2023 Fall Honors Algebra Exercise 7 (due on Thursday December 21)

For submission of homework, please finish the 15 True/False problems, and choose 10 **problems from the standard ones and** 5 **problems from the more difficult ones. Mark the question numbers clearly.**

[A] = Artin, [DF] = Dummit and Foote, [DN] = Ding and Nie (Chinese), [H] = Hungerford.

7.1. **True/False questions.** (Only write T or F when submitting the solutions.)

(1) Let $K/E/F$ be a tower of extensions of fields. If K/E is Galois and E/F is Galois, then K/F is Galois.
(2) Let $K/E/F$ be a tower of extensions of fields. If K/F is Galois, then K/E is Galois.
(3) Let $K/E/F$ be a tower of extensions of fields. If K/F is Galois, then E/F is Galois.
(4) No quintic polynomial is solvable by radicals over $\mathbb{Q}$.
(5) Every cyclic extension K over F of degree n is of the form $K = F(\sqrt[n]{a})$ for some $a \in F$.
(6) Let K/F be a finite Galois extension with Galois group G. Let H and H' be subgroups of G that are isomorphic. Then K^H is isomorphic to $K^{H'}$.
(7) Let K be an extension of $\mathbb{Q}$ that is contained in $\mathbb{Q}(\mu_n)$ for some n, then K is Galois over $\mathbb{Q}$.
(8) If K is a union of a tower of fields $K_1 \subseteq K_2 \subseteq \cdots$, each K_i finite Galois over a field F, then K is a Galois extension of F.
(9) If $L = K_1K_2$ be a field extension of a field F with intermediate fields K_1 and K_2 such that $K_1 \cap K_2 = F$, then $[L : F] = [L : K_1] \cdot [L : K_2]$.
(10) Let K be a Galois extension of a field F, and let $f(x) \in F[x]$ be an irreducible polynomial. Then if $f(x)$ splits in $K[x]$, then the Galois group $\mathrm{Gal}(K/F)$ acts transitively on all zeros of $f(x)$ in K.
(11) Any algebraic closure of $\mathbb{Q}(\sqrt{2})$ is isomorphic to an algebraic closure of $\mathbb{Q}(\sqrt{7})$.
(12) The field $\mathbb{Q}(e)$ is isomorphic to $\mathbb{Q}(\pi)$.
(13) Let K be a Galois extension of F with Galois group $G = \mathrm{Gal}(K/F)$. An intermediate field E is finite over F if and only if $\mathrm{Gal}(K/E)$ is open in $\mathrm{Gal}(K/F)$.
(14) An inverse limit of compact Hausdorff space is compact and Hausdorff.
(15) A finite index subgroup of a profinite group always contains an open normal subgroup.

7.2. **Warm-up questions.** (Do not submit solutions for the following questions)

Problem 7.2.1. [DF, page 595, problem 1]
Determine the Galois closure of the field $\mathbb{Q}(\sqrt{1+\sqrt{2}})$ over $\mathbb{Q}$.

Problem 7.2.2. Let K be a finite normal extension of the field F. Let $\varphi : K \to K'$ be an isomorphism of K with a field K' which maps F to the subfield F' of K'. Prove that the map $\sigma \mapsto \varphi\sigma\varphi^{-1}$ defines a group isomorphism $\mathrm{Gal}(K/F) \cong \mathrm{Gal}(K'/F')$.

Problem 7.2.3. [DF, page 603, problem 10]
Explain in one-sentence why $\mathbb{Q}(\sqrt[3]{2})$ is not a subfield of any cyclotomic field over $\mathbb{Q}$.

Problem 7.2.4. Determine all subfields of $\mathbb{Q}(\zeta_8)$ over $\mathbb{Q}$ and their corresponding group under Galois theory.

Problem 7.2.5. [A, page 583, problem 1]
Let K be a Galois extension of F whose Galois group is the symmetric group S_4. What numbers occur as degrees of elements of K over F?

Problem 7.2.6. Let q denote a power of a prime p. Show that the extension $\mathbb{F}_q(t^{1/n})$ over $\mathbb{F}_q(t)$ is Galois if and only if $q \equiv 1 \bmod n$. In this case, describe the Galois group $\mathrm{Gal}(\mathbb{F}_q(t^{1/n})/\mathbb{F}_q(t))$ and its action on $t^{1/n}$.

Problem 7.2.7. [DF, page 603, problem 10]
Prove that $\mathbb{Q}(\sqrt[3]{2})$ is not a subfield of any cyclotomic field over $\mathbb{Q}$.

Problem 7.2.8. Let G be a Hausdorff topological group and H a closed subgroup. Let $\pi : G \to G/H$ denote the quotient map. Show that G/H admits a natural topology so that a subset U of G/H is open if and only if $\pi^{-1}(U)$ is open. Prove that this topology is Hausdorff.

Problem 7.2.9. (an explicit version of above) Let G be a profinite group and let H be a closed normal subgroup. Prove that for any open normal subgroup N of G, the image of $H \to G/N$ denoted by H_N is a normal subgroup of G/N. Now if $N \subseteq N'$ is an inclusion of open normal subgroups of G, then $H_N \to H_{N'}$ is surjective. Show that

$$H \cong \varprojlim_{N \triangleright G \text{ open normal}} H_N.$$

7.3. **Standard questions.** (Please choose 10 problems from the following questions)

Problem 7.3.1. [DF, page 582, problem 14]

Show that $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ is a Galois extension of $\mathbb{Q}$ and determine its Galois group (over $\mathbb{Q}$).

Problem 7.3.2. [DF, page 582, problem 16]

(1) Prove that $x^4 - 2x^2 - 2$ is irreducible over $\mathbb{Q}$.
(2) Show that the roots of this quartic are

$$\alpha_1 = \sqrt{1+\sqrt{3}}, \quad \alpha_2 = \sqrt{1-\sqrt{3}}, \quad \alpha_3 = -\sqrt{1+\sqrt{3}}, \quad \alpha_4 = -\sqrt{1-\sqrt{3}}.$$

(3) Let $K_1 = \mathbb{Q}(\alpha_1)$ and $K_2 = \mathbb{Q}(\alpha_2)$. Show that $K_1 \neq K_2$ and $K_1 \cap K_2 = \mathbb{Q}(\sqrt{3}) =: F$.
(4) Prove that K_1, K_2 and K_1K_2 are Galois over F with $\mathrm{Gal}(K_1K_2/F)$ the Klein 4-group. Write out the elements of $Gal(K_1K_2/F)$ explicitly. Determine all the subgroups of the Galois group and give their corresponding fixed subfields of K_1K_2 containing F.
(5) Prove that the splitting field of $x^4 - 2x^2 - 2$ over $\mathbb{Q}$ is of degree 8 with dihedral Galois group

Problem 7.3.3. Let K/F be a finite Galois extension with Galois group G, and let H be a subgroup and $E := K^H$.

(1) Show that every automorphism E fixing F can be extended to an automorphism K. (Explain how extension of embeddings into normal closure is used here.)
(2) Let N denote the subgroup of $\mathrm{Gal}(K/F)$ that stabilizes E. Show that there is a surjective map $N \to \mathrm{Aut}_F(E)$ can compute its kernel.
(3) Show that N is the normalizer of H inside G and thus $\mathrm{Aut}_F(K)$ is isomorphic to $N_G(H)/H$.

Problem 7.3.4 (Artin–Schreier extensions)**.** Let F be a field of characteristic $p > 0$. For each element $a \in F$, show that either $x^p - x - a$ is irreducible or it splits completely in $F[x]$. Moreover, show that in the former case, adjoining a zero β of $x^p - x - a$, $F(\beta)$ is a finite Galois extension of F. Describe explicitly the elements in $\mathrm{Gal}(F(\beta)/F)$.

Challenge: Show that if F has characteristic p, then all degree p cyclic extension of F is to adjoin a zero of $x^p - x - a$ for some $a \in F$.

Problem 7.3.5. [DF, page 595, problem 4]

Let $f(x) \in F[x]$ be an irreducible polynomial of degree n over the field F, let L be the splitting field of $f(x)$ over F and let α be a root of $f(x)$ in L. If K is any Galois extension of F, show that the polynomial $f(x)$ splits into a product of m irreducible polynomials each of degree d over K, where $d = [K(\alpha) : K] = [(L \cap K)(\alpha) : L \cap K]$ and $m = n/d = [F(\alpha) \cap K : F]$.

Problem 7.3.6. [DF, page 596, problem 5]

Let p be a prime and let F be a field. Let K be a Galois extension of F whose Galois group is a p-group (i.e., the degree $[K : F]$ is a power of p). Such an extension is called a *p-extension* (note that p-extensions are Galois by definition).

(1) Let L be a p-extension of K. Prove that the Galois closure of L over F is a p-extension of F.
(2) Give an example to show that (1) need not hold if $[K : F]$ is a power of p but K/F is not Galois.

Problem 7.3.7. [DN, page 298, problem 5]
Let $p_1, \dots, p_r$ be r different prime numbers. Determine the Galois group of $K = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_r})$ over $\mathbb{Q}$.

Problem 7.3.8. [DN, page 298, problem 10]
Let $F = \mathbb{F}_p(u)$. Let K denote the splitting field of $f(x) = x^{2p} + ux^p + u$ over F. (Why is this polynomial irreducible?)
(1) Determine the Galois group $\mathrm{Gal}(K/F)$ (in this case, it means an automorphism of K that is identity on F).
(2) Determine the fixed field of K under the action of $\mathrm{Gal}(K/F)$.
(3) Determine the separable closure of F inside K.

Problem 7.3.9. [DN, page 301, problem 30]
Let $f(x) \in \mathbb{Q}[x]$ be a polynomial of degree n ($n > 4$) and the splitting field E of $f(x)$ has Galois group S_n over $\mathbb{Q}$. Let α be a zero of $f(x)$ in E.

(1) Prove that the only automorphism of $\mathbb{Q}(\alpha)$ that fixes $\mathbb{Q}$ is the identity, and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$.
(2) For any other root β of $f(x)$, show that there are precisely $(n-1)!$ elements in $\mathrm{Gal}(E/\mathbb{Q})$ that takes α to β.

Problem 7.3.10. [A, page 575, problem 18]
(1) Let $f(x)$ be an irreducible separable polynomial over a field F, and let K be the splitting field of $f(x)$. Show that $\mathrm{Gal}(K/F)$ is a subgroup of S_n. (The action on the roots of $f(x)$ defines such a homomorphism.)
(2) If $f(x) = x^4 + bx^2 + c \in F[x]$, show that $\mathrm{Gal}(K/F)$ is a subgroup of D_4.

Problem 7.3.11. [A, page 578, problem 11]
Let K/F be a Galois extension whose Galois group is the symmetric group S_3. Is it true that K is the splitting field of an irreducible cubic polynomial over F?

Problem 7.3.12. [A, page 582, problem 9]
Let p be a prime, and let a be a rational number which is not a pth power. Let K be the splitting field of the polynomial $x^p - a$ over $\mathbb{Q}$.

(1) Prove that K is generated over $\mathbb{Q}$ by a pth root α of a and a primitive pth root ζ of unity.
(2) Prove that $[K : \mathbb{Q}] = p(p-1)$. (Think about how to write the answer rigorously.)
(3) Prove that the Galois group of $K/\mathbb{Q}$ is isomorphic to the semi-direct product $Z_p \rtimes (\mathbb{Z}/p\mathbb{Z})^\times$, or more explicitly the group of invertible matrices with values in $\mathbb{F}_p$ of the form $\left(\begin{smallmatrix} a & b \\ & 1 \end{smallmatrix}\right)$. Describe the actions of $\left(\begin{smallmatrix} a & \\ & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & b \\ & 1 \end{smallmatrix}\right)$, respectively.

Problem 7.3.13. [DF, page 653, problem 7]
Let $\mathbb{F}_4$ be the field with 4 elements, t a transcendental over $\mathbb{F}_4$, and $F = \mathbb{F}_4(t^4 + t)$ and $K = \mathbb{F}_4(t)$.

(1) Show that $[K : F] = 4$.
(2) Show that K is separable over F.
(3) Show that K is Galois over F.
(4) Describe the lattice of subgroups of the Galois group and the corresponding lattice of subfields of K, giving each subfield in the form $\mathbb{F}_4(r)$, for some rational function $r(t)$.

Problem 7.3.14. [DF, page 638, problem 17]
Let $D \in \mathbb{Z}$ be a squarefree integer and let $a \in \mathbb{Q}$ be a nonzero rational number. Show that $\mathbb{Q}(\sqrt{a\sqrt{D}})$ cannot be a cyclic extension of degree 4 over $\mathbb{Q}$.

Problem 7.3.15. [DF, page 617, problem 8]
Determine the Galois group of $x^4 + 2x^2 + x + 3$.

Problem 7.3.16. Determine the Galois group of $x^3 + x - 1$.

Problem 7.3.17. Let K/F be a Galois extension with Galois group $G = \mathrm{Gal}(K/F)$. Suppose that H is a *closed* normal subgroup of G. Then K^H is a Galois extension of F. Conversely, if E is an intermediate field of K/F such that E is normal over F, then $\mathrm{Gal}(K/E)$ is a closed normal subgroup.

Problem 7.3.18. [DF, page 645]
Let k be a field. Prove that automorphisms of the rational function field $k(t)$ which fix k are precisely the fractional linear transformations determined by $t \mapsto \frac{at+b}{ct+d}$ for $a, b, c, d \in k$, $ad - bc \neq 0$ (so $f(t) \in k(t)$ maps to $f(\frac{at+b}{ct+d})$).
The automorphism group $\mathrm{Aut}(k(x)/k) \cong \mathrm{PGL}_2(k) := \mathrm{GL}_2(k)/k^\times$. Here $\mathrm{GL}_2(k)$ is the group of 2×2 invertible matrices, and $k^\times$ denotes the subgroup of scalar matrices.

Problem 7.3.19. [DF, page 567, problem 8] and [DN, page 298, problem 10]
Let k be a field.
(1) Determine the fixed field of the automorphism $t \mapsto t + 1$ of $k(t)$.
(2) Prove that the automorphism group of $\mathbb{F}_2(t)$ is isomorphic to S_3, and its fixed field is $\mathbb{F}_2(u)$ with

$$u = \frac{(t^4 - t)^3}{(t^2 - t)^5} = \frac{(t^2 + t + 1)^3}{(t^2 - t)^2}$$

Problem 7.3.20. Let t be transcendental over $\mathbb{F}_3$, let $K = \mathbb{F}_3(t)$, let $G = \mathrm{Aut}(K/\mathbb{F}_3)$ (namely the group of automorphisms of K that is identity on $\mathbb{F}_3$). Let F be the fixed field of G.

(a) Prove that $G \cong S_4$ and deduce that there is a unique field E with $F \subset E \subset K$ and $[E : F] = 2$. [Recall that $G \cong \mathrm{PGL}_2(\mathbb{F}_3)$ from Problem 7.3.18; show that $\mathrm{PGL}_2(\mathbb{F}_3)$ permutes the 4 lines in a 2-dimensional vector space over $\mathbb{F}_3$ and the kernel of this permutation representation is the scalar matrices.]

(b) Complete the description of the lattice of subfields of K containing E:

$$
\begin{tikzcd}[column sep=small]
 & & & K = \mathbb{F}_p(t) \arrow[ddlll, dash] \arrow[ddll, dash] \arrow[ddl, dash] \arrow[dd, dash] \arrow[drr, dash] \arrow[drrr, dash] \arrow[drrrr, dash] & & & & \\
 & & & & & ** \arrow[dr, dash] & E\left(\frac{t^2+1}{t+1}\right) \arrow[d, dash] & ** \arrow[dl, dash] \\
E(t^3-t) \arrow[drrr, dash] & ** \arrow[drr, dash] & ** \arrow[dr, dash] & E\left(\frac{t^2+t}{(t-1)^3}\right) \arrow[d, dash] & & & ** \arrow[dlll, dash] & \\
 & & & E\left(\frac{(t^6+t^4+t^2+1)^2}{(t^3+t)^3}\right). & & & &
\end{tikzcd}
$$

Give each subfield in the form $E(r)$ for some rational function r.

Problem 7.3.21. Let K be a subfield of $\mathbb{C}$ maximal with respect to the property that $\sqrt{2} \notin K$.

(a) Show such a field K exists.
(b) Show that $\mathbb{C}$ is algebraic over K.
(c) Prove that every finite extension of K in $\mathbb{C}$ is Galois with Galois group a cyclic 2-group.
(d) Deduce that $[\mathbb{C} : K]$ is countable (and not finite).

7.4. **More difficult questions.** (Please choose 5 problems from the following questions) I strongly recommend trying out Problem 7.4.1.

Problem 7.4.1 (Riemann zeta function for $\mathbb{F}_p[t]$)**.** Let us first recall that Riemann zeta function is

$$\zeta_{\mathbb{Z}}(s) = \sum_{n\geq 1} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}}, \qquad \mathrm{Re}(s) > 1.$$

Its functional equation takes the following form:

$$\Lambda(s) = \Lambda(2-s), \qquad \text{where } \Lambda(s) = \pi^{-s/2}\Gamma(s/2)\cdot \zeta_{\mathbb{Z}}(s).$$

Maybe an appropriate way to think of this is: $\pi^{-s/2}\Gamma(s/2)$ is the "L-factor at ∞", so that when putting this in, the functional equation "looks nicer". (Don't worry too much of this for now; read on.)

Our goal is to understand the Riemann zeta function for $\mathbb{F}_p[t]$, where p is a prime number. The analogy goes as follows.

$$\big\{\text{positive integers } n \text{ in } \mathbb{Z}\big\} \longleftrightarrow \big\{\text{monic polynomials } f(t) \text{ in } \mathbb{F}_p[t]\big\}$$

$$\big\{\text{prime ideals } (p) \text{ in } \mathbb{Z}\big\} \longleftrightarrow \big\{\text{prime ideals } p(t) \text{ in } \mathbb{F}_p[t]\big\}$$

$$\big\{\text{prime numbers } p\big\} \longleftrightarrow \big\{\text{monic irreducible polynomials } p(t)\big\}$$

$$\text{value } n^{-s} = \big(\#\tfrac{\mathbb{Z}}{(n)}\big)^{-s} \longleftrightarrow \big(\#\tfrac{\mathbb{F}_p[t]}{(f(t))}\big)^{-s} = p^{-\deg f(x) s}$$

$$\zeta_{\mathbb{Z}}(s) = \sum_{n\geq 1}\tfrac{1}{n^s} = \prod_{p \text{ prime}} \tfrac{1}{1-p^{-s}} \longleftrightarrow \zeta_{\mathbb{F}_p[t]}(s) = \sum_{\text{monic poly } f(x)} \tfrac{1}{p^{\deg f\cdot s}} = \prod_{\text{monic irred } p(t)} \tfrac{1}{1-p^{-\deg p(t)\cdot s}}.$$

The L-factor at ∞ for $\mathbb{F}_p[t]$ is different from the case of $\mathbb{Z}$, this is because we can view the point really as the "infinity" point of $\mathbb{P}^1$; so the "L-factor at infinity" is $\frac{1}{1-p^{-s}}$. We also put

$$\Lambda_{\mathbb{F}_p[t]}(s) = \zeta_{\mathbb{F}_p[t]}(s)\cdot \frac{1}{1-p^{-s}}.$$

Compute explicitly $\zeta_{\mathbb{F}_p[t]}(s)$ and $\Lambda_{\mathbb{F}_p[t]}(s)$, and prove the corresponding functional equation. (In fact, $\zeta_{\mathbb{F}_p[t]}(s)$ is a rational function in p^{-s}.) This is a very very special case of so-called Weil conjecture, an analogue of the Riemann zeta function for function fields.

Problem 7.4.2. [Yau contest 2017]

Let p be a prime number and let $K = \mathbb{F}_p(T)$ be the field of rational functions over $\mathbb{F}_p$. Consider the polynomials

$$f(X) = X^p - TX - T, \quad g(X) = X^{p-1} - T.$$

(1) Show that f and g are irreducible and separable over K.

(2) Let M be the splitting field of g over K. Show that $\mathrm{Gal}(M/K)$ is isomorphic to $\mathbb{F}_p^\times$.

(3) Let L be the splitting field of f over K. Show that g splits in L and $\mathrm{Gal}(L/K)$ is isomorphic to the semidirect product $G = \mathbb{F}_p \rtimes \mathbb{F}_p^\times$, where $\mathbb{F}_p^\times$ acts on $\mathbb{F}_p$ by homotheties.

Problem 7.4.3. Recall our group theoretical statement: if H_1 and H_2 are normal subgroups of a group G such that $H_1 \cap H_2 = \{1\}$, then $G \cong H_1 \times H_2$.

Let L be a finite extension of F (as an ambient big fields so that the intersection below makes sense. Let K_1 and K_2 be intermediate fields that are finite Galois extensions of a field F.

- Then the intersection $K_1 \cap K_2$ is Galois over F.
- The composite K_1K_2 is Galois over F. The Galois group is isomorphic to the subgroup
$$H = \{(\sigma, \tau) \mid \sigma|_{K_1\cap K_2} = \tau|_{K_1\cap K_2}\}$$
of the direct product $\mathrm{Gal}(K_1/F)\times\mathrm{Gal}(K_2/F)$ consisting of elements whose restriction to $K_1 \cap K_2$ are equal.
- In the special case that $F = K_1 \cap K_2$, show that this implies that
$$\mathrm{Gal}(K_1K_2/F) \cong \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F).$$

(This is Proposition 21 on page 592 of [DF]. But I recommend you try to prove the statement on yourself first.)

Problem 7.4.4. Show that there is no automorphism of $\mathbb{R}$ that fixes $\mathbb{Q}$.

(Some list of steps can be found on page 567, problem 7 of [DF]. But you should be able to work that out on your own.)

Problem 7.4.5. [DF, page 584, problem 27]

Let $\alpha = \sqrt{(2+\sqrt{2})(3+\sqrt{3})}$ and consider the extension $E = \mathbb{Q}(\alpha)$.

(1) Show that $\alpha = (2+\sqrt{2})(3+\sqrt{3})$ is not a square in $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
(2) Conclude from (1) that $[E : \mathbb{Q}] = 8$. Prove that the roots of the minimal polynomial over $\mathbb{Q}$ for α are 8 elements $\pm\sqrt{(2\pm\sqrt{2})(3\pm\sqrt{3})}$
(3) Let $\beta = \sqrt{(2-\sqrt{2})(3+\sqrt{3})}$. Show that $\alpha\beta \in F$. And make similar arguments to show that E is Galois over $\mathbb{Q}$. Show moreover that the Galois group is determined by mapping α to one of the 8 elements in (2).
(4) Let $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ be the automorphism that sends α to β. Show that σ has order 4 in $\mathrm{Gal}(E/\mathbb{Q})$.
(5) Show that $\mathrm{Gal}(E/\mathbb{Q}) \cong Q_8$, the quaternion group of order 8.

(Some hints might be found on page 584 of [DF])

Problem 7.4.6. Show that if H is a subgroup of a group G of index n, then the normal subgroup
$$N := \bigcap_{g\in G} gHg^{-1} \subseteq G$$
has index $\leq n!$

(I agree that this is a group theory question. But let me explain why I think this is correct using Galois theory: suppose that we are in the situation that K/F is a Galois extension of fields with Galois group G, and then $E := K^H$ is a subfield such that $[E : F] = n$. From this, we see that $g(E) = K^{gHg^{-1}}$ are conjugates of E. By Galois theory, K^N is the composite of all $g(E)$ for every $g \in \mathrm{Gal}(K/F)$; it is the normal closure of E over F. We have shown in class that the normal closure of a finite extension E/F of degree n has at most degree $\leq n!$. This would imply that $[G : N] \leq n!$, at least when these groups can be realized as Galois groups. Interesting exercise: can you prove the purely group theoretic statement? Or can you “explain” how your argument relates to the Galois theory argument I just give?)

Problem 7.4.7. [A, page 584, problem 10]

Let K be a finite extension of a field F, and let $f(x) \in K[x]$. Prove that there exists a nonzero polynomial $g(x) \in K[x]$ such that $f(x)g(x) \in F[x]$.

Problem 7.4.8. What do finite order elements in $\mathrm{SL}_2(\mathbb{Q})$ look like? (Hint: look at the eigenvalues of these matrices.)

Problem 7.4.9. [Yau contest 2010]

For a positive integer a, consider the polynomial

$$f_a = x^6 + 3ax^4 + 3x^3 + 3ax^2 + 1.$$

Show that it is irreducible. Let F be the splitting field of f_a. Show that its Galois group is solvable.

Problem 7.4.10. [H, page 278, problem 14]

Here is a method for constructing a polynomial $f(x) \in \mathbb{Q}[x]$ with Galois group S_n for a given $n > 3$. It depends on the fact that there exist irreducible polynomials of every degree in $\mathbb{F}_p[x]$ for every prime p. First choose monic polynomials $f_1, f_2, f_3 \in \mathbb{Z}[x]$ such that

(i) $\deg f_2 = n$ and $\bar{f}_2 \in \mathbb{F}_2[x]$ is irreducible.
(ii) $\deg f_3 = n$ and $\bar{f}_3 \in \mathbb{F}_3[x]$ factors in $\mathbb{F}_3[x]$ as gh with g irreducible of degree $n-1$ and h linear.
(iii) $\deg f_5 = n$ and $\bar{f}_5 \in \mathbb{F}_5[x]$ factors as gh or gh_1h_2 with g irreducible quadratic in $\mathbb{F}_5[x]$ and h, h_1, h_2 irreducible polynomials of odd degree in $\mathbb{F}_5[x]$.

(1) Let $f = -15f_2 + 10f_3 + 6f_5$ (so that it is monic and $f \equiv f_2 \bmod 2$, $f \equiv f_3 \bmod 3$, and $f \equiv f_5 \bmod 5$). Let K be the splitting field of $f(x)$ over $\mathbb{Q}$ and $G := \mathrm{Gal}(K/\mathbb{Q})$. Show that G acts transitively on the roots of f. (Use f_2.)
(2) Show that G contains a cycle of the type $(i_1 i_2 \cdots i_{n-1})$ and element $\sigma\lambda$ where σ is a transposition and λ is a product of cycles of odd order.
(3) Show that $\sigma \in G$ and thus $(i_k i_n) \in G$ for some $k \in \{1, \dots, n-1\}$.
(4) Deduce that $G = S_n$.

Problem 7.4.11 (Classical Gauss sum)**.** [DF, page 637, problem 11]

Let $K = \mathbb{Q}(\zeta_p)$ be the cyclotomic field of p^{th} roots of unity for the odd prime p, viewed as a subfield of $\mathbb{C}$, and let $G = \mathrm{Gal}(K/\mathbb{Q})$. Let H denote the subgroup of index 2 in the cyclic group G. Define

$$\eta_0 = \sum_{\tau \in H} \tau(\zeta_p), \quad \eta_1 = \sum_{\tau \in \sigma H} \tau(\zeta_p),$$

where σ is a generator of $\mathrm{Gal}(K/\mathbb{Q})$ (the two *periods* of ζ_p with respect to H, i.e., the sum of the conjugates of ζ_p with respect to the two cosets of H in G).

(1) Prove that $\sigma(\eta_0) = \eta_1$, $\sigma(\eta_1) = \eta_0$ and that

$$\eta_0 = \sum_{a=\text{square}} \zeta_p^a, \qquad \eta_0 = \sum_{b \neq \text{square}} \zeta_p^b,$$

where the sums are over the squares and nonsquares (respectively) in $(\mathbb{Z}/p\mathbb{Z})^\times$.
(2) Prove that $\eta_0 + \eta_1 = -1$.
(3) Let $g = \sum_{i=0}^{i-1} \zeta_p^{i^2}$ (the classical Gauss sum). Prove that

$$g = \sum_{i=0}^{p-2} (-1)^i \sigma^i(\zeta_p).$$

(4) Prove that $\tau(g) = g$ if $\tau \in H$ and $\tau(g) = -g$ if $\tau \notin H$. Conclude in particular that $[\mathbb{Q}(g) : \mathbb{Q}] = 2$. Recall that complex conjugation is the automorphism σ_{-1} on K.

Conclude that $\bar{g} = g$ if -1 is a square mod p (i.e., if $p \equiv 1 \bmod 4$) and $\bar{g} = -g$ if -1 is not a square mod p (i.e., if $p \equiv 3 \bmod 4$) where $\bar{g}$ denotes the complex conjugate of g.

(5) Prove that $\bar{g}g = p$.

(6) Conclude that $g^2 = (-1)^{(p-1)/2}p$ and that $\mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})$ is the unique quadratic subfield of $\mathbb{Q}(\zeta_p)$.

Problem 7.4.12. [Alibaba 2021]

Find all real numbers of the form $\sqrt[p]{2021 + \sqrt[q]{a}}$ that can be expressed as a linear combination of roots of unity with rational coefficients, where

- p and q are (possibly the same) prime numbers, and
- $a > 1$ is an integer, which is not a qth power.