MATH 437: Homework X.
Due in class on Wednesday, April 28

1. **Cyclotomic extensions** Let k be a field of characteristic zero.
(a) If $\zeta_1, \ldots, \zeta_r$ are a collection of roots of unity of orders $l_1, \ldots, l_r$ show that $k[\zeta_1, \ldots, \zeta_r] \subseteq k[\zeta]$ where ζ is a primitive Lth root of unity where $L = lcm(l_1, \ldots, l_r)$.
(b) Let $f \in k[x]$. Show that if the roots of f are k-polynomial combinations of roots of unity then $Gal_k(f) = Gal(Split_k(f)/k)$ is an Abelian group. (Hint: Show that $k \subseteq Split_k(f) \subseteq k[\zeta]$ for suitable ζ first.)
(Note: Kronecker showed the converse over $\mathbb{Q}$, i.e., if $Gal_{\mathbb{Q}}(f)$ is Abelian then the roots of f are $\mathbb{Q}$-polynomial combinations of roots of unity.)
(c) Show that $\sqrt[4]{2}$ is not a $\mathbb{Q}$-polynomial combination of roots of unity by considering $Gal_{\mathbb{Q}}(x^4 - 2)$.
(d) Recall we have shown in class that if ζ is a primitive nth root of unity then $Gal(\mathbb{Q}[\zeta]/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*$. If $n = p_1^{k_1} \ldots p_r^{k_r}$ then the Chinese Remainder theorem shows that $(\mathbb{Z}/n\mathbb{Z})^* \equiv (\mathbb{Z}/p_1^{k_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_r^{k_r}\mathbb{Z})^*$. It also can be calculated (see Lang/Hungerford) that:

$$(\mathbb{Z}/p^r\mathbb{Z})^* \equiv \begin{cases} \text{Cyclic of order } (p-1)p^{r-1} \text{ if } p \text{ odd} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{r-2}\mathbb{Z} \text{ if } p = 2 \text{ and } r \geq 3. \end{cases}$$

Use these facts to calculate the structure of $(\mathbb{Z}/15\mathbb{Z})^*$ explicitly.
(e) Dirichlet's theorem on arithmetic progressions states that if a, b are relatively prime positive integers then the arithmetic progression $\{a+mb | m \in \mathbb{N}\}$ contains infinitely many primes. Use this to show that if N is a positive integer then $N | p-1$ for infinitely many odd primes p. Use this to show that if A is a finite Abelian group, there is an integer M such that A is a quotient group of $(\mathbb{Z}/M\mathbb{Z})^*$. Use this to find a field extension $\mathbb{Q} \subseteq F \subseteq \mathbb{Q}[\zeta_M]$ such that $\mathbb{Q} \subseteq F$ Galois with $Gal(F/\mathbb{Q}) = A$. Thus every finite Abelian group may occur as the Galois group of some extension over $\mathbb{Q}$. (Note: It is still unknown if every finite group occurs as the Galois group over $\mathbb{Q}$. This is called the "Inverse Galois problem". The best so far is every finite solvable group is $Gal(F/\mathbb{Q})$ for some Galois extension F of $\mathbb{Q}$ which was proven by Shaferevich.)

2. **Splitting field of $x^n - \alpha$.**
Let k be a field, n a positive integer and $\alpha \in k$.
(a) If $char(k)$ does not divide n (this includes the case of char zero) then

show that $x^n - \alpha$ has distinct roots and that a primitive nth root of unity ζ exists in $\bar{k}$. If $\beta \in \bar{k}$ is a root of $x^n - \alpha$ show that $Split_k(x^n - \alpha)$ is equal to $k[\beta, \zeta]$ and is a finite Galois extension over k. Describe the factorization of $x^n - \alpha$ in $\bar{k}[x]$ explicitly.
(b) Explain why $k \subseteq k[\zeta]$ is a Galois extension with $Gal(k[\zeta]/k) \subseteq (\mathbb{Z}/n\mathbb{Z})^*$. Conclude $Gal(k[\zeta]/k)$ is an Abelian group. (Hint: Consider the map $\epsilon : Gal(k[\zeta]/k) \to (\mathbb{Z}/n\mathbb{Z})^*$ defined by $\sigma(\zeta) = \zeta^{\epsilon(\sigma)}$ for $\sigma \in Gal(k[\zeta]/k)$.)
(c) Explain why $k[\zeta] \subseteq k[\zeta, \beta]$ is a Galois extension and consider the map $\mu : Gal(k[\zeta, \beta], k[\zeta]) \to (\mathbb{Z}/n\mathbb{Z}, +)$ given by the identity $\sigma(\beta) = \beta\zeta^{\mu(\sigma)}$ for $\sigma \in Gal(k[\zeta, \beta], k[\zeta])$. Explain why this identity holds and show that the map μ is well-defined and is an **injective homomorphism**. Use this to show that $Gal(k[\zeta, \beta], k[\zeta])$ is cyclic of order $Irr(\beta, k[\zeta])$.
(d) Show that there exists a short exact sequence of groups:

$$0 \to C \to Gal(k[\zeta, \beta], k) \to A \to 0$$

where C is cyclic and A is Abelian. Conclude that
$Gal_k(x^n - \alpha) = Gal(k[\zeta, \beta]/k)$ is solvable.
(e) Compute $Gal_{\mathbb{Q}}(x^{15} - 2)$. You should find its order and exhibit a short exact sequence as in (d) where C and A are explicitly determined.
(f) Let $E = Split_{\mathbb{Q}}(x^{15} - 2)$ and let $\zeta = e^{\frac{2\pi i}{15}}$. Explain why there exists $\sigma \in Gal(E/\mathbb{Q}[\zeta]) \subseteq Gal(E/\mathbb{Q})$ with $\sigma(\sqrt[15]{2}) = \sqrt[15]{2}\zeta$. Explain why there exists $\tau_a \in Gal(E/\mathbb{Q}[\sqrt[15]{2}]) \subseteq Gal(E/\mathbb{Q})$ with $\tau_a(\zeta) = \zeta^a$ if a is relatively prime to 15. Compute $\tau_a \circ \sigma$ and $\sigma \circ \tau_a$ on the elements ζ and β. Is $Gal_{\mathbb{Q}}(x^{15} - 2)$ Abelian?
(g) Given a polynomial f in $k[x]$ we say that f is solvable by radicals over k if $Split_k(f) = k[\sqrt[n_1]{\alpha_1}, \ldots, \sqrt[n_r]{\alpha_n}]$ for some $\alpha_i \in k$. Note when this happens the roots $\{r_1, \ldots, r_m\}$ of f are k-polynomial combinations of certain nth roots of elements of k. Show that if $char(k) = 0$ and $f \in k[x]$ is solvable by radicals over k then $Gal(Split_k(f)/k)$ is a solvable group. (The converse is also true, as proven by Galois - we will see this in class time permitting.)
(h) Explain why if g is an irreducible polynomial over k of degree $n \geq 5$ with $Gal(Split_k(g)/k)$ equal to A_n or Σ_n then g is not solvable by radicals over k.

3. **Irreducible polynomials with Galois group Σ_p.** Let f be an irreducible polynomial of $\mathbb{Q}$ of prime degree. Suppose f has exactly two nonreal roots.
Let $E = Split_{\mathbb{Q}}(f)$ and $Gal(E/\mathbb{Q}) = G$ the corresponding Galois group. Recall that G acts transitively and faithfully on the roots $\{r_1, \ldots, r_p\}$ of f.

(a) Show that $G \subseteq \Sigma_p$ has an element μ of order p and a transposition τ. Explain why by suitable labeling of the roots, we may assume $\mu = (1, 2, \ldots, p)$ and $\tau = (1, k)$ in cycle notation of Σ_p.
(b) Recall that we had shown in a HW exercise in the first semester that $(1, 2), (2, 3), \ldots, (p-1, p)$ generate Σ_p as a group. Use this to show that τ and μ generate Σ_p and conclude that $Gal(E/\mathbb{Q}) = Gal_{\mathbb{Q}}(f) \cong \Sigma_p$. Thus for $p \geq 5$, conclude that f is not solvable by radicals.

4. **Cyclotomic polynomials.** Let ϕ_n denote the nth cyclotomic polynomial. This is the polynomial which has roots the primitive nth roots of unity in $\bar{\mathbb{Q}}$.
(a) Explain why $x^n - 1 = \prod_{d|n} \phi_d$ in $\mathbb{Z}[x]$.
(b) Check that $\phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ and $\phi_{p^k}(x) = \phi_p(x^{p^{k-1}})$ for $k \geq 1$ and primes p. Show that $\phi_{p^k}(1) = p$ for all primes p and $k \geq 1$. Check that $\phi_1(1) = 0$.
(c) Show by induction that

$$\phi_n(1) = \begin{cases} p \text{ if } n = p^k, p \text{ prime }, k \geq 1 \\ 0 \text{ if } n = 1 \\ 1 \text{ otherwise} \end{cases}$$

(Hint: For composite n, note $\phi_n(x) = \frac{x^n - 1}{(x-1)\prod_{k|n, 1<k<n} \phi_k(x)}$. Consider the prime factorization of n.)
(d) Find $\frac{(x^{30}-1)(x-1)}{(x^6-1)(x^5-1)}$ explicitly as a product of cyclotomic polynomials. If p, q are distinct primes show that $\phi_{pq}(x) = \frac{(x^{pq}-1)(x-1)}{(x^p-1)(x^q-1)}$ and use this to show $\phi_{pq}(x) = \frac{\phi_p(x^q)}{\phi_p(x)}$. Use this to find $\phi_{10}(x)$ as an integer polynomial.
(e) Since the $\phi_n(x)$ are integer polynomials, we may consider their reductions modulo p. Show that every nonzero $\alpha \in \bar{\mathbb{F}}_p$ is a root of $\phi_d(x)$ for some $d \geq 1$, d relatively prime to p. Conclude that every element of $\bar{\mathbb{F}}_p$ is a root of unity or zero.
(f) If q, p are primes. Show that $\phi_q(x)$ has a root in $\mathbb{F}_p$ if and only if $p \equiv 1$ or $0 \bmod q$. Thus ϕ_q is not irreducible in $\mathbb{F}_p[x]$ in general.
(g) Show that $\phi_5(x)$ factors into two quadratic irreducibles in $\mathbb{F}_{19}[x]$. To do this, first show that ϕ_5 splits into linear factors over $\mathbb{F}_{19^2}$ and then consider the action of $Gal(\mathbb{F}_{19^2}/\mathbb{F}_{19})$.