Problem Set 11 – Due Thursday, April 13
Last problem set!

1. Let p be an odd prime. Let $f(x)$ be ann irreducible polynomial with rational coefficients whose splitting field has Galois group (over $\mathbb{Q}$) the dihedral group of order $2p$. Show that f has either all real roots or precisely one real root.

2. Let $f(x)$ be a degree 6 polynomial with rational coefficients, whose splitting field over $\mathbb{Q}$ has Galois group S_6 and let β be a root of f. Let $\alpha_1, \alpha_2, \dots, \alpha_r$ be algebraic numbers all of which are of degree ≤ 5. Show that $\beta \notin \mathbb{Q}(\alpha_1, \dots, \alpha_r)$.

3. Let L/k be an extension of fields, which we do *not* assume to be finite. Let $\theta_1, \theta_2, \dots, \theta_n$ be elements of L. If there is no polynomial relation $f(\theta_1, \theta_2, \dots, \theta_n) = 0$, with $f \in k[x_1, \dots, x_n]$, we say that the θ_i are ***algebraically independent***. If every element of L is algebraic over $k(\theta_1, \dots, \theta_n)$, we say that the θ_i are an ***algebraic spanning set***. If both conditions hold, we say that the θ_i are a ***transendence basis for*** L ***over*** k.
   (a) Fix $\theta_1, \theta_2, \dots, \theta_r$ in L. Define the subset I of $\{1, 2, \dots, n\}$ to be the set of those i such that θ_i is *not* algebraic over $k(\theta_1, \theta_2, \dots, \theta_{i-1})$. Show that $\{\theta_i\}_{i \in I}$ is a transcendence basis for $k(\theta_1, \dots, \theta_r)$.
   (b) Fix $\theta_1, \theta_2, \dots, \theta_r$ in L. Define $I \subseteq \{1, 2, \dots, r\}$ as in part (a). Let σ be a permutation of $\{1, 2, \dots, r\}$ and define $J \subseteq \{1, 2, \dots, r\}$ to be the set of j so that $\theta_{\sigma(j)}$ is *not* algebraic over $k(\theta_{\sigma(1)}, \theta_{\sigma(2)}, \dots, \theta_{\sigma(j-1)})$. Show that $\#I = \#J$.
   (c) Let $\alpha_1, \alpha_2, \dots, \alpha_p$ be an algebraic spanning set for L over k and let $\beta_1, \beta_2, \dots, \beta_q$ be algebraically independent. Show that $p \geq q$. (Hint: Part (b) is useful.) Show any two transcendence basis for L over k have the same size.

4. Let ζ be a primitive n-th root of unity. The aim of this problem is to show that $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is all of $(\mathbb{Z}/n\mathbb{Z})^*$. We have already shown that it is a subgroup of $(\mathbb{Z}/n)^*$.

   Define $\Phi(x) = \prod_{a \in \mathbb{Z}/n^*} (x - \zeta^a)$. Let $f(x)$ be the minimal polynomial of ζ (we take minimal polynomials to be monic).

   Let p be a prime not dividing n. Assume for the sake of contradiction that $f(\zeta^p) \neq 0$. Let g be the minimal polynomial of ζ^p.
   (a) Show that $f(x)$ and $g(x)$ have integer coefficients. Show that there are polynomials $s(x)$ and $t(x)$ with **integer** coefficients such that $f(x)g(x)s(x) = x^n - 1$ and $g(x^p) = f(x)t(x)$. Because f, g, s and $t \in \mathbb{Z}[x]$, we may reduce the equations in part (a) modulo p.
   (b) Show $f(x)$ and $g(x)$ have a nonconstant common factor in $\mathbb{F}_p[x]$. Show that $x^n - 1$ is divisible by a nonconstant square in $\mathbb{F}_p[x]$.
   (c) Show that $x^n - 1$ is **NOT** divisible by the square of any nonconstant polynomial in $\mathbb{F}_p[x]$. Parts (b) and (c) contradict each other. So, for all prime p not dividing n, $f(\zeta^p) = 0$.
   (d) Show that Φ is irreducible. Deduce that $\mathrm{Gal}(\mathbb{Q}(\zeta), \mathbb{Q})$ is $(\mathbb{Z}/n\mathbb{Z})^*$.