Math 55a, Fall 2004

Twelfth Assignment, Solutions
Adapted from Andrew Cotton, George Lee, Tseno Tselkov, and earlier math 55 students

---

Problem 1

As in the problem statement, ϕ will always refer to an embedding of L into E over K. Since L is a finite extension of K, there is some primitive element $\gamma \in L$ such that $L = K[\gamma]$. Then $\{1, \gamma, \ldots, \gamma^{n-1}\}$ is a basis of L over K, which implies that the monic irreducible in $K[X]$ with root γ (which we will also refer to as "the minimal $K[X]$ polynomial of γ) has degree n.

Observe that for any embedding $\phi : L \to E$, any $p = \sum_{i=0}^{m} k_i X^i \in K[X]$, and any $\ell \in L$, we have

$$\begin{aligned}
\phi(p(\ell)) &= \textstyle\sum_{i=0}^{m} \phi(k_i)\phi(\ell)^i && \text{because } \phi \text{ is a homomorphism} \\
&= \textstyle\sum_{i=0}^{m} k_i \phi(\ell)^i && \text{because } \phi \text{ fixes each element in } K \\
&= p(\phi(\ell)).
\end{aligned}$$

We will use this result several times throughout these solutions.

Claim 1. *Suppose $\phi : L \to E$ is an embedding, $\ell \in L$, and $p \in K[X]$ such that $p(\ell) = 0$. Then $\phi(\ell)$ is a root of p.*

Proof: This follows immediately from our above observation; $p(\phi(\ell)) = \phi(p(\ell)) = \phi(0) = 0$. ∎

Claim 2. *Suppose that $L = M[\zeta]$ is a finite field extension of M. Let g be the minimal $M[X]$ polynomial of ζ. If g splits into linear factors in $L[X]$, then L is a splitting field of g over M.*

Proof: We need only prove that L is generated by the roots $\zeta, \zeta_2, \ldots, \zeta_k$ of g. But $L = M[\zeta] \subset M[\zeta, \zeta_2, \ldots, \zeta_k]$. And since ζ, ζ_2, $\ldots$, $\zeta_k \in L$ we have $M[\zeta, \zeta_2, \ldots, \zeta_k] \subset L$. Therefore indeed $L = M[\zeta, \zeta_2, \ldots, \zeta_k]$. ∎

(a) Any embedding $\phi : L \to E$ is injective because it is a nonzero homomorphism of fields. Also, any homomorphism of fields $\sigma : L \to L$ that is the identity on K is also an embedding of L into L over K; so,

σ is injective. Then σ must map the n basis elements of L over K to n linearly independent elements. These new elements thus form a basis of L, so Im $\phi = L$. Thus ϕ is bijective; and therefore, it is invertible.

(b) Every $\ell \in L$ can be written in the form $p(\gamma)$ for some $p \in K[X]$; then $\phi(\ell) = \phi(p(\gamma)) = p(\phi(\gamma))$. Therefore the embedding is completely determined by the image of $\phi(\gamma)$.

Letting f be the minimal $K[X]$ polynomial of γ, we know that f has at most n roots. From our claim, $\phi(\gamma)$ must be one of these roots, so there are at most n distinct embeddings.

(c) We prove the result is true when E is the splitting field of f, the minimal $K[X]$-polynomial of γ. (And, we will use this result again later.) E is generated by the roots $\gamma_1, \ldots, \gamma_n$ of f in E (with $\gamma_1 = \gamma$). Thus it is spanned by the finite set $\{\prod_{i=1}^{n} \gamma_i^{j_i} \mid 1 \leq i \leq n, 0 \leq j_i \leq n-1\}$, and therefore it is finite-dimensional over K. From 1(b) of Assignment 11, we know that the γ_i are distinct. Fix i such that $1 \leq i \leq n$. Then $f(\gamma) = f(\gamma_i) = 0$. From 2(b) of Assignment 10, there exists an isomorphism ϕ_i of fields $L = K[\gamma]$ to $K[\gamma_i] \subset E$ such that $\phi_i(\gamma) = \gamma_i$ and $\phi_i(a) = a$ for all $a \in K$.

Viewing each ϕ_i as a homomorphism from L to E yields n embeddings, which are all distinct because $\phi_1(\gamma), \ldots \phi_n(\gamma)$ are distinct. Thus there are indeed at least n embeddings of L into E over K; and from (b) there are at *most* n, so there must be *exactly* n embeddings.

(d)

Note: For many people, the trickiest parts of this problem were proving directions starting with (ii) or ending with (iii). While many proofs conclude or use that L is the splitting field of the minimal $K[X]$ polynomial of γ, the polynomial given in (ii) may not have γ as a root. It is true that L is generated by *all* the roots of this polynomial, but this fact can be difficult to work with. Also, some attempts to prove (iii) claimed one could "extend an embedding" from a subfield of L to an embedding from all of L; proving this is possible, however, is also difficult. Below are presented seven proofs: the first four suffice to show the problem, and the last three are for your reading pleasure. As hinted at in a note on a previously problem set, one of the proofs (the first proof to (ii) $\Longrightarrow$ (iii)) uses a past result about a single field by applying it instead to two isomorphic fields — it's a good reminder of how powerful the notion of "isomorphism" can be. And now, on with the proofs . . .

• *(i) $\Longrightarrow$ (ii).*
As before, let f be the minimal $K[X]$ polynomial of γ, and let $n = [L : K] = \deg f$. Let E be the splitting field of f over L, and let the roots of f be $\gamma_1, \gamma_2, \ldots, \gamma_n$ with $\gamma_1 = \gamma$. Then, as proven in (c), there are n distinct embeddings $\phi_i : L \to E$ with $\phi_i(\gamma) = \gamma_i$. Using (i), we have $\gamma_i = \phi_i(\gamma) \in \phi_i(L) = L$, so that all the γ_i are in L. By Claim 2, it follows that L is the splitting field of f.

• *(ii) $\Longrightarrow$ (iii).*
(Adapted from Rasheed Sabar) Suppose L is a splitting field for some polynomial g over K and that p is an irreducible polynomial in $K[X]$ with root $r_1 \in L$. Let r_2 be another zero of p in E. We claim that

$$[L(r_1) : L] = [L(r_2) : L].$$

To see this, note that for $j = 1$ or $j = 2$, we have

$$[L(r_j) : L][L : K] = [L(r_j) : K] = [L(r_j) : K(r_j)][K(r_j) : K]. \qquad (*)$$

Now, since $p(r_1) = 0$ in $K(r_1)$ and $p(r_2) = 0$ in $K(r_2)$, it follows (from work on a previous assignment) that $K(r_1)$ is isomorphic to $K(r_2)$. Thus,

$$[K(r_1) : K] = [K(r_2) : K]. \qquad (1)$$

Now, $L(r_j)$ is a pseudo-splitting field for f (not necessarily irreducible in $K(r_j)[X]$) over $K(r_j)$ for j = 1, 2. (Can you prove this?) Since $K(r_1)$ is isomorphic to $K(r_2)$ over K, and this isomorphism sends the coefficients of f in $K(r_1)[X]$ to the coefficients of f in $K(r_2)[X]$, we have (by the uniqueness of the pseudo-splitting field up to isomorphism, from work on a previous assignment) that $L(r_1)$ is isomorphic to $L(r_2)$. Hence,

$$[L[r_1] : K[r_1]] = [L[r_2] : K[r_2]]. \qquad (2)$$

Substituting (1) and (2) into $(*)$ yields

$$[L[r_1] : L] = [L[r_2] : L].$$

Therefore, $[L[r_2] : L] = [L[r_1] : L] = 1$, which implies that $r_2 \in L$. It follows that L contains all the roots of p and hence that p splits into a product of linear factors in $L[X]$.

• *(iii) $\Longrightarrow$ (iv).*
Any automorphism of L over K is a K-embedding of L into itself; conversely, any K-embedding of L into itself is an automorphism from part (a).

By (iii), the minimal $K[X]$ polynomial f of γ splits into a product of linear factors in $L[X]$ with roots $\gamma, \gamma_2, \dots, \gamma_n$. From Claim 2, L is a splitting field of f. Then by our argument in (c) we know that there are exactly n distinct embeddings from L into itself over K, i.e. there are exactly n automorphisms of L over K.

- *(iv) $\Longrightarrow$ (i).*
  Let E be an extension field of L. Each automorphism of L, viewed instead as a map from L to E, is an embedding of L into E. From (c) there can be no other embeddings $\phi : L \to E$ than these n; but each of these embeddings maps L to itself, as desired.

- *(i) $\Longrightarrow$ (iii).*
  We first prove the following claim:

Claim 3. *Suppose we have an irreducible $p \in K[X]$ with a root $\beta = \beta_1 \in L$. Let E be a finite extension of L such that p splits into a product of linear factors in $E[X]$ with roots $\beta_1, \dots, \beta_k$. Then for each β_i, there exists some embedding ϕ such that $\phi(\beta) = \beta_i$.*

Proof: E is a finite extension of K so it equals $K[\zeta]$ for some primitive element $\zeta = \zeta_1 \in E$. Let $\zeta_2, \dots, \zeta_m$ be the other roots of the minimal $K[X]$ polynomial g of ζ.

We must have $\beta = q(\zeta)$ for some $q \in K[X]$. Then $p \circ q \in K[X]$ has root ζ so it must have roots $\zeta_2, \dots, \zeta_k$ as well. Thus $q(\zeta), q(\zeta_2), \dots, q(\zeta_m)$ are all roots of p. (Some of these $q(\zeta_i)$ might be equal, but this doesn't matter.)

Consider the polynomial $r = \prod_{i=1}^{m}(X - q(\zeta_i))$. Its coefficients can be viewed as symmetric polynomials (with coefficients in K) in the ζ_i. Such polynomials, from a well-known result, are polynomials (with coefficients in K) in the coefficients of $\prod_{i=1}^{m}(X - \zeta_i) = g$. These, we know, are in K; hence, $r \in K[X]$.

Since both p, r are in $K[X]$ with root $q(\zeta)$, and p is irreducible, we must have $p \mid r$. Then every root β_i of p is a root of r, and therefore of the form $q(\zeta_{j_i})$ for some ζ_{j_i}.

Then for any β_i, consider the automorphism on E that sends any polynomial value $s(\zeta)$ to $s(\zeta_{j_i})$; this induces an embedding of L into E over K that maps $\beta = q(\zeta)$ to $q(\zeta_{j_i}) = \beta_i$, as desired. ∎

Applied to this direction, let p be the given irreducible with root $\beta \in L$; and let E be a field as described in the claim. Then given any root of p in E, some embedding maps β to that root; so by (i), that root must lie in L as well. Thus L indeed splits into a product of linear factors.

- *(ii) $\Longrightarrow$ (iii).*
  (Adapted from Luke Gustafson and Willy Meyerson) Suppose that L is a splitting field of g over K, and suppose that $p \in K[X]$ is irreducible in $K[X]$ with root $\beta \in L$. Then β can be written as a polynomial q (with coefficients in K) of the roots $r_1, r_2, \ldots, r_n$ of g. As in the above proof of (i) $\Longrightarrow$ (ii), we can show that the coefficients of $\prod_{\sigma \in S_n}(X - q(r_{\sigma 1}, r_{\sigma 2}, \ldots, r_{\sigma n}))$ are in K. Thus, this monstrous polynomial has root β and is in $K[X]$, implying that it is divisible by p. This in turn implies that each root of p is of the form $q(r_{\sigma_1}, r_{\sigma 2}, \ldots, r_{\sigma n}$ for some σ; and any element of that form is in L. Therefore, p splits into linear factors in L, as desired.

- *(iv) $\Longrightarrow$ (iii).*
  (Adapted from Gabriel Carroll) Again suppose that $p \in K[X]$ is irreducible in $K[X]$ with root $\beta \in L$. Let $m = \deg p$ and suppose that p has m' roots $\beta_1, \beta_2, \ldots, \beta_{m'}$ in L. Then $[L : K[\beta_i]] = [L : K]/[K[\beta_i] : K] = n/m$ for $i = 1, 2, \ldots, m'$.
  By (iv), there are n distinct K-automorphisms of L; from Claim 1 (stated on the first page of these solutions), each must map β to another root of p in L. Fix $i = 1, 2, \ldots, m'$, and suppose that t automorphisms $\sigma_1, \sigma_2, \ldots, \sigma_t$ map β to β_i. Then $\sigma^{-1}\sigma_1, \sigma^{-1}\sigma_2, \ldots, \sigma^{-1}\sigma_t$ are t distinct automorphisms of L over $K[\beta]$. However, by (iv) applied with fields $\tilde{L} = L$ and $\tilde{K} = K[\beta]$, we find that $t \le n/m$. Hence, for each of the m' values i, there are at most n/m K-automorphisms of L.
  This gives a total of at most nm'/m K-automorphisms of L; but because there are n such automorphisms, we must have $nm'/m \ge n$ or $m' \ge m$. Therefore, all m roots of p in L, as desired.

(e)

From the direction (iii) $\Longrightarrow$ (iv) in part (d), and from part (c), we have the following fact:

Claim 4. *Suppose L is a finite Galois extension of M, with primitive element ζ. Let $\zeta_1, \zeta_2, \ldots, \zeta_k$ be the roots to the monic irreducible $g_\zeta \in M[X]$ with root $\zeta = \zeta_1$; then* $\mathrm{Gal}(L/M)$ *consists of the k maps $p(\zeta) \longmapsto p(\zeta_i)$ (for all $p \in M[X]$), where $1 \le i \le k$.*

Now to continue with part (e):

Claim 5. *L is a finite Galois extension of any subfield $M \subset L$ containing K.*

Proof: Any M-embedding $\tilde{\phi} : L \to E$ is also a K-embedding. Because L is Galois over K, from part (d)-(i) we have that $\tilde{\phi}(L) = L$ for all such $\tilde{\phi}$; then from part (d)-(i) again, this implies that L is Galois over M.

Alternatively: We have $L = M[\zeta]$ for some primitive element $\zeta \in L$. By part (d)-(iii) applied to the Galois extension L of K, $f_\zeta \in K[X]$ splits into linear factors in L. Therefore the minimal $M[X]$ polynomial g of ζ — which divides the minimal $K[X]$ polynomial f of ζ — also splits into linear factors in L. Thus by Claim 2, L is a splitting field of g over M. Then by part (d)-(ii), we know that L is indeed a Galois extension of M. And it cannot be an infinite extension of M since it is a finite extension of $K \subset M$. ∎

Claim 6. *If L is a finite Galois extension of M, then the fixed field of* $\mathrm{Gal}(L/M)$ *is M.*

Proof: By definition, $\mathrm{Gal}(L/M)$ fixes every element in M. Now suppose, for sake of contradiction, that its fixed field M' were actually bigger than M. Because L is Galois over M' from our previous claim, there are at most $[L : M'] < [L : M]$ M'-automorphisms of L. In other words, one of the $[L : M]$ M-automorphisms of L does not fix each element in M', a contradiction. Therefore, $\mathrm{Gal}(L/M)$ indeed has fixed field M.

Alternatively: Say that L is a degree-k extension of M and write $L = M[\zeta]$ for some primitive element $\zeta \in L$. Then $\{1, \zeta, \ldots, \zeta^{k-1}\}$ is a basis for L over M; thus we can write any $\ell \in L$ in the form $q(\zeta)$ for some $q = \sum_{i=0}^{k-1} m_i X^i \in M[X]$. Furthermore, the minimal $M[X]$ polynomial g with root ζ has degree k; say its roots are $\zeta_1, \zeta_2, \ldots, \zeta_k$ (with $\zeta_1 = \zeta$).

From Claim 4, each of the maps $p(\zeta) \longmapsto p(\zeta_i)$ (for all $p \in M[X]$) is in $\mathrm{Gal}(L/M)$. So if they all fix $\ell = q(\zeta)$ then we must have that all the ζ_i are roots of $q - \ell$, so that $g \mid q - \ell$. But g has degree k while $q - \ell$ has degree at most $k - 1$. Then we must have $q - \ell = 0$ so that q is a constant in M. Thus, $\mathrm{Gal}(L/M)$ fixes no elements outside of M. This completes the proof. ∎

For any subfield $M \subset L$ containing K, from Claim 5 the group $\mathrm{Gal}(L/M)$ exists; and from Claim 6, we know that the fixed field of

$\mathrm{Gal}(L/M)$ is M. Therefore the map given in the problem statement is surjective.

Next, say that $M \subset L = M[\zeta]$ is the fixed field of H, and let g be the minimal $M[X]$ polynomial of ζ. Let $\zeta_1, \zeta_2, \dots, \zeta_k \in L$ be the roots of g (with $\zeta_1 = \zeta$); any automorphism in H fixes M and sends ζ to some ζ_i.

Look at the orbit $\{\zeta_{i_1}, \zeta_{i_2}, \dots, \zeta_{i_r}\}$ of ζ under the action of H (where $i_1 = 1$). Each map in H fixes each coefficient of $p = (X - \zeta_{i_1}) \cdots (X - \zeta_{i_r})$ (here we are not applying each map to the polynomial, but to the individual coefficients), so p's coefficients must all be in M. But since $(X - \zeta_1) \cdots (X - \zeta_k)$ is a minimal polynomial in $M[X]$ with root ζ, this implies that p must have degree k as well so that the orbit of ζ is all of $\{\zeta_1, \dots, \zeta_k\}$. Therefore H must consist exactly of those k automorphisms which fix M and map ζ to any other ζ_i. And from Claim 4, we must have $H = \mathrm{Gal}(L/M)$. Thus, the given map is injective as well, so it is a bijection. And we have also proved that $H = \mathrm{Gal}(L/L^H)$.

Next we prove the statements about normality. We first claim that H is normal in $\mathrm{Gal}(L/K)$ iff $\tau(L^H) = L^H$ for all $\tau \in \mathrm{Gal}(L/K)$. From part (a), any such τ is an automorphism. Then H is normal iff

$$\begin{aligned}
&\tau^{-1} \circ \phi \circ \tau \in H && \forall\, \phi \in H, \tau \in \mathrm{Gal}(L/K) \\
\iff\ &\tau^{-1}(\phi(\tau(x))) = x && \forall\, \phi \in H, \tau \in \mathrm{Gal}(L/K), x \in L^H \\
\iff\ &\phi(\tau(x)) = \tau(x) && \forall\, \phi \in H, \tau \in \mathrm{Gal}(L/K), x \in L^H \\
\iff\ &\tau(x) \in L^H && \forall\, \tau \in \mathrm{Gal}(L/K), x \in L^H, \\
\iff\ &\tau(L^H) \subset L^H && \forall\, \tau \in \mathrm{Gal}(L/K), \\
\iff\ &\tau(L^H) = L^H && \forall\, \tau \in \mathrm{Gal}(L/K),
\end{aligned}$$

as desired. (The last equivalence is true because $\tau|_{L^H} : L^H \to L^H$ is also an automorphism from part (a).)

First assume that L^H is Galois over K. Then applying (i) to the Galois extension L^H over K and the embedding $\tau : L^H \to L$, we find that $\tau(L^H) = L^H$ and hence H is normal in $\mathrm{Gal}(L/K)$.

Next assume that H is normal in $\mathrm{Gal}(L/K)$. Then $\tau(L^H) = L^H$, so we can consider the map ψ which restricts each map in $\mathrm{Gal}(L/K)$ to the set $\mathcal{A}$ of K-automorphisms of L^H. Because ψ is a restriction, it is a homomorphism. ψ's kernel consists of precisely those automorphisms that fix every element in L^H; that is, the automorphisms in $\mathrm{Gal}(L/L^H) = H$. Therefore, we have

$$\mathrm{Gal}(L/K)/H = \mathrm{Gal}(L/K)/\operatorname{Ker}\psi \simeq \operatorname{Im}\psi. \tag{†}$$

Observe that $\mathrm{Gal}(L/K)/H = \mathrm{Gal}(L/K)/\,\mathrm{Gal}(L/L^H)$ has $[L:K]/[L:L^H] = [L^H : K]$ elements, so $|\mathcal{A}| \geq |\operatorname{Im}\psi| = [L^H : K]$. However, from (b) we also have $|\mathcal{A}| \leq [L^H : K]$. It follows that $|\mathcal{A}| = [L^H : K]$ and hence (from part (d)-(iv)) L^H is normal over K.

We have now proved that H is a normal subgroup of $\mathrm{Gal}(L/K)$ if and only if L^H is normal over K. Using the notation and building on the results of the last paragraph, it also follows that $\operatorname{Im}\psi = \mathcal{A} = \mathrm{Gal}(L^H/K)$. Combined with (†), we find that

$$\mathrm{Gal}(L/K)/H \simeq \mathrm{Gal}(L^H/K).$$

This completes the proof.

(f) The roots of the given polynomial are $\gamma_j = \mathrm{cis}(72j)^\circ$ for $j = 1, 2, 3, 4$. Since $\gamma_j = \gamma_1^j$ we have $L = \mathbb{Q}[\gamma_1, \gamma_2, \gamma_3, \gamma_4] = \mathbb{Q}[\gamma_1]$ so that γ_1 is a primitive element generating L over $\mathbb{Q}$. Then the Galois group consists of the functions f_j that map $q(\gamma_1) \mapsto q(\gamma_j) \forall q \in \mathbb{Q}[X]$. And since f_2 maps γ_1 to γ_2 to γ_4 to γ_3 back to γ_1, it has order 4 so we know that $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathbb{Z}_4$.

(g) Nope! In order to be normal over $\mathbb{Q}$, the field L must satisfy condition (iii) in part (d). But the polynomial $X^3 - 2$ has root $\zeta \in L$ yet it does not split into linear factors in $L = \mathbb{Q} + \mathbb{Q}\sqrt[3]{2} + \mathbb{Q}\sqrt[3]{4} \subset \mathbb{R}$. This is because $X^3 - 2 = (X - \sqrt[3]{2})(X^2 + \sqrt[3]{2}X + \sqrt[3]{4})$ and the roots of $X^2 + \sqrt[3]{2}X + \sqrt[3]{4}$ are not real (in $\mathbb{C}$ they equal $\sqrt[3]{2}\,\mathrm{cis}(\pm 120^\circ)$).

Problem 2

a) For every $g \in G$ we are given a linear transformation $\pi(g) : V \to V$ such that $\pi(e) = 1_V$ and $\pi(gh) = \pi(g) \circ \pi(h)$. By the functoriality that we've discussed in class these induce natural linear transformations $\otimes^k \pi(g) : \otimes^k V \to \otimes^k V$. Let's check that the necessary properties are again satisfied, namely that $\otimes^k \pi(e) = 1_{\otimes^k V}$ and $\otimes^k \pi(gh) = \otimes^k \pi(g) \circ \otimes^k \pi(h)$. Indeed,

$$\otimes^k \pi(e)(v_1 \otimes \ldots \otimes v_k) = \pi(e)(v_1) \otimes \ldots \otimes \pi(e)(v_k) =$$

$$= v_1 \otimes \ldots \otimes v_k = 1_{\otimes^k V}(v_1 \otimes \ldots \otimes v_k),$$

where we first applied the definition of $\otimes^k \pi$ and then the properties that we know for π. Also,

$$\otimes^k \pi(gh)(v_1 \otimes \ldots \otimes v_k) = \pi(gh)(v_1) \otimes \ldots \otimes \pi(gh)(v_k) =$$

$$= \pi(g) \circ \pi(h)(v_1) \otimes \ldots \otimes \pi(g) \circ \pi(h)(v_k) =$$

$$= \otimes^k \pi(g) \left(\pi(h)(v_1) \otimes \ldots \otimes \pi(h)(v_k)\right) =$$

$$= \otimes^k \pi(g) \circ \otimes^k \pi(h)(v_1 \otimes \ldots \otimes v_k),$$

where again we only used the definition of $\otimes^k \pi$ and the properties of π.

Thus we showed that indeed any representation π on V induces a representation $\otimes^k \pi$ on $\otimes^k V$.

b) Let's just directly show that the representations $\otimes^k \pi$ of G and a of S_k commute:

$$\otimes^k \pi(g) \circ a(\sigma)(v_1 \otimes \ldots \otimes v_k) =$$

$$= \otimes^k \pi(g)(v_{\sigma^{-1}(1)} \otimes \ldots \otimes v_{\sigma^{-1}(k)}) =$$

$$= \pi(g)(v_{\sigma^{-1}(1)}) \otimes \ldots \otimes \pi(g)(v_{\sigma^{-1}(k)}) =$$

$$= a(\sigma)(\pi(g)(v_1) \otimes \ldots \otimes \pi(g)(v_k)) =$$

$$= a(\sigma) \circ \otimes^k \pi(g)(v_1 \otimes \ldots \otimes v_k).$$

Therefore $\otimes^k \pi(g) \circ a(\sigma) = a(\sigma) \circ \otimes^k \pi(g)$ and we are done.

The End.