MATH 7752 Homework 10

James Harbour

April 17, 2022

Problem 1

Let F be a field, $f(x) \in F[x]$ be an irreducible separable polynomial over F of degree n and let K be a splitting field of $f(x)$.

(a): Prove that $|\operatorname{Gal}(K/F)|$ is a multiple of n and divides $n!$.

Proof. By separability, $[K : F] = |\operatorname{Gal}(K/F)|$. Let $\alpha \in K$ be a root of f. By irreducibility of f, $f = \mu_{\alpha,F}$ whence

$$|\operatorname{Gal}(K/F)| = [K : F] = [K : F(\alpha)][F(\alpha) : F] = [K : F(\alpha)] \deg(\mu_{\alpha,F}) = [K : F(\alpha)] \cdot n,$$

so $n \mid |\operatorname{Gal}(K/F)|$.

To see that $|Gal(K/F)|$ divides $n!$, note as K is the splitting field of irreducible f of degree n, we have an injective group homomorphism $\rho : \operatorname{Gal}(K/F) \hookrightarrow S_n$ induced by a labeling of the roots of f. □

(b): Let $n = 3$. Prove that $\operatorname{Gal}(K/F)$ is isomorphic to either $\mathbb{Z}/3\mathbb{Z}$ or S_3.

Proof. Let $G = \operatorname{Gal}(K/F)$. By part (a), $3 \mid |G| = |\rho(G)|$ so by Sylow's existence theorem there is some subgroup $H \subseteq \rho(G)$ such that $|H| = 3$. Hence, there is some 3-cycle $\sigma \in H$ such that $H = \langle \sigma \rangle$.

If $\rho(G) = H$, then $G \cong \mathbb{Z}/3\mathbb{Z}$ and we would be done.

Otherwise, suppose that $\rho(G) \neq H$. Then there exists some $\tau \in \rho(G) \setminus H$. This τ must be a 2-cycle by noting that H contains the identity and all of the 3-cycles in S_3. Noting that σ is a 3-cycle, τ is a transposition, and 3 is prime, it follows by elementary group theory that S_3 is generated by σ and τ. Thus $\rho(G) = S_3$, so $G \cong S_3$. □

(c): Let $n = 4$ and assume that $|\operatorname{Gal}(K/F)| = 8$. Determine the isomorphism class of $\operatorname{Gal}(K/F)$.

Proof. Noting that $|\rho(G)| = 8 = 2^3$, it follows that $\rho(G)$ is a Sylow 2-subgroup of S_4. As all Sylow subgroups for a fixed prime are isomorphic via conjugation (by Sylow's conjugate theorem), it suffices to determine the isomorphism class of one Sylow 2-subgroup of S_4. Noting that the natural embedding of D_8 into S_4 induced by a labeling of the vertices of the square upon which D_8 acts, it follows that the identified copy of D_8 inside S_4 is a Sylow 2-subgroup of S_4. Thus, all Sylow 2-subgroups of S_4 are isomorphic to D_8, whence $\operatorname{Gal}(K/F) \cong D_8$. □

Problem 2

Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree n, and let K be a splitting field of $f(x)$ contained in $\mathbb{C}$. Label the roots of $f(x)$ by $\alpha_1, \ldots, \alpha_n$ (in some order), and let $\rho : \mathrm{Gal}(K/\mathbb{Q}) \hookrightarrow S_n$ be the associated embedding.

(a): Assume that $f(x)$ has at least one non-real root. Prove that the complex conjugation gives an element τ of $\mathrm{Gal}(K/\mathbb{Q})$ of order 2. What can you say about τ if $f(x)$ has precisely two non-real roots?

Proof. Consider the $\mathbb{Q}$-embedding $\tau : K \hookrightarrow \overline{Q} \subseteq \mathbb{C}$ given by complex conjugation. By normality of $K/\mathbb{Q}$, it follows that $\tau(K) = K$, so $\tau \in \mathrm{Gal}(K/\mathbb{Q})$. As f has a non-real root, it follows that $\tau \neq id_K$. Thus, noting that $\tau^2 = id_K$, τ has order 2.

If f has precisely two non-real roots, as $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on the set of roots of f and fixes all of the real roots it follows that the two non-real roots say α_1 and α_2 are complex conjugates of each other. In this case, $\rho(\tau)$ is in fact a single transposition. □

(b): Suppose that the degree n of $f(x)$ is a prime number, and that $f(x)$ has precisely two non-real roots. Prove that $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to S_n. **Hint:** You might need to recall some facts from Algebra I about generators of S_n.

Proof. Let $p = n$ be a prime number. Let $G = \mathrm{Gal}(K/\mathbb{Q})$. By problem 1 part (a), $p \mid |\rho(G)| \mid p!$, whence by Sylow's theorem there exists a subgroup $H \subseteq \rho(G)$ such that $|H| = p$. This subgroup is cyclic of order p, so there exists a p-cycle $\sigma \in H$ such that $H = \langle \sigma \rangle$. Let $\tau \in \rho(G)$ be as in part (a). Then $\tau \notin H$ as all elements of H are either the identity or have order p.

As τ is a transposition, σ is a p-cycle, and p is prime, it follows that $\S_p = \langle \sigma, \tau \rangle \subseteq \rho(G)$ whence $\rho(G) = S_p$, so $G \cong S_p$. □

Problem 3

Let K be the splitting field of $f(x) = x^4 - 2 \in \mathbb{Q}[x]$.

(a): Choose an order on the set of roots of $f(x)$ and describe the associated embedding $\mathrm{Gal}(K/\mathbb{Q}) \hookrightarrow S_4$. (You can use the information you obtained in Homework 8).

Proof. Let $\zeta = e^{2\pi i/4} = i$ and $\alpha_j = \zeta^{j-1}\sqrt[4]{2}$ for $1 \leq j \leq 4$. Then $f(x) = (x - \alpha_1) \cdots (x - \alpha_4)$ and $K = F(\alpha_1, \ldots, \alpha_4) = F(\sqrt[4]{2}, i)$.

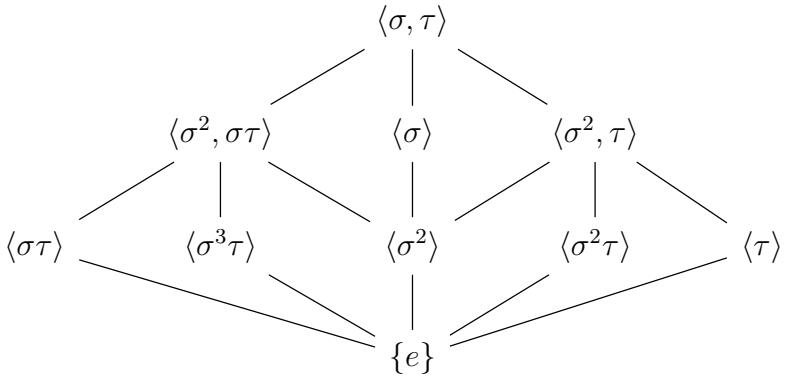
As $\deg_{\mathbb{Q}(\sqrt[4]{2})}(i) = \deg_{\mathbb{Q}}(i)$, it follows by the explicit description of Galois groups that there exist $\sigma, \tau \in \mathrm{Gal}(K/\mathbb{Q})$ such that

$$\sigma(\sqrt[4]{2}) = \zeta\sqrt[4]{2} \qquad \tau(\sqrt[4]{2}) = \sqrt[4]{2}$$
$$\sigma(\zeta) = \zeta \qquad \tau(\zeta) = \zeta^3.$$

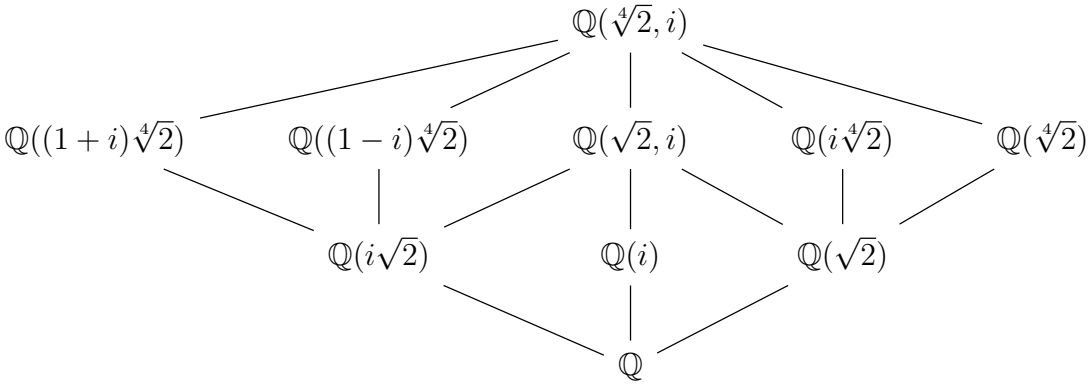
Letting $\rho : \mathrm{Gal}(K/\mathbb{Q}) \hookrightarrow S_4$ be the embedding associated to the aforementioned labeling of the roots of f, it follows that $\rho(\sigma) = (1234)$ and $\rho(\tau) = (24)$. The subgroup of S_4 generated by these two elements is an isomorphic copy of D_8, so it follows from the fact that $[K : \mathbb{Q}] = 8$ that $\mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma, \tau \rangle$, whence these values of ρ completely determine the embedding. □

(b): Describe all subgroups of $\mathrm{Gal}(K/\mathbb{Q})$ and the corresponding subfields of K.

Proof. For the subgroup diagram, we have



with its corresponding subfield diagram



where correspondence between subgroups and subfields is depicted via vertically flipping one of the diagrams. The majority of these fields were found via direct computation of fixed fields; however, those corresponding to $\langle \sigma\tau \rangle$ and $\langle \sigma^3\tau \rangle$ require more work.

First, we compute that $\rho(\sigma\tau) = (12)(34)$ and $\rho(\sigma^3\tau) = (14)(23)$. Thus, $\alpha_1 + \alpha_2 \in K^{\langle \sigma\tau \rangle}$ and $\alpha_1 + \alpha_4 \in K^{\langle \sigma^3\tau \rangle}$. We claim that in fact $K^{\langle \sigma\tau \rangle} = \mathbb{Q}(\alpha_1 + \alpha_2)$ and $K^{\langle \sigma^3\tau \rangle} = \mathbb{Q}(\alpha_1 + \alpha_4)$. Noting that $\alpha_1 + \alpha_2$ and $\alpha_1 + \alpha_4$ are both roots of the irreducible polynomial $x^4 + 8$, it follows that

$$[K : \mathbb{Q}(\alpha_1 + \alpha_2)] = 2 = |\langle \sigma\tau \rangle| = [K : K^{\langle \sigma\tau \rangle}]$$

and

$$[K : \mathbb{Q}(\alpha_1 + \alpha_4)] = 2 = |\langle \sigma^3\tau \rangle| = [K : K^{\langle \sigma^3\tau \rangle}]$$

whence the claim follows by the inclusions.

□

Problem 4

Let K/F and L/F be field extensions.
(a): Assume that L/F is finite Galois. Show that KL/K is also Galois.

Proof. As L/F is finite Galois, there is some separable $f \in F[x]$ such that L is a splitting field for f. Note that f is separable in $K[x]$. We claim that KL is a splitting field for f over K. As f splits over L, it splits over KL. Now suppose that f splits over some field E with $K \subseteq E$. Then, since L is a splitting field for f over F in KL, we have by minimality that $L \subseteq E$. Then by minimality of KL, as $K, L \subseteq E$, it follows that $KL \subseteq E$. Thus KL is a splitting field for a separable polynomial f over K, whence KL/K is Galois. □

Now suppose that both K/F and L/F are Galois extensions.

(b): Prove that the extension KL/F is also Galois and there is a natural embedding $\iota : \mathrm{Gal}(KL/F) \to \mathrm{Gal}(K/F) \times \mathrm{Gal}(L/F)$.

Proof. Fix an algebraic closure $\overline{F}$ of F. Suppose that $\sigma : KL \hookrightarrow \overline{F}$ is an embedding. Then by normality of K/F and L/F, it follows that $\sigma|_K(K) = K$ and $\sigma|_L(L) = L$, whence $\sigma(KL) = \sigma(K)\sigma(L) = KL$, so KL/F is normal.

Noting that K, L are separable over F and $KL = F(K \cup L)$, it follows that KL is separable over F, so the extension KL/F is Galois.

Define an embedding $\iota : \mathrm{Gal}(KL/F) \hookrightarrow \mathrm{Gal}(K/F) \times \mathrm{Gal}(L/F)$ by $\iota(\sigma) = (\sigma|_K, \sigma|_L)$. This mapping is well-defined as the normality of K/F and L/F forces $\sigma|_K(K) = K$ and $\sigma|_L(L) = L$. Compositiong is clearly respected, so this map is a group homomorphism. Lastly, if $\iota(\sigma) = (id_K, id_L)$, then $\sigma|_K = id_K$ and $\sigma|_L = id_L$ whence $\sigma = id$, so ι is indeed an embedding. □

(c): Assume now that K/F and L/F are both finite. Prove that the map ι in part (i) is an isomorphism if and only if $K \cap L = F$.

Proof.
$\underline{\Longrightarrow}$: Suppose that ι is an isomorphism. Then,

$$[KL : F] = |\,\mathrm{Gal}(KL/F)| = |\,\mathrm{Gal}(K/F)| \cdot |\,\mathrm{Gal}(L/F)| = [K : F][L : F].$$

Now, by homework 7 problem 6 part (b), we have that $K \otimes_F L$ is a field. Thus, the contrapositive of homework 7 problem 6 part (c) gives that $K \cap L = F$.

$\underline{\Longleftarrow}$: Suppose that $K \cap L = F$. By the theorem of natural irrationalities, $\mathrm{Gal}(KL/K) \cong \mathrm{Gal}(L/K \cap L) = \mathrm{Gal}(L/F)$. Thus,

$$|\,\mathrm{Gal}(KL/F)| = [KL : F] = [KL : K][K : F] = [L : F][K : F] = |\,\mathrm{Gal}(K/F)| \cdot |\,\mathrm{Gal}(L/F)|$$

so finiteness gives that ι is surjective. □