha^r = \sigma(\alpha^r) = (\zeta^k \alpha)^r \implies \alpha^r (\zeta^{kr} - 1) = 0 \implies \zeta^{kr} - 1 = 0,$$

so $(\zeta^r)^k = 1$. As r is coprime to n , we have that ζ^r is also a primitive n^{th} root of unity, whence $n \mid k$. As $0 \leq k \leq n-1$, it must hold that $k = 0$, so $\sigma(\alpha) = \alpha$ whence $\sigma = \text{id}$ as desired.

\Rightarrow : Suppose that $F(\alpha) = F(\beta)$. Then $G = \text{Gal}(F(\alpha)/F) = \text{Gal}(F(\beta)/F)$. By Kummer's theorem and irreducibility of f and g , G is cyclic of order n . Let $G = \langle \sigma \rangle$ and ζ is a primitive n^{th} root of unity. Then there exist $r, s \in \mathbb{N}$ both coprime to n such that $\sigma(\alpha) = \zeta^r \alpha$ and $\sigma(\beta) = \zeta^s \beta$. As ζ^r and ζ^s are both also primitive n^{th} roots of unity, there is some $k \in \mathbb{N}$ coprime to n such that $\zeta^s = (\zeta^r)^k$. Then, we observe that

$$\frac{\sigma(\beta)}{\beta} = \zeta^s = (\zeta^r)^k = \left(\frac{\sigma(\alpha)}{\alpha} \right)^k \implies \sigma \left(\frac{\beta}{\alpha^k} \right) = \frac{\beta}{\alpha^k}$$

thus $c = \frac{\beta}{\alpha^k}$ is fixed by G so $c \in F$. Thus $\beta = c\alpha^k$ for some $c \in F$ and k coprime to n . □