MA 542: Modern Algebra II / Spring 2023
Homework assignment #7
Due ~~Friday 4/28/23.~~ Wednesday 5/3 ~~is also ok~~.

Final version.

Edited 26 April 2023: typos corrected in (1f). Edited 1 May 2023 to clarify assumptions in (4).

(1) Let M be an extension of a field K, and E and L extensions of K contained in M.

(a) Show that both EL and $E \cap L$ are field extensions of K contained in M.
(Recall that if E and L are both subfields of a field M, the *compositum* EL is the smallest subfield of M containing both E and L.)
If $L = K(\alpha_1, \alpha_2, \ldots)$, show that $EL = E(\alpha_1, \alpha_2, \ldots)$.

Now assume L is finite over K.

(b) Show that $[EL : E] \leq [L : K]$. More precisely, show that $[EL : E] \leq [L : E \cap L]$.

(c) Give an example to show that $[EL : E]$ may be strictly less than $[L : E \cap L]$.

(d) If L is separable over K, show that EL is separable over E and that L is separable over $E \cap L$.

(e) If L is normal over K, show that EL is normal over E and that L is normal over $E \cap L$.

(f) If L is normal over K, show that ~~for every $\sigma \in \mathrm{Aut}(EL/L)$, we have $\sigma(L)$,~~ for every σ in $\mathrm{Aut}(EL/E)$ we have $\sigma(L) = L$, so that restriction to L gives a group homomorphism $\mathrm{res}_L : \mathrm{Aut}(EL/E) \to \mathrm{Aut}(L/E \cap L)$ (why?). Show that res_L is injective.

(g) If L is Galois (normal and separable) over K, show that EL is Galois over E. Show that res_L from (1f) is surjective, so that $\mathrm{res}_L : \mathrm{Gal}(EL/E) \to \mathrm{Gal}(L/L \cap E)$ is an isomorphism.
(Hint: If H is the image of res_L, what is L^H?)
In particular, $[EL : L] = [L : L \cap E]$.

(2) Let L/K be an extension of finite fields. Suppose $|K| = q$ for some prime power q.

(a) Show that $|L| = q^m$, where $m = [L : K]$.

(b) Show that L is a simple extension of K, so that $L \simeq K[x]/\langle \pi(x) \rangle$, where $\pi(x) \in K[x]$ is an irreducible of degree m.

(c) Show that $\varphi_K := (\alpha \mapsto \alpha^q)$ is an automorphism of L that fixes every element of K. This automorphism is still called *Frobenius*.

(d) Show that φ_K has order m in $\mathrm{Aut}(L/K)$.

(e) Let β be a root of $\pi(x)$ in L. What the complete set of roots of of $\pi(x)$ in L?

(f) Show that L is Galois over K.

(g) Show that $\mathrm{Gal}(L/K) \simeq \mathbb{Z}/m\mathbb{Z}$.

(3) Follow the setup in (2), but set $m = 6$. Describe the Galois correspondence for L/K completely explicitly.

Read BB section 8.1, 8.2, and 8.3. Note that the *Galois group* of a polynomial $f(x) \in K[x]$ over a field K is the group $\mathrm{Aut}(L/K)$ for any splitting field of L of $f(x)$ over K.

(4) BB 6.6.5. Note: By a "primitive element of $\mathbb{F}_{64}$" here BB means an element that generates the multiplicative group of units of $\mathbb{F}_{64}$, not merely an element u so that $\mathbb{F}_{64} = \mathbb{F}_2(u)$.

Extra challenge: Show that the conclusion is false if we merely assume $\mathbb{F}_{64} = \mathbb{F}_2(u)$.

(5) BB 8.1.2

(6) BB 8.1.8

(7) BB 8.2.8

(8) BB 8.2.12

Added 24 April

(9) Finish your complete analysis of the Galois correspondence for the extension $\mathbb{Q}(2^{1/4}, i)$ of $\mathbb{Q}$ from 4/26 and/or 4/28 in class. Which of the intermediate fields are conjugate?

(10) BB 8.3.5. Give the Galois correspondence explicitly.

(11) Consider the field $L = \mathbb{Q}(\zeta)$, where $\zeta = \zeta_7$ is a primitive 7^{th} root of unity.

   (a) Determine $\mathrm{Gal}(L/\mathbb{Q})$ and give the Galois correspondence explicitly.

   (b) Which element of the Galois group corresponds to complex conjugation? Does $\mathbb{Q}(\zeta)$ have a totally real subfield? Explain.

   (A *totally real* field is an extension of $\mathbb{Q}$ all of whose embeddings to $\mathbb{C}$ land in $\mathbb{R}$. For example, $\mathbb{Q}(\sqrt{2})$ is a totally real field, but $\mathbb{Q}(\sqrt[3]{2})$ is not.)

   (c) Show that $\sqrt{-7}$ is in $\mathbb{Q}(\zeta)$. Express $\sqrt{-7}$ as a polynomial in ζ.

(12) Let G be the Galois group of a separable irreducible polynomial f over a field K.

Recall from 4/24 lecture: if $\{\alpha_1, \ldots, \alpha_n\}$ are the roots of f in a splitting field L, then $G = \mathrm{Gal}(L/K)$ permutes $\{\alpha_1, \ldots, \alpha_n\}$ *faithfully* (that is if $\sigma \in G$ fixes every α_i, then σ is the identity element), so that G may be viewed as a subgroup of $\mathrm{Perm}\big(\{\alpha_1, \ldots, \alpha_n\}\big) \simeq S_n$.

   (a) Show that G is a transitive subgroup of S_n if and only if f is irreducible.

   (Recall: G is a *transitive* subgroup of S_n if for every pair of indices $1 \le i \ne j \le n$, there is a $\sigma \in G$ so that $\sigma(i) = j$. We argued one direction in class.)

   (b) If f is irreducible, show that $|G|$ is divisible by n.

   (c) If f is irreducible and $n = p$ is prime, show that G contains a p-cycle.

(13) BB 8.4.11. You may assume BB 8.4.10.
(If you have time, also do 8.4.10, but feel free to assume the fact that for $n \ge 2$ the group S_n is generated by $(1\,2)$ and the n-cycle $(1\,2\,3\,\ldots\,n)$. Why is BB 8.4.10 false if p is not prime?)

(14) Let f be an irreducible cubic polynomial over a field $\mathbb{Q}$, and let L be a splitting field for f.

   (a) Prove that $\mathrm{Gal}(L/\mathbb{Q})$ is isomorphic either S_3 or A_3.

   (b) Let $\alpha_1, \alpha_2, \alpha_3$ be the roots of f in L. Show that the *discriminant*

$$D := (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2$$

   is in $\mathbb{Q}$.

   (c) Show that $\mathbb{Q}(\sqrt{D})$ is an at-most-quadratic extension of $\mathbb{Q}$ contained in L.

   (d) Conclude that $\mathrm{Gal}(L/\mathbb{Q}) \simeq A_3$ if and only if D is a square in $\mathbb{Q}$.

   (e) **Optional algebraic number theory teaser:** If $f \in \mathbb{Z}[x]$, the Galois group of f is determined by the factorization of f modulo various primes p. Compare $f(x) = x^3 - 3x + 1$ with a random cubic, for example, using this simple SageMathCell code.