2023 Fall Honors Algebra Exercise 6 (due on December 7)

For submission of homework, please finish the 20 True/False problems, 5 examples/counterexample problems, and choose 7 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.

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

(1) A field extension of degree 2 is always normal.
(2) A field extension of degree 2 is always separable.
(3) For a finite field extension K over F, one can find always find an element $\alpha \in K$ such that $K = F(\alpha)$.
(4) A finite extension of a perfect field can be generated by one element.
(5) If L/K is the splitting field of $f(x) \in K[x]$, then for any intermediate field E of L/K, L is a splitting field of $f(x)$ over E.
(6) Let p be a prime number. The additive group of a finite field of p^n elements is a cyclic group of order p^n.
(7) If p is a prime number, there exists an irreducible polynomial of degree p in $\mathbb{F}_p[x]$.
(8) Every finite extension of a finite field is separable.
(9) If all finite extensions of F are separable, then F is a perfect field.
(10) If F is a perfect field, then any field extension of F is a perfect field.
(11) Let K/F be a finite Galois extension of fields with Galois group G. Then G is a simple group if and only if there is no intermediate field E that is Galois over F (except for K and F themselves).
(12) Let K/F be a finite Galois extension of fields with Galois group G. Then G is a simple group if and only if there is no intermediate field E such that K is Galois over E (except for K and F themselves).
(13) The Galois group of a finite extension of finite fields is always abelian.
(14) The Galois group of the splitting field of $\Phi_n(x)$ over $\mathbb{Q}$ is cyclic.
(15) Let K_1 and K_2 be two Galois extensions of F such that $\mathrm{Gal}(K_1/F) \cong \mathrm{Gal}(K_2/F)$, then $K_1 \cong K_2$.
(16) Let K be a finite Galois extension of F. If two intermediate fields K_1 and K_2 satisfies $\mathrm{Gal}(K/K_1)$ is isomorphic to $\mathrm{Gal}(K/K_2)$, then $K_1 = K_2$.
(17) Let K/F be a finite cyclic extension of fields of degree n. Then for each divisor d of n, there is a unique intermediate field of K/F that has degree d over F.
(18) $\mathbb{F}_5(y)$ is a separable extension of $\mathbb{F}_5(y^{10})$.
(19) If $f(x) \in F[x]$ is an irreducible polynomial and if α is a simple zero of $f(x)$ in some field extension of F, then the splitting field of $f(x)$ over F is separable over F.
(20) Let K be a finite extension of degree n of a *finite* field F. Then for each positive integer $d|n$, there is a unique *subfield* E of K containing F such that E is a finite extension of F of degree d.

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

Problem 6.2.1. Prove that the cardinality of every finite field is a power of a prime.

Problem 6.2.2. List all subfields of $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.
List all subfields of $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$.
Write these fields as a tower of fields.

Problem 6.2.3. Determine the splitting field of $x^6 + 2x^3 + 2$ over $\mathbb{F}_3$.

Problem 6.2.4 (DN, page 234, problem 6)**.** Find a basis of the following field extensions:
(1) $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$
(2) $K = \mathbb{Q}(\sqrt{3}, \sqrt{-1}, \omega)$ with $\omega = \frac{1}{2}(-1 + \sqrt{-3})$.

Problem 6.2.5. If F is a field that is not perfect, show that F has a nontrivial purely inseparable extension.

Problem 6.2.6. [DF, page 551, problem 6]
Let p be a prime number and $n \in \mathbb{N}$. Prove that $x^{p^n-1} - 1 = \prod_{\alpha \in \mathbb{F}_{p^n}^\times}(x - \alpha)$. Conclude that $\prod_{\alpha \in \mathbb{F}_{p^n}^\times} \alpha = (-1)^{p^n}$.
Derive from this the Wilson's Theorem: for odd prime p, $(p-1)! \equiv -1 \pmod{p}$.

Problem 6.2.7. [H, page 268, problem 12]
Let $K/E/F$ be algebraic field extensions.
(1) If $u \in K$ is separable over F, then u is separable over E.
(2) If K is separable over F, then K is separable over E and E is separable over F.

Problem 6.2.8. Let F be a field of characteristic $p > 0$. Prove that
(1) Let $f(x) \in F[x]$ be an irreducible polynomial with degree relatively prime to p. Then $f(x)$ is separable over F.
(2) Show that if an extension K/F has degree $[K : F]$ relatively prime to p, then K/F is separable.

Problem 6.2.9. [DF, page 555, probem 6]
Prove that for n odd, $n > 1$, $\Phi_{2n}(x) = \Phi_n(-x)$.

Problem 6.2.10. Let K/F be a finite separable extension. Then a normal closure of K/F is also separable over F.

Problem 6.2.11. Let $\zeta = \zeta_{11}$. Show that $\alpha := \zeta + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^9$ generates a field of degree 2 over $\mathbb{Q}$ and find its equation.
(Is there a reason to understand why this sum of powers of ζ is special?)

6.3. **Examples and counterexamples.** (Answer all 5 problems below. Only give the examples; no need to explain why.)

Problem 6.3.1. Give an example of a perfect field of positive characteristic that is not finite.

Problem 6.3.2. Give an example of a field extension that is algebraic but not finite.

Problem 6.3.3. Give an example of an extension of degree 2 that is not separable.

Problem 6.3.4. Give an example of a field extension K over F and two intermediate fields K_1 and K_2 of F such that

$$[K_1 K_2 : F] \neq [K_1 : F] \cdot [K_2 : F].$$

Problem 6.3.5. Give an example of a field F and two finite extensions K_1 and K_2 such that

- $[K_1 : F] \neq [K_2 : F]$
- K_1 is abstractly isomorphic to K_2.

6.4. **Standard questions.** (Please choose 8 problems from the following questions)

Problem 6.4.1. [DF, page 545, problems 3, 4]
Determine the splitting field and its degree over $\mathbb{Q}$ of $x^4 + x^2 + 1$, and of $x^6 - 4$.

Problem 6.4.2. [DF, page 545, problems 5 and 6]
Let K be a finite extension of F and let K_1 and K_2 intermediate fields that are normal extensions of F. Given one-line argument to show that both K_1K_2 and $K_1 \cap K_2$ are normal extensions of F.

Problem 6.4.3. [DN, page 234, problem 14]
If $F \subseteq K \subseteq L$ is a tower of field extensions and if K/F and L/K are normal extensions, is it true that L/F is normal? If true, prove it, otherwise, give a counterexample.

Problem 6.4.4. [DN, page 234, problems 17 and 18]
Let K and L be two intermediate fields of the field extension E/F. Show that

(1) if K/F is normal, then the composite KL is normal over L; and
(2) if K/F and L/F are both normal, then the composite KL and the intersection $K \cap L$ are both normal in F.

Problem 6.4.5. [DN, page 235, problem 19]
Let E/F be a finite normal extension and let $f(x) \in F[x]$ be an irreducible polynomial. Prove that $f(x)$ factors on E as the product

$$f(x) = (f_1(x)f_2(x)\cdots f_r(x))^{p^e}$$

with $e \geq 0$ and all $f_i(x)$ having the *same* degree.

Problem 6.4.6. [DN, page 235, problem 22]
Let $\mathbb{F}_p$ be the finite field of p elements (p a prime number), and $f(x) \in \mathbb{F}_p[x]$ an irreducible polynomial of degree n. Let $P_d(x)$ denote the product of all monic irreducible polynomials of degree d. Prove that

(1) $f(x) | x^{p^m} - x$ if and only if $n|m$;
(2) $(x^{p^n} - x) | (x^{p^m} - x)$ if and only if $n|m$;
(3) $x^{p^n} - x = \prod_{d|n} P_d(x)$;
(4) $P_n(x) = \prod_{d|n} (x^{p^d} - x)^{\mu(n/d)}$, where $\mu(n)$ is the Mobius function;
(5) Show that the number of irreducible monic polynomials of degree n is

$$N_n = \frac{1}{n} \sum_{d|n} \mu\Big(\frac{n}{d}\Big) p^d.$$

Problem 6.4.7. [DN, page 236, problem 27]
Let F be a field of characteristic $p > 0$ and let $a \in F$ but $a \notin F^p$. Then $x^{p^e} - a$ with $e \geq 1$ is irreducible over F.

Problem 6.4.8. Write $\zeta_{13} = e^{2\pi i/13}$.
(1) Find a generator for the unique cubic subfield of $\mathbb{Q}(\zeta_{13})$.
(2) Find the minimal polynomial of that generator over $\mathbb{Q}$.

Problem 6.4.9. [DF, page 556, problem 8]

Let ℓ be a prime and let $\Phi_\ell(x) = \frac{x^\ell - 1}{x-1} = x^{\ell-1}+x^{\ell-2}+\cdots+x+1 \in \mathbb{Z}[x]$ be the ℓth cyclotomic polynomial, irreducible in $\mathbb{Z}[x]$. This exercise determines the factorization of $\Phi_\ell(x)$ modulo p for any prime p. Let ζ denote any fixed primitive ℓth root of unity.

(1) Show that if $p = \ell$ then $\Phi_\ell(x) = (x-1)^{\ell-1} \in \mathbb{F}_\ell[x]$.
(2) Suppose $p \neq \ell$ and let f denote the order of p mod ℓ, i.e., f is the smallest power of p with $p^f = 1$ mod ℓ. Show that $n = f$ is the smallest power p^n of p that contains a primitive ℓth root of unity ζ, i.e. a zero of $\Phi_\ell(x)$ mod p. Conclude that the minimal polynomial of ζ over $\mathbb{F}_p$ has degree f.
(3) Show that $\mathbb{F}_p(\zeta) = \mathbb{F}_p(\zeta^a)$ for any integer a not divisible by ℓ. Conclude using (2) that, in $\mathbb{F}_p[x]$, $\Phi_\ell(x)$ is the product of $\frac{\ell-1}{f}$ distinct irreducible polynomials of degree f.
(4) In particular, prove that, viewed in $\mathbb{F}_p[x]$, $\Phi_7(x) = x^6 + x^5 + \cdots + 1$ is $(x-1)^6$ for $p = 7$, a product of distinct linear factors for $p \equiv 1 \bmod 7$, a product of 3 irreducible quadratics for $p \equiv 6 \bmod 7$, a product of 2 irreducible cubics for $p \equiv 2, 4 \bmod 7$, and is irreducible for $p \equiv 3, 5 \bmod 7$.

Problem 6.4.10. [DF, page 595, problem 3]

Let F be a field contained in the ring of $n \times n$ matrices over $\mathbb{Q}$. Prove that $[F : \mathbb{Q}] \leq n$. (Hint: Cayley–Hamilton theorem.)

Problem 6.4.11. [DF, page 603, problem 7]

Show that complex conjugation restricts to the automorphism $\sigma_{-1} \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ of the cyclotomic field of nth roots of unity. Show that the field $K^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ is the subfield of real elements in $K = \mathbb{Q}(\zeta_n)$, called the *maximal real subfield* of K.

Problem 6.4.12. [DF, page 603, problem 11]

Prove that the primitive n^{th} roots of unity form a basis over $\mathbb{Q}$ for the cyclotomic field of n^{th} roots of unity if and only if n is squarefree.

Problem 6.4.13. [DF, page 617, problem 3]

Prove that for any $a, b \in \mathbb{F}_{p^n}$ that if $x^3 + ax + b$ is irreducible then $-4a^3 - 27b^2$ is a square in $\mathbb{F}_{p^n}$.

Problem 6.4.14. Let $F \subseteq E$ be finite fields, where $|F| = q < \infty$ and $[E : F] = n$.

(1) Prove that every monic irreducible polynomial in $F[X]$ of degree dividing n is the minimal polynomial over F of some element of E.

(2) Compute the product of all the monic irreducible polynomials in $F[X]$ of degree dividing n.

(3) Suppose $|F| = 2$. Determine the number of monic irreducible polynomials of degree 10 in $F[X]$.

Problem 6.4.15. Let k be a perfect field of characteristic $p > 0$. Let $F = k(t)$ be the field of rational functions in one variable over k. Show that every finite extension E of F can be generated by one element, that is, there exists $\alpha \in E$ such that $E = F(\alpha)$.

6.5. **More difficult questions.** (Please choose 4 problems from the following questions)

Problem 6.5.1. [DN, page 220, Lemma 2]

Let F be a field of characteristic $p > 0$ and $a \in F$. Then $x^p - a$ is either irreducible or it factors completely as $x^p - a = (x-b)^p$ for some $b \in F$.

Problem 6.5.2. Let K/F be a finite extension.

(1) Show that $K^s := \{\alpha \in K \text{ separable over } F\}$ is the maximal intermediate field that is separable over F.

Define

$$[K : F]_s := [K^s : F] \quad \text{and} \quad [K : F]_i := [K : K^s].$$

(2) Show that, if E is a normal extension of F that contains K, then

$$|\mathrm{Hom}_F(K, E)| = |\mathrm{Hom}_F(K^s, E)| = [K : F]_s.$$

(The latter equality is a theorem from the class; so no need to prove.)

(3) Show that if $L/K/F$ be finite extensions, then

$$[L : F]_s = [L : K]_s \cdot [K : F]_s \quad \text{and} \quad [L : F]_i = [L : K]_i \cdot [K : F]_i.$$

Challenge: What if we only assume K/F is algebraic? (Tricky part: even if an extension is infinite, the separable or the inseparable degrees could still be finite.)

Problem 6.5.3. [DF, page 551, problem 5] and Yau contest 2021

For any prime p and any nonzero $a \in \mathbb{F}_p$ prove that $x^p - x + a$ is irreducible and separable over $\mathbb{F}_p$.

(There are hints on the book.)

Problem 6.5.4. [H, page 282, problem 9]

If $n \geq 3$, then $x^{2^n} + x + 1$ is *reducible* in $\mathbb{F}_2$.

Problem 6.5.5. [DN, page 237, problems 38 and 39]

(1) Let K/F be a simple algebraic extension. Let $K = F(\theta)$. Let L be an intermediate field of K/F. Show that the minimal polynomial of θ over L: $g(x) = x^r + \alpha_1 x^{r-1} + \cdots + \alpha_r$, satisfies that $F(\alpha_1, \ldots, \alpha_r) = L$. From this, deduce that a simple algebraic extension can only have finitely many intermediate fields.

(2) Let F be an infinite field and K/F an algebraic extension. Show that if K/F has only finitely many intermediate field, then for every elements $\alpha, \beta \in K$, the composite of $F(\alpha)$ and $F(\beta)$ inside K is still a simple extension of F.

From this, deduce that if an algebraic extension K/F has only finitely many intermediate fields, then K/F is a simple extension.

Problem 6.5.6. [DF, page 556, problems 10 and 12]

Let φ denote the Frobenius map $x \mapsto x^p$ on the finite field $\mathbb{F}_{p^n}$. Prove that φ^n is the identity map and no lower power of φ is the identity.

Determine the Jordan canonical form over $\mathbb{F}_p$ when viewing φ as an $\mathbb{F}_p$-linear operator on the n-dimensional $\mathbb{F}_p$-vector space $\mathbb{F}_{p^n}$. (What if $p|n$?) Here, by Jordan canonical form, we meant to first write φ in terms of an $n \times n$ matrix (with entries in $\mathbb{F}_p$) and then take the compute the canonical form in an extension $\mathbb{F}_{p^N}$ of $\mathbb{F}_p$ (for N sufficiently divisible).

Problem 6.5.7. [DF, page 556, problem 13] (Wedderburn's Theorem on Finite Division Rings)

This exercises aim to prove Wedderburn's Theorem that a finite division ring D is a field (i.e. is commutative).

(1) Let Z denote the center of D. Prove that Z is a field containing $\mathbb{F}_p$ for some prime p. If $Z = \mathbb{F}_q$, prove that D has order q^n for some integer n.

(2) The nonzero elements $D^\times$ of D form a multiplicative group. For any $x \in D^\times$ show that the elements of D which commute with x form a division ring which contains Z.

Show that this division ring is of order q^m for some integer m and that $m < n$ if x is not an element of Z.

Show that the class equation for the group $D^\times$ is

$$q^n - 1 = (q-1) + \sum_{i=1}^{r} \frac{q^n - 1}{|C_{D^\times}(x_i)|},$$

where $x_1, \dots, x_r$ are representatives of the distinct conjugacy classes in $D^\times$ not contained in the center of $D^\times$.

Conclude from (2) that for each i, $|C_{D^\times}(x_i)| = q^{m_i} - 1$ for some $m_i < n$.

(4) Prove that since $\frac{q^n-1}{q^{m_i}-1}$ is an integer (being the index $[D^\times : C_{D^\times}(x_i)]$), then m_i divides n.

Conclude that the integer $\Phi_n(q)$ divides $(q^n-1)/(q^{m_i}-1)$ for $i = 1, \dots, r$.

(5) Prove that (3) and (4) implies that $\Phi_n(q) = \prod_{\zeta \text{primitive}}(q - \zeta)$ divides $q-1$. Prove that $|q - \zeta| > q - 1$ (in terms of complex absolute values) for any root of unity $\zeta \neq 1$. Conclude that $n - 1$, i.e. $D = Z$ is a field.

Problem 6.5.8. (Transcendental degree, following [Ar, page 525-526]) Let K be a field extension of F. We say a set of elements $\{\alpha_1, \dots, \alpha_n\} \subset K$ is *algebraically independent over* F if there is a nonzero polynomial in n variables $f(x_1, \dots, x_n) \in F[x_1, \dots, x_n]$ such that

$$f(\alpha_1, \dots, \alpha_n) = 0.$$

If no such nonzero polynomial f exist, we say that $\{\alpha_1, \dots, \alpha_n\}$ is algebraically independent.

(1) Show that $\{\sqrt{\pi}, \sqrt[4]{\pi}\sqrt{\pi - 1}\}$ is algebraically dependent over $\mathbb{Q}$.

(2) Show that if $\alpha_1, \dots, \alpha_n$ are algebraically independent over F, then $F(\alpha_1, \dots, \alpha_n)$ is isomorphic to $F(x_1, \dots, x_n)$ of rational functions in $x_1, \dots, x_n$.

We say that $\{\alpha_1, \dots, \alpha_n\}$ is a *transcendental basis* of K over F if $\{\alpha_1, \dots, \alpha_n\}$ is linearly independent over F, and K is an algebraic extension over $F(\alpha_1, \dots, \alpha_n)$.

(3) Let $\{\alpha_1, \dots, \alpha_m\}$ and $\{\beta_1, \dots, \beta_n\}$ be elements in an extension K of a field F. Assume that K is algebraic over $F(\beta_1, \dots, \beta_n)$ and that $\alpha_1, \dots, \alpha_m$ are algebraically independent over F. Then $m \leq n$, and $\{\alpha_1, \dots, \alpha_m\}$ can be completed into a transcendental basis for K by adding at most $(n - m)$ elements from $\{\beta_1, \dots, \beta_n\}$.

(Corollary of (3): when K has a (finite) transcendental basis over F, we may define its transcendental degree over F to be, tr.deg(K/F) the cardinality of a transcendental basis. By (3), such number does not depend on the choice of transcendental bases.)

Note: examples of transcendental extensions to keep in minds include $\mathbb{Q}(x)(\sqrt{x^3 - x})$ (having transcendental degree 1).

Problem 6.5.9 (Chevalley–Warning problem)**.** Let $\mathbb{F}_q$ be a finite field of cardinality $q = p^r$.

(a) Let $0 \leq a < q - 1$ be an integer. Show that

$$S(X^a) := \sum_{a \in \mathbb{F}} x^a$$

is equal to 0. Here we adopt the convention that $a^0 = 1$ in $\mathbb{F}_q$ even for $x = 0$.

(b) Let $f_1, \ldots, f_m \in \mathbb{F}_q[X_1, \ldots, X_n]$ be polynomials in n variables satisfying

$$\sum_{i=1}^{m} \deg(f_i) < n.$$

Show that $P = \prod_{i=1}^{m}(1 - f_i^{q-1})$ satisfies

$$S(P) := \sum_{(x_1,\ldots,x_n)\in\mathbb{F}_q^n} P(x_1, \ldots, x_n)$$

Deduce that p divides the cardinality of the set

$$V = \left\{(x_1, \ldots, x_n) \in \mathbb{F}_q^n \,\middle|\, f_i(x_1, \ldots, x_n) = 0,\ \forall i\right\}.$$

(c) When f_i are homogeneous polynomials satisfying $f_i(0, \ldots, 0) = 0$ for all i and $\sum_{i=1}^{m} \deg(f_i) < n$, show that $f_1, \ldots, f_n$ has a common zero in the projective space $\mathbb{P}^n(\mathbb{F}_q)$.