MATH 437: Homework VIII.
Due in class on Wednesday, April 7

1. **Complex conjugation.**
(a) Let $k \subseteq E$ be a field extension. (Which could be transcendental.) Show that there exists an algebraic closure $\bar{k}$ of k within a fixed algebraic closure $\bar{E}$ of E. Show that if $\sigma \in Gal(\bar{E}/E)$ then σ restricts to a map which maps $\bar{k}$ into $\bar{k}$ and defines an element of $Gal(\bar{k}/k)$ by restriction. Thus conclude that there is a restriction homomorphism $Res_k^E : Gal(\bar{E}/E) \to Gal(\bar{k}/k)$ between the two absolute Galois groups. Show that this homomorphism is not onto in general by considering the case when E is algebraically closed.
(b) Show that complex conjugation $\tau : \mathbb{C} \to \mathbb{C}$ given by $\tau(a+bi) = a - bi$ for $a, b \in \mathbb{R}$ defines a **nontrivial** element (of order two) in $Gal(\bar{k}/k)$ for any subfield k of $\mathbb{R}$. Check that if $z \in \mathbb{C}$ has $|z| = 1$ then $\tau(z) = \frac{1}{z}$.
(c) A polynomial $p(x)$ is called **reciprocal** if whenever ξ is a root of p, so is $\frac{1}{\xi}$ a root of p.
Let k be a subfield of $\mathbb{R}$ and let $f \in k[x]$ be irreducible of degree ≥ 2 with a root $\xi \in \bar{k} \subseteq \mathbb{C}$ with $|\xi| = 1$. Show that f is a reciprocal polynomial and that the degree of f is even. (Hint: $Gal(\bar{k}/k)$ acts transitively on the roots of f).

2. $Gal(\mathbb{R}/\mathbb{Q})$
We define $Gal(\mathbb{R}/\mathbb{Q}) = \{f : \mathbb{R} \to \mathbb{R} | f \text{ a field aut with } f|_{\mathbb{Q}} = Id\}$ as usual. This is a group under composition but it is not the absolute Galois group of $\mathbb{Q}$ as $\mathbb{R}$ is not the algebraic closure of $\mathbb{Q}$. We will study this group in this exercise.
(a) Let $P = \{x \in \mathbb{R} | x > 0\}$. Show that if $f \in Gal(\mathbb{R}/\mathbb{Q})$ then $f(P) \subseteq P$. Use this to show that f is a strictly increasing function i.e., $x < y$ then $f(x) < f(y)$. (Hint: Characterize the elements of P algebraically.)
(b) Show that any $f \in Gal(\mathbb{R}/\mathbb{Q})$ defines a continuous function $f : \mathbb{R} \to \mathbb{R}$ and use this to show that $Gal(\mathbb{R}/\mathbb{Q}) = \{Id\}$. Conclude that the only field automorphism of $\mathbb{R}$ is the identity map.

3. **Difference Equations.** Let E be a field and consider $E^\infty = \prod_{n=0}^{\infty} E$, the set of sequences in E. E^∞ is a E-vector space under componentwise addition and scalar multiplication. We may define a shift map $S : E^\infty \to E^\infty$ given by $S(a_0, a_1, a_2, \dots) = (a_1, a_2, \dots)$ which is easily shown to be an E-homomorphism.
(a) For any $r \in E$ show that the r-eigenspace of S consists exactly of the

geometric sequences with common ratio r. Use this to show that nonzero geometric sequences with different common ratios are E-independent in E^∞.
(b) Let $k \subseteq E$ be a field extension. An mth order linear difference equation (also called a recurrence relation) defined over k is an equation of the form: $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_m a_{n-m}$ for $n \geq m$ and fixed $c_1, \ldots, c_m \in k$.
The set of solutions over E to this difference equation is the subset S of E^∞ which consist of sequences $(a_0, a_1, \ldots)$ which satisfy the recurrence relation. Show that S is a subspace of E^∞. Show that the projection map $\pi : E^\infty \to E^m$ given by $\pi(a_0, a_1, \ldots, a_{m-1}, a_m, \ldots) = (a_0, a_1, \ldots, a_{m-1})$ induces a k-isomorphism between S and E^m and conclude $dim_k(S) = m$.
(c) Show that the geometric sequence $a_n = r^n$, $r \neq 0$ fixed, is a solution of the difference equation in (b) if and only if r is a root of the characteristic polynomial of the equation given by $p_{char}(x) = x^m - c_1 x^{m-1} - c_2 x^{m-2} - \cdots - c_m$. Use this to describe an E-basis for the solution subspace S of E^∞ in the case that $p_{char}(x)$ has distinct roots all of which are contained in E.
(d) In the case when $p_{char}(x)$ has distinct roots $\{r_1, \ldots, r_m\}$ all of which are contained in E, we have seen that a solution to the recurrence relation must be of the form:
$a_n = b_1 r_1^n + b_2 r_2^n + \cdots + b_m r_m^n$ for some fixed $b_1, \ldots, b_m \in E$ and all $n \geq 0$.
Show that the constants $b_1, \ldots, b_m$ must satisfy the following linear system:

$$\begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{m-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 & \ldots & 1 \\ r_1 & r_2 & \ldots & r_m \\ r_1^2 & r_2^2 & \ldots & r_m^2 \\ \vdots & \vdots & \ldots & \vdots \\ r_1^{m-1} & r_2^{m-1} & \ldots & r_m^{m-1} \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}$$

The square matrix above is denoted $V(r_1, \ldots, r_m)$ and is called a **Van der Monde** matrix.
(e) Show that $det(V(r_1, \ldots, r_m)) = \prod_{i>j}(r_i - r_j)$ for $m \geq 2$. (Hint: Consider row operations of multiplying a row by $-r_1$ and adding it to the row below it, starting from the bottom.)
The number $\Delta(r_1, \ldots, r_m) = det(V(r_1, \ldots, r_m))$ is called the **discriminant** of $r_1, \ldots, r_m$. Thus under the conditions in (d), the system in (d) can be inverted and we may solve uniquely for the b_i given the initial conditions $a_0, \ldots, a_{m-1}$.

4. **Transitive action on roots.** Let k be a field of characteristic zero.

Recall in class we showed all irreducible polynomials $p(x)$ over k have distinct roots and that $Gal(\bar{k}/k)$ acts transitively on $X_p^{\bar{k}} = \{z \in \bar{k} | p(z) = 0\}$. Note $|X_p^{\bar{k}}| = deg(p)$. Thus the action homomorphism of the action of the absolute Galois group on the roots of p gives us a homomorphism $\rho_p : Gal(\bar{k}/k) \to \Sigma_n$ where $n = deg(p)$. The image of ρ_p is a transitive subgroup of Σ_n, i.e., a subgroup H which acts transitively on $\{1, 2, \ldots, n\}$ under the natural action induced from Σ_n.

Finally, recall since all elements in $\bar{k}$ are separable over k, the fixed field of $Gal(\bar{k}/k)$ is just k itself.

(a) If H is a transitive subgroup of Σ_n, show that n divides $|H|$. Use this to show that if $deg(p) = 2$ then $Im(\rho_p) \cong \Sigma_2 \cong \mathbb{Z}/2\mathbb{Z}$. and that if $deg(p) = 3$ then $Im(\rho_p) = \Sigma_3$ or A_3.

(b) Find all the transitive subgroups H of Σ_4 as follows: First argue that $|H| = 4, 8, 12$ or 24. Explain why A_4 and Σ_4 are the unique subgroups of order 12 and 24 respectively. Explain why all subgroups of order 8 are conjugate and show that they are isomorphic to D_8, the dihedral group of order 8. Finally show that if H has order 4 and is cyclic, then H is conjugate to $< (1, 2, 3, 4) >$ but if it is not cyclic, it must equal the Klein 4-group and is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(c) Let $\{r_1, \ldots, r_n\} = X_p^{\bar{k}}$ and consider the discriminant $\Delta = \Delta(r_1, \ldots, r_n) \in \bar{k}$. If $\sigma \in Gal(\bar{k}/k)$ show that $\sigma(\Delta) = \pm\Delta$ where the sign is $+1$ if $\rho_p(\sigma)$ is an even permutation and -1 if $\rho_p(\sigma)$ is an odd permutation.

(d) Prove that Δ^2 is always in k while $\Delta \in k$ if and only if $Im(\rho_p) \subseteq A_n$.

(e) If $p(x)$ is a monic irreducible with roots $\{r_1, \ldots, r_m\}$ (distinct as we are in char zero). For any fixed i we may write $p(x) = (x - r_i)g_i(x)$ where $g_i(x) = \prod_{j \neq i}(x - r_j)$. Show that $p'(r_i) = \prod_{j \neq i, i \text{ fixed}}(r_i - r_j)$ and that $\prod_{i=1}^m p'(r_i) = (-1)^{\frac{m(m-1)}{2}}\Delta^2$. Thus it is $-\Delta^2$ when $m \equiv 2, 3 \bmod 4$ and it equals Δ when $m \equiv 0, 1 \bmod 4$.