Week 4, Due Mon 4/23

1. (**Primitive Element Theorem, I**) Suppose that L/K is a finite extension, and suppose additionally that there only exists **finitely many** intermediate fields E with $K \subset E \subset L$. Assume that K is infinite. Say that an element $\theta \in L$ is *primitive* if $L = K(\theta)$. We prove (under the assumptions of the problem) that a primitive element exists.

   (a) Let $K_0 = K$. If $K_0 = L$, show (this is obvious) that L has a primitive element. If $K_0 \neq L$, show that there exists an element $\theta_1 \in L \setminus K_0$. Let $K_1 = K_0(\theta_1)$. If $K_1 = L$, show (this is obvious) that L has a primitive element. Assume that $K \subsetneq K_1 \subsetneq \ldots \subsetneq K_n \subset L$, and assume that $K_n = K(\theta_n)$. If $K_n = L$, show (this is obvious) that L has a primitive element.

   (b) If $K_n \neq L$, show there exists an element $\alpha \in L \setminus K_n$. For $\lambda \in K$, let $K_\lambda := K(\theta_n + \lambda\alpha)$. Prove that there exist $\lambda_1 \neq \lambda_2$ such that $K_{\lambda_1} = K_{\lambda_2}$.

   (c) If there is an equality of fields
   $$K(\theta_n + \lambda_1\alpha) = K(\theta_n + \lambda_2\alpha),$$
   prove that both fields are isomorphic to $K(\theta_n, \alpha)$.

   (d) Deduce that there exists $\lambda \in K$ and $\theta_{n+1} = \theta_n + \lambda\alpha$ so that $K_{n+1} := K_n(\theta_{n+1})$ strictly contains K_n.

   (e) Deduce (under the conditions of the problem) that L/K has a primitive element.

   (f) Find a primitive element for the following extensions:

      i. The splitting field of $X^3 - 2$ over $\mathbf{Q}$.

      ii. The splitting field of $X^3 - 2$ over $\mathbf{F}_7$.

      iii. The splitting field of $(X^2 - 2)(X^2 - 3)$ over $\mathbf{Q}$.

2. (**Primitive Element Theorem, II**) Let L/K be a finite extension.

   (a) Assume that L/K is separable — that is, any element $\alpha \in L$ is the root of a separable irreducible polynomial in L. Prove that there exists a normal extension (splitting field of a separable polynomial) M/K containing L.

   (b) Deduce that if L/K is separable, then L/K has only finitely many intermediate subfields.

   (c) Deduce that if L/K is separable, then L/K contains a primitive element.

   (d) Deduce that if $\mathrm{Char}(K) = 0$ or K is finite, then L/K contains a primitive element.

3. Suppose that $K = \mathbf{F}_p(X, Y)$, the field of rational functions in two variables X and Y.

   (a) Let $L = \mathbf{F}_p(X^{1/p}, Y^{1/p})$. Show that L is the splitting field of $(T^p - X)(T^p - Y)$.

   (b) Prove that $[L : K] = p^2$.

   (c) Prove that, if $\eta \in L$ is any element, then $\eta^p \in K$.

   (d) Prove that, if $\eta \in L$ is any element, then $[K(\eta) : K] = 1$ or p.

   (e) Prove that there are infinitely many subfields $K \subset E \subset L$.

4. Let $a(x)$ and $b(x)$ be irreducible polynomials of degree n over $\mathbf{Q}$, and let $A = \mathbf{Q}[x]/a(x)$, $B = \mathbf{Q}[x]/b(x)$. Suppose that K is the splitting field of both $a(x)$ and $b(x)$. Let $G = \mathrm{Gal}(K/\mathbf{Q})$, $H_A = \mathrm{Gal}(K/A)$, and $H_B = \mathrm{Gal}(K/B)$.

   (a) Prove that $\bigcap \sigma H \sigma^{-1} = 1$. for $H = H_A$ and H_B.

(b) Prove that $|H_A| = |H_B|$.

(c) Prove that $A \simeq B$ if and only if H_A is conjugate to H_B in G.

(d) Prove that if $n = 2$ or $n = 3$, then $A \simeq B$.

(e) Prove that if $n = 4$, and $G = D_8$, then A is not necessarily isomorphic to B.

(f) Give an explicit example of polynomials $a(x)$ and $b(x)$ of degree 4 such that A is not isomorphic to B.

(g) Prove that if G is abelian, then $A = B = K$.

(h) Prove that if $G = S_n$, then A is isomorphic to B provided that $n \neq 6$.

5. Let $K/\mathbf{Q}$ be a Galois extension.

   (a) If $[K : \mathbf{Q}] = 2009$, prove that $\mathrm{Gal}(K/\mathbf{Q})$ is abelian.

   (b) If $[K : \mathbf{Q}] = 2010$, prove that K contains an extension E with $[E : \mathbf{Q}] = 2$.

   (c) If $[K : \mathbf{Q}] = 2011$, prove that $\mathrm{Gal}(K/\mathbf{Q})$ is abelian.

   (d) If $[K : \mathbf{Q}] = 2012$, prove that K contains an extension E with $[E : \mathbf{Q}] = 503$.

   (e) If $[K : \mathbf{Q}] = 2013$, prove that K contains an extension E with $[E : \mathbf{Q}] = 3$.

6. Determine $\mathrm{Aut}(K/\mathbf{Q})$ for the following fields, and determine which ones are Galois.

   (a) $\mathbf{Q}(\sqrt[3]{2})$.

   (b) $\mathbf{Q}(2\cos(2\pi/7))$.

   (c) $\mathbf{Q}(\sqrt{1+\sqrt{2}})$.

   (d) $\mathbf{Q}(\sqrt[3]{1+\sqrt{2}})$.

7. Prove that the Galois group of the splitting field of $x^4 + ax^2 + b$ is a subgroup of $D_8 \subset S_4$.

8. Let $f(x)$ be an irreducible separable polynomial over K with splitting field L. Suppose that $\mathrm{Gal}(L/K) = Q$, the quaternion group of order 8. Determine the possible degrees of $f(x)$.

9. Let L/K be an extension, and let $\alpha, \beta \in L$ be elements with $[K(\alpha) : K] = 2$ and $[K(\beta) : K] = 3$. Determine the possible degrees $[K(\alpha + \beta) : K]$.