Math 562 **Spring 2012**
Homework 5 **Drew Armstrong**

Problems that are all connected:

We say that a polynomial $f(x_1, x_2, \ldots, x_n) \in F[x_1, x_2, \ldots, x_n]$ is symmetric if for **every** permutation σ of $\{1, 2, \ldots, n\}$ we have

$$f = f(x_1, x_2, \ldots, x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) = \sigma(f).$$

The elementary symmetric polynomials $e_1, \ldots, e_n \in F[x_1, \ldots, x_n]$ are defined implicitly by

$$t^n - e_1 t^{n-1} + e_2 t^{n-2} - \cdots + (-1)^n e_n := (t - x_1)(t - x_2) \cdots (t - x_n),$$

where t is an indeterminate. Newton's Theorem says that the subring of $F[x_1, \ldots, x_n]$ consisting of symmetric polynomials is equal to $F[e_1, \ldots, e_n]$ (i.e. every symmetric polynomial can be written uniquely as a polynomial in $e_1, \ldots, e_n$).

1. The polynomial $x_1^3 + x_2^3 + \cdots + x_n^3$ is clearly symmetric. Express it as an element of $F[e_1, e_2, \ldots, e_n]$.

2. Consider a polynomial $f(x) \in F[x]$ and let $F \subseteq K$ be a field extension that contains the roots $\alpha_1, \ldots, \alpha_n$ of $f(x)$ (i.e. K contains the splitting field of $f(x)$). If $\alpha = g(\alpha_1, \ldots, \alpha_n) \in K$ for some **symmetric** polynomial g, prove that α is actually in F.

3. The Splitting Theorem. Consider $f(x) \in F[x]$ with splitting field $F \subseteq K$ (i.e. $K = F(\alpha_1, \ldots, \alpha_n)$ where $\alpha_1, \ldots, \alpha_n$ are the roots of $f(x)$.) If $g(x) \in F[x]$ is irreducible over F and has one root in K, then $g(x)$ actually **splits** in K. Your assignment is to **read and understand the following proof**.

Proof. Suppose that $g(x) \in F[x]$ is irreducible and has a root $\beta_1 \in K$. Then we can write $\beta_1 = p(\alpha_1, \ldots, \alpha_n)$ for some polynomial p in the roots of $f(x)$. Let $\{\beta_1, \ldots, \beta_k\}$ be the set of values of $p(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) \in K$ as σ runs over all permutations of $\{1, 2, \ldots, n\}$ (you can note that $k \leq n!$, but this fact is not important). We claim that the polynomial

$$h(x) := (x - \beta_1)(x - \beta_2) \cdots (x - \beta_k) \in K[x]$$

is actually in $F[x]$. Indeed, the coefficients of $h(x)$ are the elementary symmetric polynomials in $\beta_1, \ldots, \beta_k$. Since each $\beta_i \in K$ is a polynomial in the α_j (as is **any** element of K), the coefficients of $h(x)$ are polynomials in the α_j. Now note that any permutation of the α_j induces a permutation of the β_i (by definition). Since the coefficients of $h(x)$ are symmetric under permutations of the β_i, they are also symmetric under permutations of the α_j. By Problem 2, we conclude that $h(x) \in F[x]$.

Finally, note that $g(x)$ is the minimal polynomial for β_1 over F; i.e. the evaluation map $\varphi_{\beta_1} : F[x] \to K$ has kernel $(g(x))$. Since $h(\beta_1) = 0$ we have $h(x) \in (g(x))$, hence $g(x)$ divides $h(x)$. Then since $h(x)$ splits in K, so does $g(x)$. $\square$

4. Let $F \subseteq K$ be a normal field extension (this means that K is the splitting field for some (non-unique) polynomial over F). Given any $\alpha \in K$, let $m_\alpha(x) \in F[x]$ be its minimal polynomial. Then we define the **norm of** α by

$$N_{K/F}(\alpha) := (\alpha_1 \alpha_2 \cdots \alpha_k)^{[K:F]/\deg(m_\alpha(x))},$$

where $\alpha_1, \ldots, \alpha_k$ are the roots of $m_\alpha(x)$. (Without loss, you can say $\alpha = \alpha_1$.)

(a) Prove that $[K : F]/\deg(m_\alpha(x)) \in \mathbb{Z}$.
(b) Use The Splitting Theorem to prove that $N_{K/F}(\alpha) \in K$.
(c) Then use Problem 2 to prove that actually $N_{K/F}(\alpha) \in F$.

(d) Suppose $0 \neq d \in \mathbb{Z}$ is squarefree (i.e. has no repeated prime factor) and consider the quadratic field extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{d})$. Given $a, b \in \mathbb{Q}$, find the minimal polynomial of $a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ over $\mathbb{Q}$ and use this to compute the norm $N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(a + b\sqrt{d})$. Do you recognize this? (All things are connected.)

5. Consider $\gamma = \sqrt[3]{2} \in \mathbb{R}$ and $\omega = e^{2\pi i/3} \in \mathbb{C}$.

(a) Prove that $\mathsf{Gal}(\mathbb{Q}(\gamma)/\mathbb{Q})$ is trivial, and hence $\mathbb{Q}(\gamma)$ is **not** the splitting field of $x^3 - 2 \in \mathbb{Q}[x]$.
(b) Prove that the splitting field of $x^3 - 2 \in \mathbb{Q}[x]$ is $\mathbb{Q}(\gamma, \omega)$.
(c) Prove that $G = \mathsf{Gal}(\mathbb{Q}(\gamma, \omega)/\mathbb{Q})$ is isomorphic to the dihedral group D_3 of size 6. [Hint: An element is determined by how it acts on γ and ω. Define σ by $(\sigma(\gamma) := \omega\gamma, \sigma(\omega) := \omega)$ and define ρ by $(\rho(\gamma) := \gamma, \rho(\omega) := \omega^2)$. Recall the description of D_3 as a semi-direct product.] Note: This is the smallest nonabelian group in the world.

6. The norm from Problem 4 can be defined equivalently in terms of the Galois group. Let $F \subseteq K$ be a normal extension with Galois group $G = \mathsf{Gal}(K/F)$. For each $\alpha \in K$ we define the **norm**

$$N_{K/F}(\alpha) := \prod_{\sigma \in G} \sigma(\alpha) \in K.$$

(a) Use this definition to give a different proof that actually $N_{K/F}(\alpha) \in F$. [Hint: For all $\mu \in G$, show that $\mu(N_{K/F}(\alpha)) = N_{K/F}(\alpha)$.]
(b) Consider the field $\mathbb{Q}(\omega)$, where $\omega = e^{2\pi i/3}$. The minimal polynomial of ω over $\mathbb{Q}$ is $x^2 + x + 1$, hence $\mathbb{Q}(\omega)$ has basis $1, \omega$ as a vector space over $\mathbb{Q}$. Compute a formula for the inverse of $a + b\omega \in \mathbb{Q}(\omega)$. Use the norm in your answer. [Hint: It's "the same" as the formula for inverting a complex number; i.e. $z^{-1} = \bar{z}/|z|^2$.]