189-371B: Algebra 4

Assignment 3

Due: Friday, February 24

1. For each of the following extensions K/F, describe its automorphism group (over $\mathbf{Q}$) and determine whether it is Galois. If it is Galois, determine its Galois group.

a) $F = \mathbf{Q}$, $K = \mathbf{Q}(3^{1/3})$;

b) $F = \mathbf{Q}(\omega)$, $K = F(3^{1/3})$, where $\omega := \frac{-1+\sqrt{-3}}{2}$.

c) $F = \mathbf{Q}$, $K = \mathbf{Q}[x]/(x^4+1)$;

d) $F = \mathbf{Q}$, $K = \mathbf{Q}(\sqrt{2}, \sqrt{2+\sqrt{2}})$.

e) $F = \mathbf{Z}/p\mathbf{Z}(t)$, $K = F(t^{1/p}) = F[x]/(x^p - t)$, where t is a transcendental element.

f) $F = \mathbf{Z}/p\mathbf{Z}(t)$, $K = F[x]/(x^p - x - t)$.

2. The fundamental *Galois correspondence* asserts that, if K/F is a Galois extension, then the assignment which to any subgroup $H \subset G = \mathrm{Gal}(K/F)$ associates the fixed field K^H determines a bijection between the subgroups of G and the subfields of K containing F. For each of the extensions K/F described in question 1 which are Galois, enumerate all of the subfields of K containing F. (We will be proving the Galois correspondence in class. The purpose of this problem is to get you to appreciate its power and develop some proficiency in applying it in concrete settings.)

3. Let $\mathbf{F}_p$ be the finite field with p elements, let $F = \mathbf{F}_p(t)$ be the field of rational functions in an indeterminate t, let $f(x) = x^{p^2} - tx^p - x \in F[x]$, and let K denote the splitting field of $f(x)$ over F. Show that $f(x)$ is seperable, so that K/F is Galois. Show that $[K : F]$ divides $p(p+1)(p-1)^2$. (Hint: show that the Galois group of K over F is a subgroup of the group of 2×2 invertible matrices with entries in $\mathbf{F}_p$.)

4. Let $\zeta = e^{2\pi i/7}$ be a primitive 7th root of unity and let $\mathbf{Q}(\zeta)$ be the cyclotomic field generated by this root of unity. List the subfields of $\mathbf{Q}(\zeta)$, and for each subfield give an irreducible polynomial whose roots generate it.

5. Let $f(x) \in F[x]$ be an irreducible polynomial of degree n whose Galois group is the permutation group S_n on n letters. Show that $f(x)$ factors over the field $K := F[y]/(f(y))$ as $(x-y)g(x)$, where $g(x)$ is an irreducible polynomial of degree $n-1$ in $K[x]$.

6. Let $F \subset K$ be fields and let $\alpha \in K$ be an element which is algebraic over F and satisfies an irreducible polynomial of odd degree over F. Show that $F(\alpha^2) = F(\alpha)$.

7. Show that a field K of degree n over a field F is isomorphic to a subring of the ring $M_n(F)$ of $n \times n$ matrices with entries in F.

8. Let G be the group of affine linear transformations of the form $x \mapsto ax+b$ with $a \in \mathbf{F}_p^\times$ and $b \in \mathbf{F}_p$, acting on the set $X := \mathbf{F}_p$ of cardinality p. Let $f(x) \in F[x]$ be a polynomial with Galois group G, i.e., assume that there are identifications of G with the Galois group of the splitting field K of f, and of X with the set R of roots of f in K, compatible with the actions of G on X and of $\mathrm{Gal}(K/F)$ on R respectively. Show that any subfield of K which contains two distinct roots of f is equal to K.

9. Let p be a prime and let F be a field containing all the p-th roots of unity. If K is a *Galois* extension of F of degree p, show that there exists $a \in F$ for which $K = F(a^{1/p})$. (Hint: view a generator σ of $\mathrm{Gal}(K/F)$ as an F-linear transformation of K viewed as an F vector space, and diagonalise it.)

10. Let $F = \mathbf{F}_p(u,v)$ be the field of rational functions with coefficients in $\mathbf{F}_p$ in two indeterminates u and v, and let $K = F(u^{1/p}, v^{1/p})$.

a) Show that K is an algebraic extension of F of degree p^2.

b) Show that $\mathrm{Aut}(K/F) = \{1\}$, and hence that K is not Galois over F.

c) Show that K contains *infinitely many* distinct subfields of degree p over F.

Remark: This exercise illustrates how the Galois correspondence can go dramatically wrong in the setting of inseperable extensions of fields of characteristic p.