E. Dummit's Math 5111 $\sim$ Algebra 1, Fall 2020 $\sim$ Homework 6, due Fri Oct 23rd.

Justify all responses with proof and in complete sentences unless otherwise stated. Write up your solutions cleanly and neatly, and clearly identify all problem numbers. You may use results from earlier parts of problems in later parts, even if you were unable to solve the earlier parts.

---

1. Let F be a field. We say that a polynomial $q(x) \in F[x]$ is "consecutive-root" if there exists some root α of q (in some splitting field K/F) such that $\alpha + 1$ is also a root of q.

   (a) Suppose $q(x)$ is nonconstant and $q(x) = q(x+1)$. Show that q is consecutive-root.

   (b) Suppose that $q(x)$ is irreducible and consecutive-root. Show that $q(x) = q(x+1)$. [Hint: Consider the gcd of $q(x)$ and $q(x+1)$.]

   (c) Show that there are no irreducible consecutive-root polynomials in $\mathbb{Q}[x]$, and that any irreducible consecutive-root polynomial in $\mathbb{F}_p[x]$ must have degree divisible by p.

   (d) If p is prime and $a \in \mathbb{F}_p$ is nonzero, show that the polynomial $q(x) = x^p - x + a \in \mathbb{F}_p[x]$ is separable, consecutive-root, and irreducible. [Hint: For the irreducibility, first show that the roots are of the form α, $\alpha+1$, $\alpha+2$, ..., $\alpha+(p-1)$, and then use the fact that the sum of the roots of $(x-r_1)(x-r_2)\cdots(x-r_n)$ is a coefficient of the polynomial to obtain a contradiction.]

---

2. Let $\overline{\mathbb{Q}}$ denote the algebraic closure of $\mathbb{Q}$. Recall that we have shown that $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$.

   (a) Show in fact that $\overline{\mathbb{Q}}$ is not even finitely generated over $\mathbb{Q}$: in other words, that there cannot exist elements $r_1, r_2, \dots, r_n \in \overline{\mathbb{Q}}$ such that $\overline{\mathbb{Q}} = \mathbb{Q}(r_1, r_2, \dots, r_n)$.

   (b) Show that $\overline{\mathbb{Q}}$ is the algebraic closure of any of its subfields.

---

3. Let p and q be distinct primes, and set $\alpha = q^{1/p}$ and $\beta = p^{1/q}$.

   (a) Let F be a subfield of $\mathbb{R}$ not containing α. If $\alpha^n \in F$ for some $n > 0$, show that $p|n$.

   (b) Let F be a subfield of $\mathbb{R}$ not containing α. Show that $[F[\alpha] : F] = p$. [Hint: Consider the constant term of the minimal polynomial of α over F.]

   (c) Prove that $[\mathbb{Q}(\alpha + \beta) : \mathbb{Q}] = pq$.

---

4. Let F be a field of characteristic $p > 0$ and $g(x) \in F[x]$ be monic, irreducible, and such that not all its coefficients are pth powers in F. The goal of this problem is to show that the polynomial $f(x) = g(x^p)$ is an irreducible inseparable polynomial in $F[x]$, which extends the result we showed in class (namely, that $x^p - \beta$ is irreducible if β is not a pth power).

   (a) First suppose that f factors as $f = f_1 f_2$ where f_1 and f_2 are relatively prime and nonconstant. Show that $f_1'(x) = f_2'(x) = 0$. Deduce that $f_1(x) = g_1(x^p)$ and $f_2(x) = g_2(x^p)$ for some g_1, g_2, and obtain a contradiction.

   (b) Now suppose that $f(x) = [f_1(x)]^n$ for some integer $n > 1$ that is not divisible by p. Show that $f_1'(x) = 0$ and obtain a contradiction.

   (c) Finally, suppose that $f(x) = [f_1(x)]^p$ for some polynomial f_1. Show that all coefficients of f are pth powers, and obtain a contradiction.

   (d) Deduce that $f(x) = g(x^p)$ must be irreducible.

---

5. Let t be an indeterminate over the field $\mathbb{C}$, and let $F = \mathbb{C}(t, \sqrt{1-t^2})$.

   (a) Prove that $F/\mathbb{C}$ has transcendence degree 1.

   (b) Prove that F is purely transcendental over $\mathbb{C}$. [Hint: Let $\alpha = \dfrac{t}{1+\sqrt{1-t^2}}$ and compute $\alpha \pm \dfrac{1}{\alpha}$.]

   - Remark: This argument is (in fact) a rephrasing of the geometric fact that the circle $x^2 + y^2 = 1$ has a rational parametrization given by $x = \dfrac{2\alpha}{1+\alpha^2}$, $y = \dfrac{1-\alpha^2}{1+\alpha^2}$.

---

6. Let t be an indeterminate over the field $\mathbb{C}$, and let $K = \mathbb{C}(t, \sqrt{t^3+t})$.

   (a) Prove that $K/\mathbb{C}$ has transcendence degree 1.

   (b) Suppose that $p, q \in \mathbb{C}(x)$ are nonconstant and have the property that $q^2 = p^3 + p$. Show that $p = p_0/w^2$ and $q = q_0/w^3$ for some polynomials $p_0, q_0, w \in \mathbb{C}[x]$ where w is relatively prime to p_0 and q_0. [Hint: Use polynomial divisibility.]

   (c) Suppose that $p, q \in \mathbb{C}(x)$ are nonconstant and have the property that $q^2 = p^3 + p$. Show that $g(x) = \dfrac{q'(x)}{3p(x)^2+1} = \dfrac{p'(x)}{2q(x)}$ is actually a polynomial in $\mathbb{C}[x]$. [Hint: Show that g cannot have any roots in its denominator. Use the expressions from (b) to ensure any quantities you analyze are actually defined.]

   (d) Prove that K is not purely transcendental over $\mathbb{C}$. [Hint: If it were, there would exist $p, q \in \mathbb{C}(x)$ with $q^2 = p^3 + p$. Apply (c) to $p(x), q(x)$ and also to $p(1/x), q(1/x)$.]

   - Remark: The argument given here is (really) also a geometric argument: the point is that on the elliptic curve $E : y^2 = x^3 + x$, the differential $\omega = \dfrac{dx}{2y} = \dfrac{dy}{3x^2+1}$ is holomorphic (i.e., it has no poles). But if E were rational (i.e., if the function field $K/\mathbb{C}$ were purely transcendental) then ω would be a holomorphic differential on $\mathbb{C}$ with no poles, which by the maximum modulus principle would have to be constant; this is not possible.
