Math 5286H: Fundamental Structures of Algebra I

Take Home Exam 2, (Due in class, April 13th, 2012)

This is an open book, open notes, open library take-home exam. You are allowed to consult other Algebra texts for reference as long as you cite your sources, but you are not permitted to copy answers out of them. You are not allowed to collaborate, use the internet, or use electronic devices, other than the course website, an e-book of Artin, or a basic calculator. The instructor is the only human source you are allowed to consult. Give reasoning for all of your answers. Good luck!

1) For the following irreducible polynomials $f(x)$ over $\mathbb{Q}$, compute the Galois group of $K/\mathbb{Q}$, where $K$ is the splitting field for $f(x)$.
   (a) (3 points) $f(x) = x^3 + 3x + 15$.
   (b) (3 points) $f(x) = x^3 - 21x + 7$.
   (c) (4 points) $f(x) = x^4 + 4x^2 + 2$.
   (d) (5 points) Let $\zeta_{11}$ denote a primitive 11th root of unity and $K = \mathbb{Q}(\zeta_{11})$. Compute $\text{Gal}(K/\mathbb{Q})$, and determine all intermediate fields $L$, i.e. $K \supseteq L \supseteq \mathbb{Q}$.
   (e) (10 points) Let $p$ be a prime and $f(x) = x^p - a \in F[x]$ be irreducible. Let $\alpha$ be a root of $f$ in an extension field. Show that if $F(\alpha)/F$ is a Galois extension, then $g(x) = x^p - 1$ splits in the field $F$.

2) (a) (5 points) Let $p$ be an odd prime. Prove that exactly half of the elements of $\mathbb{F}_p^\times$ are squares.
   (b) (5 points) Show if $p$ is an odd prime and $\alpha, \beta$ are both nonsquares in $\mathbb{F}_p$, then their product $\alpha\beta$ is a square.
   (c) (5 points) Prove that in a finite field $\mathbb{F}_q$ of even order, every element is a square.
   (d) (5 points) Use the above to give a counter-example to the converse of Proposition 12.4.3. In other words, show that there exists an irreducible polynomial $f$ in $\mathbb{Q}[x]$ such that its residue modulo $p$, $\overline{f} = \psi_p(f)$, is reducible for every prime $p$.

Hint: Consider the irreducible polynomial for $\gamma = \sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$. 

1
3) Let $F = \mathbb{F}_p$, where $p$ is a prime, and $K = \mathbb{F}_q$, where $q = p^r$. Recall that the Frobenius map $\phi$, defined by $\phi(x) = x^p$, is an automorphism of $F$.

(a) (5 points) Prove that $Gal(K/F)$ is a cyclic group of order $r$, and that this group is generated by the Frobenius map $\phi$. Show that $K/F$ is a Galois extension.

(b) (5 points) Let $L$ be an intermediate field, i.e. $K \supseteq L \supseteq F$. Are $L/F$ and $K/L$ Galois extensions? What are their Galois groups?

(c) (5 points) Prove that the Main Theorem of Galois Theory, Theorem 16.7.1, is satisfied for the extension $K/F$ even though $F$ is not characteristic zero.

4) Let $p$ be a prime number. For every integer $d \geq 0$, there is a polynomial $P_d(x)$ so that $P_d(p)$ counts the number of monic irreducible polynomials of degree $d$ in $\mathbb{F}_p[x]$.

(a) (3 points) Find and prove such a formula for $d = 2$.

(b) (5 points) For $d = 3$?

(c) (7 points) For $d = 4$?

**Hint:** Consider Problem 15.7.4 from HW 4.

5) Let $K/F$ be a Galois extension. We define the Norm of $\alpha \in K$ (with respect to the field extension $K/F$) as $N_{K/F}(\alpha) := \prod_{\sigma \in Gal(K/F)} \sigma(\alpha)$.

(a) (5 points) Prove that $N_{K/F}(\alpha) \in F$.

(b) (5 points) Prove that $N_{K/F}(\alpha \beta) = N_{K/F}(\alpha)N_{K/F}(\beta)$.

(c) (5 points) Let $K = F(\sqrt{D})$. (You may assume char $F \neq 2$.) Show that $N_{K/F}(a + b\sqrt{D}) = a^2 - Db^2$ using this definition.

(d) (5 points) Let $f(x) = x^d - a_1x^{d-1} + \cdots + (-1)^da_d \in F[x]$ be the irreducible polynomial for $\alpha \in K/F$. Let $[K : F] = n$.

Prove that $d$ divides $n$ and that there are $(n/d)$ automorphisms $\sigma \in Gal(K/F)$ such that $\sigma(\alpha) = \alpha$.

(e) (5 points) Conclude from (d) that $N_{K/F}(\alpha) = a_d^{n/d}$.

(f) (Bonus) Define the trace, $Tr_{K/F}(\alpha) = \sum_{\sigma \in Gal(K/F)} \sigma(\alpha)$ under the same assumptions as above.

Prove that $Tr_{K/F}(\alpha) \in F$, $Tr_{K/F}(\alpha + \beta) = Tr_{K/F}(\alpha) + Tr_{K/F}(\beta)$, and $Tr_{K/F}(\alpha) = \frac{n}{d}a_1$. Here, $a_1$ is the coefficient of $-x^{d-1}$ in $f(x)$, the irreducible polynomial for $\alpha$. 