ALGEBRA 612, SPRING 2010. HOMEWORK 3

1. Let $p_1, \ldots, p_r \in \mathbb{Z}$ be distinct primes and let $K = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_r})$. (a) Compute the Galois group $\mathrm{Gal}(K/\mathbb{Q})$. (b) Describe explicitly all intermediate subfields L such that either $[L : \mathbb{Q}] = 2$ or $[K : L] = 2$. (c) Describe explicitly all intermediate subfields when $r = 4$.
2. Let p be an odd prime and let a be an integer coprime to p. Show that the quadratic symbol $(\frac{a}{p})$ is equal to $a^{\frac{p-1}{2}}$ modulo p.
3. Consider a tower $K \subset L \subset F$. Suppose L/K and F/L are finite Galois extensions. Is it true that F/K is Galois?
4. Let $\alpha_r = \sqrt{2 + \sqrt{2 + \sqrt{2 + \ldots + \sqrt{2}}}}$ (r radicals). (a) Show that the minimal polynomial $f_r(x) \in \mathbb{Q}[x]$ of α_r can be computed inductively as follows: $f_r(x) = f_{r-1}(x^2 - 2)$, where $f_1(x) = x^2 - 2$. Describe all roots of $f_r(x)$. (b) Show that $\mathbb{Q}(\alpha_2)/\mathbb{Q}$ is a Galois extension with a Galois group $\mathbb{Z}_4$.
5. Let $K \subset L \subset \bar{K}$ and suppose that L/K is separable. Show that there exists the unique minimal (by inclusion) Galois extension F/K such that $L \subset F \subset \bar{K}$. Show that if L/K is finite then F/K is finite.
6. (a) Let $\bar{K}$ be an algebraic closure of K. Show that there exists the unique maximal (by inclusion) subfield $K \subset K^{ab} \subset \bar{K}$ such that K^{ab}/K is Galois and the Galois group $\mathrm{Gal}(K^{ab}/K)$ is Abelian. (b) Deduce from the Kronecker-Weber Theorem that

$$\mathbb{Q}^{ab} = \bigcup_{n \geq 1} \mathbb{Q}(\zeta_n).$$

7. Let F/K be a finite Galois extension with a Galois group G. Let $H \subset G$ be a subgroup and let $L = F^H$. Show that the number of fields of the form $g(L)$ for $g \in G$ is equal to $\frac{|G|}{|N_G(H)|}$.
8. Let F/K be a finite Galois extension with a Galois group G. Let $H \subset G$ be a subgroup and let $L = F^H$. Let $N = \bigcap\limits_{g \in G} gHg^{-1}$. Prove that N is normal in G and characterize the field F^N in terms of the tower $K \subset L \subset F$.
9. Let F/K be a splitting field of a polynomial $f(x) = (x - a_i) \ldots (x - a_r) \in K[x]$ without multiple roots. Let

$$\Delta = \prod_{1 \leq i < j \leq n} (a_i - a_j)^2$$

be the discriminant of $f(x)$. (a) Show that $\Delta \in K$. (b) Let $G \subset S_n$ be the Galois group of F/K acting on roots of $f(x)$. Show that $G \subset A_n$ if and only if Δ is a square in K.
10. Let $F = \mathbb{C}(x_1, \ldots, x_n)$ be the field of rational functions in n variables. (a) Suppose A_n acts on F by even permutations of variables. Show that F^{A_n} is generated

[0]This homework is due before class on Monday Feb 22. The grader will grade 5 random problems from this assignment. A problem with multiple parts (a), (b), etc. counts as one problem. You can ask the grader not to grade *two* of the problems.

over $\mathbb{C}$ by elementary symmetric functions $\sigma_1, \dots, \sigma_n$ in variables $x_1, \dots, x_n$ and by $\prod_{1\leq i<j\leq n}(x_i - x_j)$. (b) Suppose $n = 4$ and suppose D_4 acts on F by permutations of variables (here we identify variables with vertices of the square). Show that F^{D_4} is generated over $\mathbb{C}$ by 4 functions and find them.

11. Let G be a finite Abelian group. (a) Show that there exists a positive integer n and a subgroup $\Gamma \subset \mathbb{Z}_n^*$ such that $G \simeq \mathbb{Z}_n^*/\Gamma$. (b) Show that there exists a Galois extension $K/\mathbb{Q}$ with a Galois group G. (It is a famous open problem to remove an Abelian assumption from this exercise).

12. Compute the Galois group of the polynomial (a) $x^3 - x - 1$ over $\mathbb{Q}(\sqrt{-23})$; (b) $x^3 - 2tx + t$ over $\mathbb{C}(t)$ (the field of rational functions in one variable).

13. Compute the Galois group of the polynomial $x^4 - 4x^2 - 1$ over $\mathbb{Q}$.

14. Suppose $f(x) \in \mathbb{Q}[x]$ is an irreducible polynomial such that one of its complex roots has absolute value 1. Show that $f(x)$ has even degree and is palindromic: if $f(x) = a_0 + a_1x + \ldots + a_nx^n$ then $a_0 = a_n$, $a_1 = a_{n-1}$, etc.

15. Let $\Phi_n(x)$ be the n-th cyclotomic polynomial, a a non-zero integer, p a prime. Assume that p does not divide n. Prove that $p|\Phi_n(a)$ if and only if a has order n in $(\mathbb{Z}/p\mathbb{Z})^*$.

16. Let $K = \mathbb{C}[z^{-1}, z]]$ be the field of Laurent series (series in z, polynomials in z^{-1}). Let $K_m = \mathbb{C}[z^{\frac{-1}{m}}, z^{\frac{1}{m}}]] \supset K$. (a) Show that K_m/K is Galois with a Galois group $\mathbb{Z}/m\mathbb{Z}$. (b) Show that any Galois extension F/K with a Galois group $\mathbb{Z}/m\mathbb{Z}$ is isomorphic to K_m. (c) In the notation of Problem 6, show that

$$K^{ab} = \bigcup_{m\geq 1} K_m,$$

the field of Puiseux series[1].

17. Show that any group of order n is solvable, where (a) $n = p^2q$ and p, q are distinct primes; (b) $n = 2pq$ and p, q are odd primes.

18. Let M be a module over a ring R. A sequence of submodules

$$M = M_1 \supset M_2 \supset \ldots \supset M_r = 0$$

is called a filtration of M (of length r). A module M is called simple if it does not contain any submodules other than 0 and itself. A filtration is called simple if each M_i/M_{i+1} is simple. A module M is said to be of finite length if it admits a simple finite filtration. Two filtrations of M are called equivalent if they have the same length and the same collection of subquotients $\{M_1/M_2, M_2/M_3, \dots, M_{r-1}/M_r\}$ (up to isomorphism). Prove that if M has finite length then any two simple filtrations of M are equivalent and any filtration of M can be refined to a simple filtration.

19. Describe all Abelian groups G that fit into the exact sequence

$$0 \to \mathbb{Z}_n \to G \to \mathbb{Z}_m \to 0$$

(n and m are not necessarily coprime).

[1] Newton proved that K^{ab} is in fact algebraically closed.