MATH 437: Homework IX.
Due in class on Wednesday, April 21

1. **Examples in characteristic p.**
(a) Let k be a field of characteristic p and let $a \in k$ be an element which does not have a pth root in k, i.e., there does not exist $y \in k$ with $y^p = a$. For any $n \geq 1$ show that the polynomial $x^{p^n} - a$ is irreducible in $k[x]$ as follows: First if $\alpha \in \bar{k}$ is a root of this polynomial, discuss the multilpicity of α as a root of $x^{p^n} - a$ and the form of its factorization in $\bar{k}[x]$. Suppose $x^{p^n} - a = f(x)g(x)$ in $k[x]$ where $f(x)$ is a monic irreducible polynomial of $k[x]$, determine the possible forms of the factorization of $f(x)$ in $\bar{k}[x]$. Use this to consider the constant term of $f(x)$ and argue that $x^{p^n} - a = f(x)$ and is hence irreducible in $k[x]$.
(b) Let $F = \mathbb{F}_p(t)$ be the field of fractions of $\mathbb{F}_p[t]$. This is the field of rational functions of the form $\frac{g(t)}{h(t)}$ where $g(t), h(t) \in \mathbb{F}_p[t]$ are polynomials and h is not the zero polynomial. For $l \geq 1$ let $E_l = \mathbb{F}_p(t^{p^l})$ be the subfield consisting of rational functions of the form $\frac{g(t^{p^l})}{h(t^{p^l})}$ where $g, h \in \mathbb{F}_p[t]$ as before.
Prove that $t \in F$ is algebraic over E_l with $Irr(t, E_l)(x) = x^{p^l} - t^{p^l}$. Show that $F = E_l[t]$ and that $|F : E_l| = |F : E_l|_i = p^l$, $|F : E_l|_s = 1$ and conclude that the extension $E_l \subseteq F$ is purely inseparable. Explain why $Gal(F/E_l) = \{Id\}$. (As usual $Gal(F/E_l)$ is the group of field automorphisms of F which are the identity on E_l which is a group under composition.)
(c) Let k be an infinite field of characteristic p. (For example k might be the field of fractions in example (b)). Let $F = k(t_1, t_2)$ be the field of rational functions in two variables over k, thus the elements are of the form $\frac{g(t_1,t_2)}{h(t_1,t_2)}$ where g and h are k-polynomials in two variables, h nonzero. Consider the subfield $E = k(t_1^p, t_2^p)$.
Show that $|F : E| = p^2 = |F : E|_i$.
For any $c \in k$ we let $\alpha_c = t_1 + ct_2 \in F$ and define $F_c = E[\alpha_c]$. Find $Irr(\alpha_c, E)$ and show that $|F_c : E| = p$ for all $c \in k$. **Show** that if $F_c = S = F_{c'}$ for $c \neq c' \in k$ then $t_1, t_2 \in S$ which gives $S = F = F_c$ giving a contradiction. Conclude that the fields $\{F_c | c \in k\}$ are an infinite family of distinct intermediate fields between E and F even though the extension $E \subseteq F$ is finite.

2. **Finite fields.**
Let p be a prime and $l \geq 1$. Let $\mathbb{F}_{p^l}$ denote the finite field of order p^l (we will

view it as a subfield of $\bar{\mathbb{F}}_p$. Since every finite subgroup of a multiplicative group of a field is cyclic, $(\mathbb{F}_{p^l}^\times, \cdot)$ is a cyclic group of order $p^l - 1$ generated by γ say.
(a) Show that $\mathbb{F}_{p^l} = \mathbb{F}_p[\gamma]$.
(b) Explain why there exists an irreducible polynomial in $\mathbb{F}_p[x]$ of degree l for every integer $l \geq 1$. (Hint: Use (a)). In fact also show that if ψ is any irreducible polynomial in $\mathbb{F}_p[x]$ of degree l then ψ divides $x^{p^l} - x$ in $\mathbb{F}_p[x]$.
(c) If ψ is an irreducible polynomial of degree l then explain why $\mathbb{F}_p[x]/(\psi)$ is isomorphic to $\mathbb{F}_{p^l}$ as rings. If $\mathbb{A}$ is the companion matrix to ψ in $Mat_l(\mathbb{F}_p)$ then show that the subring generated by $\mathbb{A}$ in $Mat_l(\mathbb{F}_p)$ is isomorphic to $\mathbb{F}_{p^l}$.
(d) Explain briefly why $x^2 + x + 1$ is irreducible in $\mathbb{F}_p[x]$ if and only if $p \equiv 2 \mod 3$. (Hint: You have done this in previous HW!) Use this to give a matrix model for $\mathbb{F}_4$ and $\mathbb{F}_{25}$, i.e. describe a set of matrices so that these fields are isomorphic to those sets under matrix addition and matrix multiplication.
(e) Given an algebraic field extension $E \subseteq F$ we say that $\gamma \in F$ is a primitive generator if $F = E[\gamma]$. We will see later that any finite separable extension has a primitive generator. Explain from this why any finite separable extension $E \subseteq F$ can be realized by a matrix model, $F \subseteq Mat_n(E)$ and explain how n and the set of matrices used depend on γ.

3. **Discriminant of cubics.** Let f be a separable irreducible polynomial in $k[x]$, then we have seen that $E = Split_k(f) = k[r_1, \ldots, r_m]$ where r_i are the roots of f is a finite Galois extension of k with Galois group $Gal(E/k)$ which we will denote $Gal_k(f)$, as E is the splitting field of f over k. $Gal_k(f)$ has order $|E : k|$ and acts transitively and faithfully on $\{r_1, \ldots, r_m\}$. Thus $Gal_k(f)$ can be regarded as a subgroup of Σ_m. Recall if $\delta = \prod_{j>i}(r_j - r_i)$ is a discriminant (associated to the given ordering of the roots), then $\delta^2 \in k$ and $\delta \in k$ if and only if $Gal_k(f) \subseteq A_m$. The object of the next few parts of this question is to derive an expression for δ^2 from the coefficients of the polynomial in the cubic case. $Char(k) \neq 2, 3$ thruout this problem.
(a) Let $f(x) = x^3 + \alpha x^2 + \beta x + \gamma \in k[x]$ be a monic, irreducible, cubic polynomial. Let $c \in k$ and consider $g(x) = f(x + c)$. Show that g is still a monic, irreducible, cubic polynomial in $k[x]$ and that it has the same splitting field as f over k. Thus $Gal_k(g) = Gal_k(f)$. Show that c may be chosen so that $g(x) = x^3 + ax + b$. This is called the **normal** form of the cubic.
(b) Let $g(x) = x^3 + ax + b$ have roots r_1, r_2, r_3. Show that $r_1 + r_2 + r_3 = 0$, $r_1r_2 + r_2r_3 + r_3r_1 = a$ and $r_1r_2r_3 = -b$. From this show that $r_1^2 + r_2^2 + r_3^2 = -2a$.

Show that

$$(r_1r_2 + r_2r_3 + r_3r_1)^2 = (r_1^2r_2^2 + r_2^2r_3^2 + r_3^2r_1^2) + 2(r_1 + r_2 + r_3)(r_1r_2r_3)$$

and hence conclude that $r_1^2r_2^2 + r_2^2r_3^2 + r_3^2r_1^2 = a^2$.
(c) Recall we have shown in a previous homework that the discriminant δ of a polynomial g satisfies the following equation:
$-\delta^2 = \prod_{r_i} g'(r_i)$ where r_i are the roots of g. Use this and part (b) to compute the discriminant of $g(x) = x^3 + ax + b$ and show that $\delta^2 = -27b^2 - 4a^3$.
(d) If $g(x) = x^3 + b$ is irreducible in $k[x]$ show that

$$Gal_k(g) = \begin{cases} A_3 \text{ if } \sqrt{-3} \in k \\ \Sigma_3 \text{ if } \sqrt{-3} \notin k. \end{cases}$$

In either case, show that g is still irreducible over $k[\sqrt{-3}]$ and $Gal_{k[\sqrt{-3}]}(g) = A_3$.

4. **Special quartic polynomials.**
Let $f(x) = x^4 + ax^2 + b$ be an irreducible polynomial over a field k of characteristic not equal to two or three.
(a) Explain why f is separable (has distinct roots) and conclude that $k[r_1, r_2, r_3, r_4] = E$ is a finite Galois extension of k with Galois group $Gal(E/k)$ which we will denote by $Gal_k(f)$. Recall that $Gal(E/k)$ will act transitively and faithfully on the roots of f and has order equal to $|E : k|$. Explain why the roots in this case are of the form $\{\pm\alpha, \pm\beta\}$ for some $\alpha, \beta \in E$.
(b) If $\sigma \in Gal_k(f) = Gal(E/k)$, explain why there at most 4 possibilities for $\sigma(\alpha)$ and for each of these possibilities, there are at most two possibilities for $\sigma(\beta)$. Conclude that $|Gal_k(f)| \leq 8$ and from this prove that $Gal_k(f)$ is isomorphic to one of the following subgroups of Σ_4:
(i) $\mathbb{Z}/4\mathbb{Z}$ (ii) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or (iii) D_8.
(c) Prove that $(\alpha^2 - \beta^2)^2$ is nonzero and lies in k. (Hint: For the second part, show it is invariant under $Gal_k(f)$.)
(d) Ordering the roots as $r_1 = \alpha, r_2 = -\alpha, r_3 = \beta, r_4 = -\beta$, calculate the discriminant δ directly from its definition $\delta = \prod_{j>i}(r_j - r_i)$. Show that $\delta \in k$ if and only if $\alpha\beta \in k$ if and only if $Gal_k(f) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.