E. Dummit's Math 5111 ~ Algebra 1, Fall 2020 ~ Homework 12, due Fri Dec 11th.

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. For each polynomial, determine its Galois group over $\mathbb{Q}$. (You may assume each polynomial is irreducible.)
   (a) $f(y) = y^3 - 4y - 2$.
   (b) $f(y) = y^3 + y^2 - 4y + 1$.
   (c) $f(y) = y^4 + 5y - 5$.
   (d) $f(y) = y^4 - 5y^2 + 3$.
   (e) $f(y) = y^4 + 4y + 6$.
   (f) $f(y) = y^4 + 36y + 63$.
   (g) $f(y) = y^4 - 13y^2 - 2y + 19$.
   (h) $f(y) = y^4 - 4y^2 + 2$.
   (i) $f(y) = y^5 - 3y^4 + 6$. [Hint: Count real roots.]
   (j) $f(y) = y^5 + 3y^4 + 15$. [Hint: Factor it modulo 2.]

---

2. For each irreducible polynomial, determine its most probable Galois group over $\mathbb{Q}$ based on its discriminant and its factorization structure modulo $p$ for the 100 smallest primes not dividing its discriminant:
   (a) $f(t) = t^5 - 5t^3 + 5t - 20$, with $\Delta = 2^4 \cdot 3^4 \cdot 5^5 \cdot 11^2$.

| Factorization Type | 1 | 2,2 | 4 | 5 |
|---|---|---|---|---|
| # Appearances | 3 | 26 | 52 | 19 |

   (b) $f(t) = t^7 - 14t^5 + 56t^3 - 56t - 22$, with $\Delta = 2^6 \cdot 7^{10}$.

| Factorization Type | 1 | 3,3 | 7 |
|---|---|---|---|
| # Appearances | 2 | 68 | 30 |

   (c) $f(t) = t^6 + t^4 + 23$, with $\Delta = -2^6 \cdot 23^3$.

| Factorization Type | 1 | 2,2 | 2,2,2 | 3,3 | 4 |
|---|---|---|---|---|---|
| # Appearances | 3 | 9 | 27 | 36 | 24 |

   (d) $f(t) = t^6 - 6t^3 - 6t^2 - 6t - 2$, with $\Delta = 2^6 \cdot 3^6 \cdot 13^2$.

| Factorization Type | 2,2 | 2,4 | 3 | 3,3 | 5 |
|---|---|---|---|---|---|
| # Appearances | 8 | 24 | 13 | 14 | 41 |

   (e) Assuming your predictions are correct, which of the polynomials $f(t)$ from (a)-(d) are solvable in radicals?

---

3. The goal of this problem is to give a method for computing the discriminant of a polynomial in terms of values of its derivative. So suppose $f(x) = (x - r_1)(x - r_2) \cdots (x - r_n)$ is a monic polynomial.
   (a) Show that $f'(r) = \prod_{r_i \neq r} (r - r_i)$ for any root $r$ of $f$.
   (b) Show that $\Delta(x_1, x_2, \ldots, x_n) = (-1)^{n(n-1)/2} \displaystyle\prod_{i=1}^{n} \prod_{j=1,\, j\neq i}^{n} (x_i - x_j)$.
   (c) Show that $\Delta(f) = (-1)^{n(n-1)/2} \prod_{i=1}^{n} f'(r_i)$.

---

4. The Kronecker-Weber theorem says that every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension. The goal of this problem is to prove this fact for quadratic extensions. Let $p$ be an odd prime.
   (a) Show that the discriminant of the polynomial $q(x) = x^p - 1$ is $(-1)^{(p-1)/2} p^p$. [Hint: Use problem 3(c).]
   (b) Show that $\mathbb{Q}(\zeta_p)$ contains $\sqrt{(-1)^{(p-1)/2} p}$, and in fact that $\mathbb{Q}(\sqrt{(-1)^{(p-1)/2} p})$ is the unique quadratic subfield of $\mathbb{Q}(\zeta_p)$.
   (c) Show that every quadratic extension of $\mathbb{Q}$ is contained in a cyclotomic extension. (Don't forget about $\sqrt{2}$ and $\sqrt{-1}$!)

   - Remark: If we write $p^* = (-1)^{(p-1)/2} p$, this problem shows that $\sqrt{p^*}$ is an element of $\mathbb{Q}(\zeta_p)$. It is natural to seek a simple formula for $\sqrt{p^*}$ in terms of $\zeta_p$; with a fair bit of additional work, one can show that $\sqrt{p^*}$ is given by the classical Gauss sum $\sum_{i=0}^{p-1} \zeta_p^{i^2}$.

---

5. Suppose that $q(x) \in \mathbb{Z}[x]$ is an irreducible polynomial of degree $n$.
   (a) Suppose that the Galois group over $\mathbb{Q}$, considered as a subgroup of $S_n$, contains no $n$-cycles. Prove that $q(x)$ is reducible modulo $p$ for every prime $p$. [Hint: If $p$ divides the discriminant, $q(x)$ has a repeated factor. Otherwise, use the Dedekind-Frobenius theorem.]

(b) Show that the polynomial $x^4 + 1$ is reducible modulo $p$ for every prime $p$, but is irreducible over $\mathbb{Q}$. (Compare problem 1e of homework 1.)

(c) Suppose that $n$ is even and the discriminant of $q(x)$ is a perfect square. Prove that $q$ is reducible modulo $p$ for every prime $p$.

---

6. The goal of this problem is to discuss Berlekamp's factorization algorithm in $\mathbb{F}_p[x]$. So suppose that $f(x) \in \mathbb{F}_p[x]$ has irreducible factorization $f(x) = q_1(x)^{a_1} q_2(x)^{a_2} \cdots q_n(x)^{a_n}$ where the $q_i$ are distinct, monic, and irreducible, and $f$ has degree $D$.

(a) Suppose that $\deg(g) < \deg(f)$ and suppose that the remainder upon dividing $g(x^p)$ by $f(x)$ in $\mathbb{F}_p[x]$ is $g(x)$. Prove that for each $1 \leq i \leq n$, there exists an $r_i \in \mathbb{F}_p$ such that $q_i(x)^{a_i}$ divides $g(x) - r_i$. [Hint: Use the factorization of $x^p - x$ over $\mathbb{F}_p$ to factor $g(x^p) - g(x) = g(x)^p - g(x)$ as a product of $p$ relatively prime terms.]

(b) Suppose that $\deg(g) < \deg(f)$ and that for each $1 \leq i \leq n$, there exists an $r_i \in \mathbb{F}_p$ such that $q_i(x)^{a_i}$ divides $g(x) - r_i$. Prove that the remainder upon dividing $g(x^p)$ by $f(x)$ in $\mathbb{F}_p[x]$ is $g(x)$.

(c) Let $V$ be the vector space of polynomials $g$ such that$\deg(g) < \deg(f)$ and the remainder upon dividing $g(x^p)$ by $f(x)$ in $\mathbb{F}_p[x]$ is $g(x)$. Show that the map $\varphi : V \to \mathbb{F}_p^n$ given by ($g \bmod q_1^{a_1}$, $g \bmod q_2^{a_2}, \ldots, g \bmod q_n^{a_n}$) is a well-defined vector space isomorphism. [Hint: Part (a) shows this map is well-defined. Use the Chinese remainder theorem and part (b) to show it is surjective.]

(d) Deduce that if $q_1(x)^{a_1}$ and $q_2(x)^{a_2}$are two factors of $f$, then there is some $g(x)$ such that $g(x^p) \equiv g(x) \bmod f(x)$ and some $r \in \mathbb{F}_p$ such that $q_1(x)^{a_1}$ divides $g(x) - r$ but $q_2(x)^{a_2}$ does not. [Hint: Some polynomial has $\varphi(g) = (1, 0, 0, \ldots, 0)$ in part (c).]

(e) Suppose that the remainder upon dividing $x^{pj}$ by $f(x)$ is $a_{0,j} + a_{1,j}x + \cdots + a_{D-1,j}x^{D-1}$ for $0 \leq j \leq D-1$. If $g(x) = b_0 + b_1 x + \cdots + b_{D-1}x^{D-1}$, show that the remainder upon dividing $g(x^p)$ by $f(x)$ equals $g(x)$ if and only if $\begin{bmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,D-1} \\ a_{1,0} & a_{1,1} & \cdots & a_{1,D-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{D-1,0} & a_{D-1,1} & \cdots & a_{D-1,D-1} \end{bmatrix} \cdot \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{D-1} \end{bmatrix} = \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{D-1} \end{bmatrix}$. [Hint: If $A$ is the matrix and $B$ is the column vector, $AB$ computes the coefficients after dividing $g(x^p)$ by $f(x)$.]

(f) If $A$ is the matrix described in part (e), show that the dimension of the kernel of $A - I$ is $n$. [Hint: This is a rephrasing of part (c).]

(g) Prove that the following procedure, Berlekamp's factorization algorithm, calculates the full irreducible factorization $q_1(x)^{a_1}, \ldots, q_n(x)^{a_n}$ of $f$. [Hint: Use part (d) to justify why there are always $n$ terms at the end of step (iii) by showing that any two factors $q_i^{a_i}$ and $q_j^{a_j}$ will be split into separate terms, and also justify (iv).]

i. Calculate the matrix $A$ described in part (e) by finding the remainders of $x^{pj}$ upon dividing by $f(x)$.

ii. Compute a basis for the kernel of $A - I$ via row-reduction. If the kernel is $n$-dimensional, then take $g_1 = 1$, $g_2$, ... , $g_n$ to be a basis for the corresponding space of polynomials $g$ of degree less than $D$ such that $g(x^p) \equiv g(x) \bmod f(x)$, obtained by reading coefficients from the vectors in $\ker(A - I)$.

iii. Start with the list $\{f(x)\}$. Then for each $i = 2, 3, \ldots, n$ and each $r \in \mathbb{F}_p$, compute the gcd of each term currently on the list with $g_i(x) - r$. For any nontrivial factorization obtained (i.e., where a gcd is a nontrivial proper divisor of a term on the list), replace the given term with its two factors. Continue until $n$ factors are obtained.

iv. The $n$ factors on the list will be the terms $q_1(x)^{a_1}, \ldots, q_n(x)^{a_n}$. For each factor $Q = q_i(x)^{a_i}$, compute $Q'$. If $Q' = 0$ then $Q$ is a $p$th power; take its $p$th root and return to the beginning of this step. Otherwise, compute $\gcd(Q, Q')$: if this is 1 then $Q$ is irreducible, and otherwise $Q/\gcd(Q, Q')$ will be the polynomial $q_i(x)$. Calculate all of the appropriate exponents to obtain the full factorization $f(x) = q_1(x)^{a_1} q_2(x)^{a_2} \cdots q_n(x)^{a_n}$ of $f$.

(h) Use Berlekamp's algorithm to find the irreducible factorization of $f(x) = x^5 + x^3 + 1$ over $\mathbb{F}_5$.

(i) Use Berlekamp's algorithm to show $x^6 + x^4 + 1$ is irreducible over $\mathbb{F}_7$. [Hint: Compute the matrix rank.]

(j) Use Berlekamp's algorithm to factor $x^7 + x^4 + x^2 + x + 1$ over $\mathbb{F}_2$.

---