Problems

1. **[Field Embeddings, I]** Let $E/\mathbf{Q}$ be a finite extension. Let $K/\mathbf{Q}$ be a Galois extension with Galois group $G = \mathrm{Gal}(K/\mathbf{Q})$. Let $N = \mathrm{Hom}(E, K)$ be the set of ring homomorphisms from E to K (so 1 maps to 1).

   (a) Prove that either N is empty, or there exists an inclusion from E to K.

   (b) If $\phi \in N$, show that $\phi(E)$ is a subfield of K.

   (c) Prove that if $\sigma \in G$, and $\phi : E \to K$ is an element of N, then the map $\sigma.\phi$ defined by sending x to $\sigma(\phi(x))$ is an element of N.

   (d) Prove that this construction gives a group action of G on N.

   (e) Prove that the stabilizer of ϕ is $\mathrm{Gal}(K/\phi(E))$.

   (f) Prove that G acts transitively on N.

   (g) Prove that either N is empty, or $|N| = [E : \mathbf{Q}]$.

   (h) Prove that for any field K (not necessarily finite or Galois) containing the splitting field of E, $N = \mathrm{Hom}(E, K)$ has order $[E : \mathbf{Q}]$.

   (i) If $K = \mathbf{C}$, one can write $N = N_{\mathbf{R}} \cup N_{\mathbf{C}}$, where $N_{\mathbf{R}} = \mathrm{Hom}(E, \mathbf{R})$, and $N_{\mathbf{C}}$ consists of the homomorphisms from E to $\mathbf{C}$ which do *not* land in $\mathbf{R}$. Prove that $|N_{\mathbf{C}}|$ is even. Thus, attached to E, there are a pair of integers (r_1, r_2) such that $r_1 = |N_{\mathbf{R}}|$ and $2r_2 = |N_{\mathbf{C}}|$, so $[E : \mathbf{Q}] = r_1 + 2r_2$. The pair (r_1, r_2) is called the *signature* of E. If E has signature $(r_1, 0)$, we say that E is totally real, and if E has signature $(0, r_2)$ we say that E is totally complex.

   (j) Prove that if $E/\mathbf{Q}$ is a finite Galois extension, then E either has signature $(n, 0)$ (where $n = [E : \mathbf{Q}]$), or $[E : \mathbf{Q}] = n = 2m$ and E has signature $(0, m)$.

   (k) Suppose that $E/\mathbf{Q}$ is a finite Galois extension with $\Gamma = \mathrm{Gal}(E/\mathbf{Q})$. Let K be any field (not necessarily finite or Galois) containing the splitting field of E. Prove that there is an action of $\Gamma = \mathrm{Gal}(E/\mathbf{Q})$ on $N = \mathrm{Hom}(E, K)$ given by

   $$\sigma.\phi = \phi(\sigma^{-1}(x)).$$

   (Note that the inverse is there to ensure that $gh.(\phi) = g.(h.\phi)$.)

   (l) Suppose that $E/\mathbf{Q}$ is a Galois extension of degree $2m$ with signature $(0, m)$, and $\Gamma = \mathrm{Gal}(E/\mathbf{Q})$. Let Γ act on $N = N_{\mathbf{C}}$ as in part 1k.

      i. Show that for every $\phi \in N = N_{\mathbf{C}}$, there exists a unique element $c \in \Gamma$ of order two such that $c.\phi$ is ϕ composed with complex conjugation on $\mathbf{C}$.

      ii. Show that the elements c obtained in this way for all $\phi \in N$ are conjugate, and moreover every element that is conjugate to c occurs in this way.

      iii. Let Φ be the smallest normal subgroup of Γ containing (any) c. Prove that E^{Φ} is totally real. Moreover, if $F \subset E$ is totally real, then $F \subseteq E^{\Phi}$.

      iv. If $E/\mathbf{Q}$ is Galois with *abelian* Galois group Γ, then either E is totally real, or there exists a unique totally real subfield $E^+ \subset E$ such that $[E : E^+] = 2$.

      v. If $E/\mathbf{Q}$ is Galois with $G = A_5$, and E is the splitting field of a degree 5 irreducible polynomial $p(x)$, prove that $F = \mathbf{Q}[x]/p(x)$ has signature $(5, 0)$ or $(1, 2)$.

2. **[Field Embeddings, II]** Let $E/\mathbf{Q}$ be a finite extension. Let $K/\mathbf{Q}$ be a Galois extension with Galois group $G = \mathrm{Gal}(K/\mathbf{Q})$. Let M be the set of subfields of K that are isomorphic to E.

   (a) Prove that M is empty, or there exists an inclusion from E to K.

(b) Prove that G acts on M.

(c) If $F \in M$, prove that the stabilizer of F is the normalizer N_F of $\mathrm{Gal}(K/F)$.

(d) Prove that G acts transitively on M.

(e) Prove that $|M| = [G : N_F]$, for any $F \in M$.

(f) Prove that $|M| = 1$ if and only if $E/\mathbf{Q}$ is Galois.

(g) If $F \in M$, let $H = K^{N_F}$. Prove that:

  i. H is contained in F.

  ii. F/H is Galois.

  iii. If $H' \subset F$ is any subfield of F such that F/H' is Galois, then H' contains H.

  iv. H does not depend on K.

(h) Deduce that for any field $E/\mathbf{Q}$, there is a well defined minimal field $H/\mathbf{Q}$ in E such that E/H is Galois.