ALGEBRA PRELIMINARY EXAM: PART II

Choose two of the following three problems.

Problem 1

Let K/F be a finite Galois extension and $g \in \text{Gal}(K/F)$. Compute the characteristic polynomial of g, where g is considered as an F-linear map from K to K.
(Hint: first consider the case where K/F is cyclic, i.e., $\text{Gal}(K/F)$ is a cyclic group.)

Problem 2

Consider the polynomial $f(x) = x^6 - 4x^3 + 1$. Let L be the splitting field of $f(x)$ over $\mathbb{Q}$.

(a) Show that
  (i) $f(x)$ has two real roots: α and α^{-1}.
  (ii) $x^3 - 1$ splits in L.

  Let $\zeta \in L$ be a primitive cube root of unity.

(b) Determine the degree of $L/\mathbb{Q}$. (You may use without proof the fact that when viewed modulo 5 the polynomial $f(x)$ does not have any quadratic factors in $\mathbb{F}_5[x]$.)

(c) Prove that $\sqrt[7]{5} \notin L$.

(d) Prove that $\text{Gal}(L/\mathbb{Q}) \simeq D_{12}$, here D_{12} denotes the dihedral group of order 12. (Hint: consider the action of $\text{Gal}(L/\mathbb{Q})$ on the roots of $f(x)$.)

(e) Use α and ζ to describe all the subfields $F \subseteq L$ such that L/F is quadratic and $L/\mathbb{Q}$ is Galois.

Problem 3

Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial and $p \in \mathbb{Z}$ be a prime. Consider the reduction of $f(x)$ modulo p, denoted $\overline{f}(x) \in \mathbb{F}_p[x]$, and assume that $\overline{f}$ has no multiple roots.

Let $L/\mathbb{Q}$ be the splitting field of f. Consider the roots of $f(x)$

$$\alpha_1, \dots, \alpha_r \in L,$$

and the subring of L that they generate

$$A := \mathbb{Z}[\alpha_1, \dots, \alpha_r] \subseteq L.$$

You may use without proof the fact that $A \cap \mathbb{Q} = \mathbb{Z}$.

Set $G := \text{Gal}(L/\mathbb{Q})$ and $\overline{G}$ to be the Galois group of $\overline{f}$ over $\mathbb{F}_p$.

Date: August 22, 2013.

(a) Consider the set S_p of maximal ideals $Q \subseteq A$ such that $Q \cap \mathbb{Z} = p\mathbb{Z}$. Show that the set S_p is non-empty, and that the action of G on L induces an action of G on S_p.

(b) Fix $P \in S_p$. Let $H \subseteq G$ be the stabilizer of the ideal P in G.
   (i) Show that the choice of the maximal ideal $P \in S_p$ induces a homomorphism $\pi : H \to \overline{G}$.
   (ii) Prove that the homomorphism $\pi : H \to \overline{G}$ is injective.
   (Hint: consider the action of $\pi(h)$ on the roots of $\overline{f}$ for $h \in H \setminus \{1_G\}$.)

(c) For every $a \in A$, there exists $t_a \in A$ such that

$$t_a \equiv a \bmod P,$$
$$g(t_a) \in P \text{ for } g \notin H.$$

The existence of t_a (which you may assume without proof) is a consequence of the Chinese Remainder Theorem for the ring A. Using $t_a \in A$ as above, we define the polynomial

$$w_a(x) = \prod_{g \in G} (x - g(t_a)) \in A[x].$$

   (i) Show that $w_a(x) \in \mathbb{Z}[x]$, and let $\overline{w}_a(x)$ be its reduction modulo p. Show that if the reduction $\overline{a}$ (mod P) is non-zero, then every conjugate of $\overline{a}$ is of form $\overline{h}(\overline{a})$ for some $h \in H$.
   (ii) Prove that $\pi : H \to \overline{G}$ is an isomorphism.

(d) Consider the factorization of $\overline{f}$ into irreducible factors in $\mathbb{F}_p[X]$

$$\overline{f} = \overline{g}_1 \cdot \overline{g}_2 \cdot \cdots \cdot \overline{g}_r$$

where $d_i := \deg(\overline{g}_i)$. Prove that there exists an element $h \in H$ of cycle type $(d_1, d_2, \ldots, d_r)$, here h is viewed as a permutation of the roots of f.

Recall the cycle type refers to the lengths of the cycles when you express a permutation as a product of disjoint cycles. E.g. the permutation $(12)(345) \in S_5$ has cycle type $(2, 3)$.