MATH 603: HOMEWORK #6

THESE PROBLEMS ARE DUE IN TED'S MAILBOX BY 5 P.M. ON MAY 5, 2017.

1. Constructing A_4 extensions of fields.

This set of exercises has to do with constructing A_4 extensions N of a field F of characteristic not 2.

1. Suppose L/F is a cyclic cubic extension of fields of characteristic not equal to 2. Write $H = \mathrm{Gal}(L/F) = \{e, \sigma, \sigma^2\}$. For $\beta \in L$ define $\mathrm{Norm}_{L/F}(\beta) = \prod_{h \in H} h(\beta)$. Suppose $\beta \in L^*$ is not in F or $(L^*)^2$, and that $Norm_{L/F}(\beta) = 1$. Show that if ξ_1 is a root of $X^2 - \beta$, then the Galois closure of $L(\xi_1)$ over F is an A_4-extension N of F. (Hints: If $L(\xi_1)$ were already Galois over F, show $\sigma(\beta)/\beta \in (L^*)^2$ and get a contradiction from $Norm_{L/F}(\beta) = 1$.)
2. Suppose $F = \mathbb{Q}$ and $L = \mathbf{Q}(\zeta_7 + \zeta_7^{-1})$. Use the cyclotomic theory discussed in class to show that L/F is a cyclic cubic extension. Then show $\beta = \zeta_7 + \zeta_7^{-1}$ has the properties required in problem #1 to produce an A_4 extension of $\mathbf{Q}$. (Hint: Consider the embeddings of L into $\mathbf{R}$.)
3. Suppose $F = F_q$ is a finite field of odd order q and that L/F is a cyclic cubic extension. Can there be an element β with the properties in problem #1? Can you give an alternate proof of your conclusion using what you know about the multiplicative group of L and a canonical generator σ of $\mathrm{Gal}(L/F)$?

2. Kummer Theory.

Suppose L is a field, $n > 0$ is prime to the characteristic of L and that L contains a root of unity ζ of order n. Let μ_n be the cyclic subgroup of L^* generated by ζ. Suppose B is a subgroup of L^*. Let L_B be the compositum in an algebraic closure of L of all the extensions $L(a^{1/n})$ with $a \in B$. The extension L_B/L is Galois; let $G = Gal(L_B/L)$. The Kummer pairing

$$G \times \left(\frac{B \cdot (L^*)^n}{(L^*)^n} \right) \to \mu_n$$

is defined by

$$\langle g, [b] \rangle = \frac{g(b^{1/n})}{b^{1/n}}$$

for any choice of n^{th} root $b^{1/n}$ of $b \in B$ in L_B.

4. Suppose L/F is a Galois extension with group $\Gamma = Gal(L/F)$. Suppose the action of Γ takes B to B. Show that the extension L_B is Galois over F. Define $H = Gal(L_B/F)$. Show that the Kummer pairing is Γ-equivariant, in the following sense. Suppose $\sigma \in H$. Then for $g \in Gal(L_B/L)$, one has $\sigma g \sigma^{-1} \in G = Gal(L_B/L)$ and

   $$\langle \sigma g \sigma^{-1}, [\sigma(b)] \rangle = \sigma(\langle g, [b] \rangle).$$

   Note that in the exact sequence

   $$\{1\} \to Gal(L_B/L) \to Gal(L_B/F) \to Gal(L/F) \to \{1\}$$

   the group $Gal(L_B/L)$ is abelian. So $\sigma g \sigma^{-1}$ depends only on g and the image $\tilde{\sigma}$ of σ in $Gal(L/F)$. This describes the conjugation action of the quotient group $\Gamma = Gal(L/F)$ of H on the normal abelian subgroup $G = Gal(L_B/L)$.

5. In class we said that the Kummer pairing gives an isomorphism
$$G = Hom(\frac{B \cdot (L^*)^n}{(L^*)^n}, \mu_n).$$
Show that this is a Γ-equivariant in the following sense. The action of Γ on G is the conjuation action described in problem 9. If M and F are Γ modules, the action of $\gamma \in \Gamma$ on $f \in Hom(M, N)$ sends f to the homorphism (γf) defined by $(\gamma f)(m) = \gamma(f(\gamma^{-1}m))$ for $m \in M$.
6. Suppose G and Γ are finite of co-prime orders. Show that $Gal(L_B/F)$ is isomorphic to the semi-direct product of $\Gamma = Gal(F/L)$ and $G = Gal(L_B/L)$ with conjugation action defined in problems 4 and 5.
7. Suppose L/F is cyclic of degree 3 and that $char(L)$ does not have characteristic 2. Show that the A_4 extensions of F which contain L correspond bijectively to the order 4 subgroups $(B \cdot (L^*)^2)/(L^*)^2$ of $L^*/(L^*)^2$ which are stable under the action of $Gal(L/F)$ and have no non-trivial invariant elements under the action of $Gal(L/F)$. What kind of extensions of F would one get if you dropped the last condition about invariant elements?

3. Traces and Norms.

Suppose L/F is a finite extension of fields and that $\alpha \in L$. Multiplication by $\alpha \in L$ gives an F-linear transformation $m(\alpha) : L \to L$. Suppose $M(\alpha)$ is the matrix of this linear transformation relative to some basis for L over F. The characteristic polynomial of $M(\alpha)$ is
$$c_\alpha(z) = \det(z \cdot I - M(\alpha))$$
where I is the identity matrix of size $[L : F] \times [L : F]$. This does not depend on the choice of basis for L over F. The constant term of $c_\alpha(z)$ is
$$c_\alpha(0) = (-1)^{[L:F]}\det(M(\alpha))$$
and the sum $Tr_{L/F}(\alpha)$ of the diagonal entries of $M(\alpha(z))$ is -1 times the coefficient of $z^{[L:F]-1}$ in $c_\alpha(z)$. Here $Tr_{L/F}(\alpha)$ is the trace of α and $\det(M(\alpha))$ is the norm $\mathrm{Norm}_{L/F}(\alpha)$ of α from L to F.

9. Let
$$f(x) = \mathrm{Irred}(X, \alpha, F) = x^d + b_{d-1}x^{d-1} + \cdots + b_d = \prod_{i=1}^{d_s}(x - \gamma_i)^{d/d_s}$$
be the irreducible polynomial of α in $F[x]$ where $d_s = [F(\alpha) : F]_s$ is the separable degree of $F(\alpha)$ over F, $\{\gamma_i\}_{i=1}^{d_s}$ are the distinct roots of $f(x)$ in an algebraic closure containing L and d/d_s is the inseparable degree of $F(\alpha)$ over F. Show that if we make L into an $F[x]$ module by letting x act by multiplication by α, the associated rational canonical form is a block diagonal matrix with the companion matrix of $f(x)$ in each block. How many blocks are there?
10. With the notations of the previous problem, show that
$$\mathrm{Tr}_{L/F} = -[L : F(\alpha)]b_{d-1} = [L : F(\alpha)_s]\sum_{i=1}^{d_s}\gamma_i$$
and
$$\mathrm{Norm}_{L/F} = (-1)^{[L:F]}b_0^{[L:F(\alpha)]} = (\prod_{i=1}^{d_s}\gamma_i)^{[L:F(\alpha)_s]}$$
where $F(\alpha)_s$ is the maximal subextension of $F(\alpha)$ which is separable over F.
11. Explain why this definition of the trace and the norm generalizes the ones given for Galois extensions L/F in problems #17 and #18 of section 14.2 of Dummit and Foote's book.

12. Show that the trace $Tr_{L/F} : L \to F$ is the zero function if and only if L/F is not a separable extension. (You can use the fact that if L/F is a finite extension, the distinct embeddings of L into an algebraic closure $\overline{F}$ of F are $\overline{F}$-linearly independent.)

13. Suppose $F = \mathbb{Q}$, $n \geq 1$ is an integer and that L is the cyclotomic field $\mathbb{Q}(\zeta_n)$ generated by a primitive n^{th} root of unity ζ_n. Calculate $\mathrm{Tr}_{L/\mathbb{Q}}(\zeta_n)$ in terms of the factorization $n = p_1^{a_1} \cdots p_m^{a_m}$ of n into a product of powers of distinct primes. (Hint: show that you can take $\zeta_n = \prod_i \zeta_{p_i^{a_i}}$ and use $\mathrm{Gal}(L/\mathbb{Q}) = (\mathbb{Z}/n)^* = \prod_i (\mathbb{Z}/p_i^{a_i})^*$.)