GALOIS THEORY 2019: HW 5 SOLUTIONS

For assessment: Problems 1, 2, 3

Due by noon Tuesday, week 11 of the term

Note: comments in square brackets [such as these] are not necessary for a complete solution on an exam.

1. (This is part of the proof of Theorem 11.1(c) – TYPO: this should have said this is a part of the proof of Theorem 11.1(b) and (c).) Suppose that $L : K_0$ is a finite Galois extension with $G = Gal(L : K_0)$ and $H \lhd G$. We let ϕ, γ be the maps as defined in section 11 of the notes. Here you show that for any $\sigma \in G$, $\phi(H) = \sigma\phi(H)$ (which by Theorem 11.1(b) is equivalent to showing that for any $\sigma \in G$, $H = \gamma\sigma\phi(H)$).
   (a) Take $\sigma \in G$. Show that $\sigma\phi(H) \subseteq \phi(H)$.
   (b) Show that for $\sigma \in G$, we have $\sigma\phi(H) = \phi(H)$.

   Solutions:

   (a) Take $\alpha \in \phi(H)$. Take $\tau \in H$. Since $H \lhd G$, there is some $\rho \in H$ so that $\tau\sigma = \sigma\rho$; since $\rho \in H$ we have $\rho(\alpha) = \alpha$. Thus

   $$\tau(\sigma(\alpha)) = \sigma(\rho(\alpha)) = \sigma(\alpha).$$

   This holds for all $\tau \in H$, so for $\alpha \in \phi(H)$ we have $\sigma(\alpha) \in \phi(H)$, or in other words, $\sigma\phi(H) \subseteq \phi(H)$.

   (b) The argument above holds with σ replaced by σ^{-1}, giving us $\sigma^{-1}\phi(H) \subseteq \phi(H)$, and this gives us $\phi(H) \subseteq \sigma\phi(H)$. Since we already have $\sigma\phi(H) \subseteq \phi(H)$, we have $\sigma\phi(H) = \phi(H)$.

2. (This is a variation of a HW problem from 2014.) Let f denote the polynomial $t^3 - 7 \in \mathbb{Q}[t]$.
   (a) Find a splitting field extension $L : \mathbb{Q}$ for f.
   (b) Construct $Gal(L : \mathbb{Q})$; show that $Gal(L : \mathbb{Q}) \simeq S_3$ (where S_3 denotes the symmetric group on 3 letters).
   (c) Use the Fundamental Theorem of Galois Theory (Theorem 11.1) to find all subgroups H of $Gal(L : \mathbb{Q})$, and for each subgroup H, find $Fix_L(H)$, clearly explaining your reasoning. (It may be helpful to draw the lattice of subfields and corresponding lattice of subgroups of S_3.)

   Solutions:

   (a) Let $\zeta = e^{2\pi i/3} = \frac{1}{2}(-1 + \sqrt{-3}) \in \mathbb{C}$ be a primitive cube root of unity, and put $\alpha = \sqrt[3]{7} \in \mathbb{R}_+$. Then f splits as $(t-\alpha)(t-\zeta\alpha)(t-\zeta^2\alpha)$ over $\mathbb{C}$, and a splitting field for f is $L = \mathbb{Q}(\alpha, \zeta)$. [One can also show that $L = \mathbb{Q}(\sqrt[3]{7}, \sqrt{-3})$.]

   (b) Note that f is irreducible by Eisenstein's criterion. We know that $f = m_\alpha(\mathbb{Q})$, so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg f = 3$. We also know that ζ is a root of $(t^3 - 1)/(t - 1) = t^2 + t + 1$. As we have $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$ and $\zeta \notin \mathbb{R}$, we know that $\deg m_\zeta(\mathbb{Q}(\alpha)) > 1$ and $m_\zeta(\mathbb{Q}(\alpha))$ divides $t^2 + t + 1$; hence $m_\zeta(\mathbb{Q}(\alpha)) = t^2 + t + 1$. Thus

   $$[L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 3 = 6.$$

[Alternatively, we know that the Galois group is thus (isomorphic to) a transitive subgroup of S_3, and hence either S_3 or A_3. Arguing as above that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ and $[L : \mathbb{Q}(\alpha)] > 1$, we must have $Gal(L : \mathbb{Q}) \simeq S_3$.]

(c) Let $G = Gal(L : \mathbb{Q})$. Given that $m_\alpha(\mathbb{Q}) = t^3 - 7$ and $m_\zeta(\mathbb{Q}(\alpha)) = t^2 + t + 1$, we can build $\sigma \in G$ by first extending the identity map on $\mathbb{Q}$ to $\varphi : \mathbb{Q}(\alpha) \to L$ with $\varphi(\alpha) = \alpha\zeta$; this is possible since $\alpha\zeta$ is a root of $m_\alpha(\mathbb{Q})$. Then we can extend φ to $\sigma \in G$ by setting $\sigma(\zeta) = \zeta$; this is possible since ζ is a root of $\varphi(m_\zeta(\mathbb{Q}(\alpha)))$. Similarly, we build $\tau \in G$ by first extending the identity map on $\mathbb{Q}$ to $\varphi : \mathbb{Q}(\alpha) \to L$ with $\varphi(\alpha) = \alpha$; this is possible since α is a root of $m_\alpha(\mathbb{Q})$. Then we can extend φ to $\tau \in G$ by setting $\tau(\zeta) = \zeta^2$; this is possible since ζ^2 is a root of $\varphi(m_\zeta(\mathbb{Q}(\alpha)))$.

[Note: since we know (i) $G = Gal(L : \mathbb{Q})$ is isomorphic to a subgroup of S_3, (ii) every elements of G is determined by how it permutes the roots of f, and (iii) $|G| = |S_3|$, we can conclude that every permutation of the roots of f corresponds to an element of G. But in general, this is not true! So in this problem, either one has to make the oberservations (i), (ii), (iii), and then the conclusion as above, or one has to describe how to construct the elements of G.]

We find that σ has order 3, τ has order 2, and $\tau\sigma = \sigma^2\tau$ [this last equality we find by applying $\tau\sigma$ to α and to ζ]. As $|G| = 6$, every proper subgroup of G is cyclic. So the subgroups of G are $\{id\}$ (whose fixed field is L), G (whose fixed field is $\mathbb{Q}$), $H_1 = \langle\sigma\rangle$, $H_2 = \langle\tau\rangle$, $H_3 = \langle\sigma\tau\rangle$, $H_4 = \langle\sigma^2\tau\rangle$.

To find the fixed fields of each of the nontrivial, proper subgroups of G:
We know that $\mathbb{Q}(\alpha), \mathbb{Q}(\alpha\zeta), \mathbb{Q}(\alpha\zeta^2), \mathbb{Q}(\zeta)$ are fields that properly contain L and are properly contained in L; thus each of these must be $\phi(H_i)$ for some i. [Note: in other situations, it is not always obvious what all the intermediate fields are.] As $\sigma(\zeta) = \zeta$ and σ is a $\mathbb{Q}$-homomorphism [meaning that it fixes every element of $\mathbb{Q}$], we have $\mathbb{Q}(\zeta) \subseteq \phi(H_1)$. Also, $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2 = [G : H_1]$, so we must have $\mathbb{Q}(\zeta) = \phi(H_1)$. We know that $\tau(\alpha) = \alpha$, so (similar to what is above), we have $\mathbb{Q}(\alpha) \subseteq \phi(H_2)$. Since $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3 = [G : H_2]$, we have $\mathbb{Q}(\alpha) = \phi(H_2)$. [We now check: $\sigma\tau(\alpha\zeta) = \sigma(\alpha\zeta^2) = \alpha$, $\sigma^2\tau(\alpha\zeta) = \sigma^2(\alpha\zeta^2) = \sigma(\alpha) = \alpha\zeta$. Also, $\sigma\tau(\alpha\zeta^2) = \sigma(\alpha\zeta) = \alpha\zeta^2$.] As $\sigma\tau(\alpha\zeta^2) = \alpha\zeta^2$, we have $\mathbb{Q}(\alpha\zeta^2) \subseteq \phi(H_3)$, and $[\mathbb{Q}(\alpha\zeta^2) : \mathbb{Q}] = 3 = [G : H_3]$, we have $\mathbb{Q}(\alpha\zeta^2) = \phi(H_3)$. Similarly, we have $\sigma^2\tau(\alpha\zeta) = \alpha\zeta$, we have $\mathbb{Q}(\alpha\zeta) \subseteq \phi(H_4)$, and $[\mathbb{Q}(\alpha\zeta) : \mathbb{Q}] = 3 = [G : H_4]$, we have $\mathbb{Q}(\alpha\zeta) = \phi(H_4)$.

ALTERNATIVELY, to find the fixed fields of each of the nontrivial, proper subgroups of G:
We have $\alpha + \sigma\tau(\alpha) = \alpha + \alpha\zeta \in Fix_L(H_3)$, and $[L : \mathbb{Q}] > [\mathbb{Q}(\alpha + \alpha\zeta) : \mathbb{Q}] > 1$, so we must have $\mathbb{Q}(\alpha + \alpha\zeta) = Fix_L(H_3)$. [We know $\alpha + \alpha\zeta \notin \mathbb{R}$, but we made a leap here that $\alpha \notin \mathbb{Q}(\alpha + \alpha\zeta)$. Accepting this, by the Tower Law we must have $[\mathbb{Q}(\alpha + \alpha\zeta) : \mathbb{Q}] = 2$ or 3. To verify that $\alpha \notin \mathbb{Q}(\alpha + \alpha\zeta)$, we can compute $m_{\alpha+\alpha\zeta}(\mathbb{Q})$: remembering that

$m_\zeta(\mathbb{Q}) = t^2+t+1$, we see $(\alpha+\alpha\zeta)^2 = \alpha^2\zeta \notin \mathbb{Q}$ and $(\alpha+\alpha\zeta)^3 = -7$, so $m_{\alpha+\alpha\zeta}(\mathbb{Q})$ must divide t^3+7. Thus we have $[\mathbb{Q}(\alpha+\alpha\zeta) : \mathbb{Q}] = 3 = [G : H_3]$.] Similarly, we have $\alpha+\sigma^2\tau(\alpha) = \alpha+\alpha\zeta^2 \in Fix_L(H_4)$, and arguing as with H_4 in place of H_3, we get $Fix_L(H_4) = \mathbb{Q}(\alpha+\alpha\zeta^2)$.

[**Alternatively, to describe G and find the fixed fields of all the nontrivial, proper subgroups of G:** Write $\beta_1 = \alpha$, $\beta_2 = \zeta\alpha$, $\beta_3 = \zeta^2\alpha$, and consider the Galois group G of t^3-7, namely $\mathrm{Gal}(L : \mathbb{Q}) \cong S_3$. Since all possible permutations of roots must occur as automorphisms in G, we have in particular the automorphism σ that cyclically permutes the β_i, so that

$$\alpha \mapsto \zeta\alpha \quad \text{and} \quad \zeta \mapsto \zeta,$$

and also the permutation τ that interchanges two of the roots, leaving the third fixed, so that

$$\alpha \mapsto \alpha \quad \text{and} \quad \zeta \mapsto \zeta^2.$$

Notice that

$$G \cong \langle \sigma, \tau | \sigma^3 = \tau^2 = 1, \tau\sigma = \sigma^2\tau \rangle.$$

The fields L, and $\mathbb{Q}$, are the fixed fields of $\{id\}$, and G, respectively. As for the intermediate fields, we have the three cubic extensions $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\zeta\alpha)$ and $\mathbb{Q}(\zeta^2\alpha)$, corresponding to the subgroups $\langle\tau\rangle$, $\langle\sigma^2\tau\rangle$ and $\langle\sigma\tau\rangle$, respectively, of index 3 in G. Finally, the subgroup $\langle\sigma\rangle$ of index 2 in G fixes the quadratic extension $\mathbb{Q}(\zeta) = \mathbb{Q}(\sqrt{-3})$. One needs to justify this correspondence between the subgroups and their fixed fields, as done above.]

3. (Here you prove Theorem 12.2(a); this is similar to #4(b) on the 2016 exam.) Let p be a prime and $q = p^n$ where $n \in \mathbb{Z}_+$. Let $\mathbb{F}_p$ denote a field of order p, and let $\mathbb{F}_q$ denote a field of order q; recall that by Theorem 12.1, $\mathbb{F}_q : \mathbb{F}_p$ is a splitting field extension and $[\mathbb{F}_q : \mathbb{F}_p)] = n$. Assume that $\mathbb{F}_p \subseteq \mathbb{F}_q$.
   (a) Briefly explain why $\mathbb{F}_q : \mathbb{F}_p$ is a Galois extension.
   (b) Let ϕ denote the Frobenius map on $\mathbb{F}_q$. Show that $\langle\phi\rangle = Gal(\mathbb{F}_q : \mathbb{F}_p)$, and use this to show that $Gal(\mathbb{F}_q : \mathbb{F}_p) \simeq \mathbb{Z}/n\mathbb{Z}$.

   Solutions.

   (a) Since $\mathbb{F}_q : \mathbb{F}_p$ is a splitting field extension for $f = t^q - t$, it is a normal extension. Also, [by Theorem 12.1 (b)] each of the q elements of $\mathbb{F}_q$ are roots of f, and as f can have at most q roots, f has no repeated roots. So f is separable over $\mathbb{F}_p$, and hence $\mathbb{F}_q : \mathbb{F}_p$ is a separable extension; thus $\mathbb{F}_q : \mathbb{F}_p$ is a Galois extension.

   (b) We have $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$, so every element of $\mathbb{F}_p$ is fixed by ϕ. Also, [by Theorem 8.4] ϕ is injective, and since $\mathbb{F}_q$ is finite, ϕ is an automorphism of $\mathbb{F}_q$. So $\phi \in G = Gal(\mathbb{F}_q : \mathbb{F}_p)$. We also know that for any $\beta \in \mathbb{F}_q$, we have [by Theorem 12.1]

$$\beta = \beta^q = \beta^{p^n} = \phi^n(\beta).$$

[So the order of ϕ on $\mathbb{F}_q$ is bounded above by n.] Now let α be a generator of the cyclic group $\mathbb{F}_q^\times$. Thus for any $m \in \mathbb{Z}_+$ with $m < n$,

we have $1 \neq \alpha^{p^m-1}$ and so $\alpha \neq \alpha^{p^m} = \phi^m(\alpha)$. Hence the order of ϕ is n. Thus $\langle\phi\rangle \simeq \mathbb{Z}/n\mathbb{Z}$, a cyclic group of order n. Further, $|G| = [\mathbb{F}_q : \mathbb{F}_p] = n$ [using Theorem 10.4], so we musthave$\langle\phi\rangle = G$.

4. (Parts (a) and (b) are from #4(c), 2015 exam.) Let $L : \mathbb{Q}$ be a splitting field extension for $g(X) = X^4 - 5$.
   (a) Show that $[L : \mathbb{Q}] = 8$.
   (b) Describe the Galois group $Gal(L : \mathbb{Q})$; that is, give generators and relations.
   (c) Use the Fundamental Theorem of Galois Theory (Theorem 11.1) to find all subgroups H of $Gal(L : \mathbb{Q})$, and for each subgroup H, find $Fix_L(H)$, clearly explaining your reasoning. (It may be helpful to draw the lattice of subfields and corresponding lattice of subgroups of $Gal(L : \mathbb{Q}$.)

Solutions:

(a) Let $\alpha = \sqrt[4]{5} \in \mathbb{R}$, and let $i \in \mathbb{C}$ be a primitive 4th root of unity. By Eisenstein's Criterion (with $p = 5$), one sees that g is irreducible over $\mathbb{Q}$. Thus $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Further, one has $[\mathbb{Q}(i) : \mathbb{Q}] = 2$, since i is a root of $\Phi_4 = X^2 + 1$ (which is irreducible over $\mathbb{Q}$). So $[L : \mathbb{Q}(\alpha)] = 1$ or 2. But $i \notin \mathbb{Q}(\alpha) \subset \mathbb{R}$, so that $X^2 + 1$ must be irreducible over $\mathbb{Q}(\alpha)$. Hence we have $[L : \mathbb{Q}(\alpha)] = 2$, and so the Tower Law gives

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \times 4 = 8.$$

(b) The Galois group $Gal(L : \mathbb{Q})$ is generated by σ and τ, where σ and τ leave $\mathbb{Q}$ fixed pointwise, and $\sigma(\alpha) = i\alpha$ and $\sigma(i) = i$, and $\tau(\alpha) = \alpha$ and $\tau(i) = i^3 = -i$. Thus $Gal(L : \mathbb{Q}) = \langle\sigma, \tau : \sigma^4 = 1 = \tau^2, \sigma\tau = \tau\sigma^3\rangle$.

(c) The elements of $G = Gal(L : \mathbb{Q})$ are

$$1,\ \tau,\ \sigma,\ \sigma^2,\ \sigma^3,\ \sigma\tau,\ \sigma^2\tau,\ \sigma^3\tau.$$

The elements σ, σ^3 have order 4, 1 (the identity map) has order 1, and all other elements have order 2. Any noncyclic subgroup of order 4 is generated by 2 elements of order 2. [Note that 2 elements of order 2 can generate the entire group G; for instance, $\langle\tau, \sigma\tau\rangle = G$.]

Let us name the order 2 subgroups as follows:

$$H_1 = \langle\tau\rangle,\ H_2 = \langle\sigma^2\rangle,\ H_3 = \langle\sigma\tau\rangle,\ H_4 = \langle\sigma^2\tau\rangle,\ H_5 = \langle\sigma^3\tau\rangle.$$

We name the order 4 subgroups as follows: $N_1 = \langle\sigma\rangle$,

$$N_2 = \langle\sigma^2, \tau\rangle = \langle\sigma^2, \sigma^2\tau\rangle = \langle\tau, \sigma^2\tau\rangle,$$

$$N_3 = \langle\sigma^2, \sigma\tau\rangle = \langle\sigma^2, \sigma^3\tau\rangle, \langle\sigma\tau, \sigma^3\tau\rangle.$$

[Recall that whenever $H_j \subseteq N_k$ then we have $\phi(H_j) \supseteq \phi(N_k)$ where $\phi(H) = Fix_L(H)$.]

We begin with the most obvious computations of fixed fields [especially as this can help us with other computations].

- We have $\alpha \in \phi(H_1)$. Also, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4 = [G : H_1]$ so we must have $\mathbb{Q}(\alpha) = \phi(H_1)$.

- We have $i \in \phi(N_1)$, and $[\mathbb{Q}(i) : \mathbb{Q}] = 2 = [G : N_1]$, so $\mathbb{Q}(i) = \phi(N_1)$.
- [We have $H_2 \subseteq N_1$, so we have $\mathbb{Q}(i) = \phi(N_1) \subseteq \phi(H_2) \subseteq L = \mathbb{Q}(\alpha, i)$ with

  $$[\mathbb{Q}(\alpha, i) : \phi(H_2)] = 2 = [\phi(H_2) : \mathbb{Q}(i)].$$

  So we might guess that $\phi(H_2) = \mathbb{Q}(\alpha^2)$.]
  We have $\sigma^2(\alpha^2) = \alpha^2 = \sqrt{5}$ and $\sigma^2(i) = i$, so $\alpha^2, i \in \phi(H_2)$. We have previously seen that $[\mathbb{Q}(\alpha^2, i) : \mathbb{Q}] = 4$. As $4 = [G : H_2]$, we must have $\phi(H_2) = \mathbb{Q}(\alpha^2, i)$.
- [We have $\phi(N_2) \subseteq \phi(H_1)$ and $\phi(N_2) \subseteq \phi(H_2)$ so $\phi(N_2) \subseteq \mathbb{Q}(\alpha)$ and $\phi(N_2) \subseteq \mathbb{Q}(\alpha^2, i)$. As $[\phi(N_2) : \mathbb{Q}] = 2$, we can guess that $\phi(N_2) = \mathbb{Q}(\alpha^2)$.]
  We have $\sigma^2(\alpha^2) = \alpha^2$ and $\tau(\alpha^2) = \alpha^2$, so $\alpha^2 \in \phi(N_2)$. We know that $\alpha^2 = \sqrt{2}$ and we have seen that $[\mathbb{Q}(\alpha^2) : \mathbb{Q}] = 2$. Since $2 = [G : N_2]$, we must have $\mathbb{Q}(\alpha^2) = \phi(N_2)$.
- [We know that $i\alpha$ is also a root of $t^4 - 5$, so $\mathbb{Q}(i\alpha) = \phi(H_j)$ for j =3, 4, or 5. So we test.]
  We have $\sigma^2\tau(i\alpha) = i\alpha$, so $i\alpha \in \phi(H_4)$. As $[\mathbb{Q}(i\alpha) : \mathbb{Q}] = 4 = [G : H_4]$ we have $\phi(H_4) = \mathbb{Q}(i\alpha)$.
- To find $\phi(H_3)$, we note that since $(\sigma\tau)^2 = 1$, we that

  $$\alpha + i\alpha = \alpha + \sigma\tau(\alpha) \in \phi(H_3).$$

  We have $(\alpha + i\alpha)^2 = 2i\alpha^2$ and $(\alpha + i\alpha)^4 = -20$. Thus $\alpha + i\alpha$ is a root of $t^4 + 20$, which is irreducible over $\mathbb{Q}$ (by Eisenstein's Criterion and Gauss' Lemma). Hence $[\mathbb{Q}(\alpha + i\alpha) : \mathbb{Q}] = 4 = [G : H_3]$, and thus $\mathbb{Q}(\alpha + i\alpha) = \phi(H_3)$.
- [We argue as above to find $\phi(H_5)$.] We have $\sigma^3\tau(\alpha - i\alpha) = \alpha - i\alpha$ so $\alpha - i\alpha \in \phi(H_5)$. Also, $\alpha - i\alpha$ is a root of $t^4 + 20$ so $[\mathbb{Q}(\alpha - i\alpha) : \mathbb{Q}] = 4 = [G : H_5]$. Hence $\mathbb{Q}(\alpha - i\alpha) = \phi(H_5)$.
- [We have $H_2, H_3, H_5 \subseteq N_3$ so $\phi(N_3) \subseteq \mathbb{Q}(\alpha^2, i) \cap \mathbb{Q}(\alpha + i\alpha) \cap \mathbb{Q}(\alpha - i\alpha)$. We know from our above computations that $i\alpha^2 \in \mathbb{Q}(\alpha^2, i) \cap \mathbb{Q}(\alpha + i\alpha) \cap \mathbb{Q}(\alpha - i\alpha)$.]
  We have $\sigma^2(i\alpha^2) = i\alpha^2 = \sigma\tau(i\alpha^2)$ so $i\alpha^2 \in \phi(N_3)$. We know that $i\alpha^2$ is a root of $t^2 + 5$ which is irreducible over $\mathbb{Q}$. Hence $[\mathbb{Q}(i\alpha^2) : \mathbb{Q}] = 2 = [G : N_3]$ and so $\mathbb{Q}(i\alpha^2) = \phi(N_3)$.

5. (Parts (a) and (b) are from #4(b), 2015 exam.)
   (a) Let $L : \mathbb{Q}$ be a splitting field extension for $f(X) = (X^2-2)(X^2+7)$. Determine the degree of the extension $L : \mathbb{Q}$, justifying your answer.
   (b) Describe the Galois group $Gal(L : \mathbb{Q})$ (that is, give generators and relations for the Galois group).
   (c) Use the Fundamental Theorem of Galois Theory (Theorem 11.1) to determine all subfields of the splitting field that you wrote down in part (a). (It may be helpful to draw the lattice of subfields and corresponding lattice of subgroups of S_3.)

   Solution:

(a) We have $L = \mathbb{Q}(\sqrt{2}, \sqrt{-7})$. We have $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, since the minimal polynomial for $\sqrt{2}$ over $\mathbb{Q}$ is $X^2 - 2$. The minimal polynomial for $\sqrt{-7}$ over $\mathbb{Q}(\sqrt{2})$ divides $X^2 + 7$. Since $\sqrt{-7} \notin \mathbb{R}$ and $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$, we see that X^2+7 has no root in $\mathbb{Q}(\sqrt{2})$, and hence is irreducible over $\mathbb{Q}(\sqrt{2})$. Thus $[L : \mathbb{Q}(\sqrt{5})] = 2$, and so

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4.$$

(b) The group $\mathrm{Gal}(L : \mathbb{Q})$ is generated by σ and τ, where these maps fix $\mathbb{Q}$ pointwise, and $\sigma(\sqrt{2}) = -\sqrt{2}$ and $\sigma(\sqrt{-7}) = \sqrt{-7}$, and $\tau(\sqrt{2}) = \sqrt{2}$ and $\tau(\sqrt{-7}) = -\sqrt{-7}$. Thus $\sigma\tau(\sqrt{2}) = \tau\sigma(\sqrt{2}) = -\sqrt{2}$ and $\sigma\tau(\sqrt{-7}) = \tau\sigma(\sqrt{-7}) = -\sqrt{-7}$. Then σ, τ, $\sigma\tau$ each have order 2, and $\mathrm{Gal}(L : \mathbb{Q}) = \langle \sigma, \tau : \sigma^2 = \tau^2 = 1, \sigma\tau = \tau\sigma \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
(iii) Apply the Fundamental Theorem of Galois Theory to find all fields M for which $\mathbb{Q} \subsetneq M \subsetneq L$, explaining carefully how you applied the Fundamental Theorem in this process.
Solution: We know that $\mathrm{Gal}(L : \mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\}$. The fields M that we are to find are the fixed fields of the subgroups $H_1 = \langle \sigma \rangle$, $H_2 = \langle \tau \rangle$, and $H_3 = \langle \sigma\tau \rangle$. With M_i the fixed field of H_i, we have $M_1 = \mathbb{Q}(\sqrt{-7})$, $M_2 = \mathbb{Q}(\sqrt{2})$, $M_3 = \mathbb{Q}(\sqrt{-14})$.

6. (This is #5(b), 2015 exam.) Let p be a prime number, and let $\mathbb{F}_p$ be the finite field with p elements. Put $f(t) = t^p - t + 1$, and let $K = \mathbb{F}_p(\alpha)$, where α is a root of f.
   (a) Show that for all $\xi \in \mathbb{F}_p$, the element $\alpha + \xi$ is a root of f.
   (b) Let σ be the Frobenius map on K. Show that for $1 \leq d < p$, one has that $\sigma^d(\alpha)$ is a root of f.
   (c) Show that f is irreducible over $\mathbb{F}_p$.

   Solution:
   (a) When $\xi \in \mathbb{F}_p$, one has

   $$(\alpha + \xi)^p - (\alpha + \xi) + 1 = (\alpha^p - \alpha + 1) + (\xi^p - \xi) = 0.$$

   Here we used that $\alpha^p - \alpha + 1 = 0$, and by Fermat's Little Theorem also $\xi^p = \xi$.

   (b) Observe first that $\sigma(\alpha) = \alpha^p = \alpha - 1$, since $\alpha^p - \alpha + 1 = 0$. It therefore follows by induction that $\sigma^d(\alpha) = \alpha - d$ for each positive integer d, and by part (i) one sees that $\alpha - d$ is a root of f for any $d \in \mathbb{F}_p$.

   (c) Since $\sigma \in \mathrm{Gal}(K : \mathbb{F}_p)$, we have $\sigma^d \in \mathrm{Gal}(K : \mathbb{F}_p)$ (or equivalently, since σ fixes $\mathbb{F}_p$ pointwise, so too does σ^d). Thus σ^d leaves $m_\alpha(\mathbb{F}_p)$ fixed, and hence maps roots of $m_\alpha(\mathbb{F}_p)$ to roots of $m_\alpha(\mathbb{F}_p)$. Then $\alpha - d = \sigma^d(\alpha)$ must be a root of $m_\alpha(\mathbb{F}_p)$. Then $\alpha, \alpha-1, \ldots, \alpha-(p-1)$ are distinct roots of $m_\alpha(\mathbb{F}_p)$, whence $\deg(m_\alpha(\mathbb{F}_p)) \geq p$. But we have also that $m_\alpha(\mathbb{F}_p)$ divides f, and thus it follows that $\deg(f) = p$. But f is monic, and so $f = m_\alpha(\mathbb{F}_p)$, which is irreducible.

7. Let L be a field, G a subgroup of $Aut(L)$, and $K = Fix_L(G)$. Suppose that each G-orbit in L is finite; thus by Theorem 10.2, we know that $L : K$ is a Galois extension.
   (a) Briefly explain why G is a subset of $Gal(L : K)$.
   (b) Take $\alpha \in L$, and let $\alpha, \alpha_2, \ldots, \alpha_r$ be the distinct elements in the G-orbit of α. With
   $$f_\alpha = (t - \alpha)(t - \alpha_2) \cdots (t - \alpha_r),$$
   we have seen in the proof of Theorem 10.2 that $f_\alpha \in K[t]$. Set $g = m_\alpha(K)$; show that $f_\alpha = g$.

Solution:

(a) Every element of G is an automorphism of L, and by the definiton of K, each element of G is a K-homomorphism. Thus $G \subseteq Gal(L : K)$.

(b) We have $f_\alpha, g \in K[t]$ with α a root of both f_α and g; as g is irreducible over K, this means that $g|f$. Consider α_i where $1 < i \leq r$; since α_i is in the G-orbit of α, there is some $\sigma_i \in G$ so that $\sigma_i(\alpha) = \alpha_i$. Since $\sigma_i \in Gal(L : K)$ and $g(\alpha) = 0$, we have
$$0 = \sigma_i(g(\alpha)) = g(\sigma_i(\alpha)) = g(\alpha_i).$$
Hence in $L[t]$, $t - \alpha_i$ divides g. As this holds for all i with $1 < i \leq r$, and as $t - \alpha$ divides g in $L[t]$ since α is a root of g, we have $f_\alpha | g$. Since we also have $g | f_\alpha$ and both f_α and g are monic, we have $f_\alpha = g$.