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 $F[e_1, e_2, \ldots, e_n]$.

Proof. I will use the notation

$$p_k := x_1^k + x_2^k + \cdots + x_n^k$$

for the kth power sum symmetric polynomial. The difficulty here is how to deal with n. For $n = 1$ we have $p_3 = x_1^3 = e_1^3$ and for $n = 2$ we have $p_3 = x_1^3 + x_2^3 = (x_1 + x_2)^3 - 3(x_1 + x_2)(x_1 x_2) = e_1^3 - 3e_1 e_2$. I claim that for all $n \geq 3$ we have $p_3 = e_1^3 - 3e_1 e_2 + 3e_3$ (i.e. the problem stabilizes).

To show this I will introduce the lexicographic order on degree sequences: say that

$$\alpha = (\alpha_1, \ldots, \alpha_n) < \beta = (\beta_1, \ldots, \beta_n)$$

if there exists ℓ such that $\alpha_\ell < \beta_\ell$ and $\alpha_i = \beta_i$ for all $1 \leq i < \ell$. (That is, in the leftmost position in which α and β differ, β is larger. Note that this is the same as the natural order on integers with at most n decimal digits.) Given $f \in F[x_1, \ldots, x_n]$, its leading term is the term with the largest degree sequence.

So let $n \geq 3$ and observe that p_3 has leading term x_1^3. Next note that e_1^3 has leading term x_1^3 and second-largest term $3x_1^2 x_2$. (Indeed, every term of e_1^3 has degrees summing to 3.) Subtracting e_1^3 from p_3 gives us another symmetric polynomial with **smaller leading term**: $p_3 - e_1^3 = -3x_1^2 x_2 +$ lower order terms. Next note that $3e_1 e_2$ has leading term $3x_1^2 x_2$. (Again, every term of $e_1 e_2$ has degrees summing to 3, so the only possible term higher than $x_1^2 x_2$ is x_1^3, and this does not occur.) Adding $3e_1 e_2$ to $p_3 - e_1^3$ then gives

$$p_3 - e_1^3 + 3e_1 e_2 = 3x_1 x_2 x_3 + \text{lower order terms}.$$

I claim that the expression on the right actually equals $3e_3$. How do I know this? Since $p_3 - e_1^3 + 3e_1 e_2$ is symmetric, we must have $p_3 - 3e_1^3 + 3e_1 e_2 = 3e_3 + f$, for some symmetric $f \in F[x_1, \ldots, x_n]$ with highest term of degree strictly less than $(1, 1, 1, 0, \ldots, 0)$. But every term of f has degrees adding to 3, thus the only possibilities are permutations of $\{3, 0, \ldots, 0\}$, $\{2, 1, 0, \ldots, 0\}$ or $\{1, 1, 1, 0, \ldots, 0\}$. If f contains any of these three types, then by symmetry it must contain a term with degree sequence $(3, 0, \ldots, 0)$, $(2, 1, 0, \ldots, 0)$ or $(1, 1, 1, 0, \ldots, 0)$. This contradicts the fact that every term of f is strictly smaller than $(1, 1, 1, 0, \ldots, 0)$. Hence $f = 0$ and we conclude that $p_3 = e_1^3 - 3e_1 e_2 + 3e_3$. $\square$

[At every step of the algorithm we subtract a polynomial of the form $e_\alpha := e_1^{\alpha_1} e_2^{\alpha_2} \cdots e_n^{\alpha_n}$. Note that every term of e_α has degrees summing to exactly $1\alpha_1 + 2\alpha_2 + \cdots + n\alpha_n$ (just call this constant d), hence we say that the polynomial e_α is **homogeneous of degree** d. More generally, we say that a polynomial $f \in F[x_1, \ldots, x_n]$ has "total degree" d if d is the maximum sum of exponents over the terms of f.. It follows from these observations that every symmetric polynomial $f \in F[x_1, \ldots, x_n]$ of total degree d satisfies $f \in F[e_1, \ldots, e_d]$, independently of n. (Note that p_3 is homogeneous of degree 3, hence $p_3 \in F[e_1, e_2, e_3]$.)]

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.

Proof. By assumption, the polynomial $f(x) \in K[x]$ splits as

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

It follows that the elementary symmetric polynomials $e_1, \ldots, e_n$ evaluated at $(\alpha_1, \ldots, \alpha_n)$ are in the field F (because by definition these are $\pm$ the coefficients of $f(x)$, which is in $F[x]$). Finally, let $g \in F[x_1, \ldots, x_n]$ be symmetric. By Newton's theorem we can write g as a polynomial in $e_1, \ldots, e_n$ with coefficients in F. Evaluate everything at $(x_1, \ldots, x_n) \mapsto (\alpha_1, \ldots, \alpha_n)$ to conclude that $g(\alpha_1, \ldots, \alpha_n) \in F$. □

[This proof has two steps. 1. Note that every symmetric combination of the roots is a polynomial in **elementary** symmetric combinations of the roots (Newton's Theorem). 2. Note that every elementary symmetric combination of the roots is a coefficient, hence it's in F. You could think of this as the very first theorem of Galois theory.]

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 $g(x)$. □

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 $[K : F]/\deg(m_\alpha(x)) \in \mathbb{N}$.
(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.)

Proof. First we prove (a). Given any $\alpha \in K$ with minimal polynomial $m_\alpha(x) \in F[x]$, we consider the intermediate field $F \subseteq F(\alpha) \subseteq K$. Then the Tower Law says

$$[K : F] = [K : F(a)] \cdot [F(a) : F] = [K : F(a)] \cdot \deg(m_\alpha(x)).$$

We conclude that $\deg(m_\alpha(x))$ divides $[K : F]$, hence $[K : F]/\deg(m_\alpha(x)) \in \mathbb{N}$.

To prove (b), note that the irreducible polynomial $m_\alpha(x) \in F[x]$ has one root in K (namely, α). Since K is the splitting field for some polynomial in $F[x]$ (namely, $m_\alpha(x)$), the Splitting Theorem says that all of the roots $\alpha_1, \alpha_2, \ldots, \alpha_k$ are in K. We conclude that any power of the product $\alpha_1 \cdots \alpha_k$ is in K, hence $N_{K/F}(\alpha) \in K$.

To prove (c), let $r = [K : F]/\deg(m_\alpha(x))$. Then the polynomial $g(x_1, \ldots, x_k) := x_1^r x_2^r \cdots x_k^r$ is symmetric, hence Problem 2 implies that $N_{K/F}(\alpha) = g(\alpha_1, \ldots, \alpha_k) \in F$.

Finally, let $d \in \mathbb{Z}$ be squarefree, so $\sqrt{d}$ is irrational and $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{d})$ is a degree 2 field extension. In fact, $\mathbb{Q}(\sqrt{d})$ is the splitting field of $x^2 - d \in \mathbb{Q}[x]$, so parts (a),(b),(c) will apply. Now consider an element $a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ with $b \neq 0$. The minimal polynomial of $a + b\sqrt{d}$ over $\mathbb{Q}$ is

$$(x - (a + b\sqrt{d}))(x - (a - b\sqrt{d})) = x^2 - 2ax + (a^2 - db^2) \in \mathbb{Q}[x].$$

(Since $a \pm b\sqrt{d}$ are irrational, this quadratic polynomial has no rational root, hence it's irreducible over $\mathbb{Q}$.) We conclude that the norm is

$$N_{\mathbb{Q}(d)/\mathbb{Q}}(a \pm b\sqrt{d}) = ((a + b\sqrt{d})(a - b\sqrt{d}))^{2/2} = a^2 - db^2 \in \mathbb{Q}.$$

If $b = 0$ then the minimal polynomial of $a \in \mathbb{Q}(d)$ over $\mathbb{Q}$ is $x - a \in \mathbb{Q}[x]$. In this case the formula gives $N_{\mathbb{Q}(d)/\mathbb{Q}}(a) = (a)^{2/1} = a^2$, which still looks good. □

[Notice that the norm is a natural generalization of $|z|^2$ for complex numbers. In fact if $d < 0$ (the case of imaginary quadratic fields) then $|a + b\sqrt{d}|^2 = a^2 - db^2$ is a true statement. (See Chapter 13 of Artin.) You used this on HW2 to prove that $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain.]

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.

Proof. Let $\mu \in \mathsf{Gal}(\mathbb{Q}(\gamma)/\mathbb{Q})$. Then μ is determined by the single value $\mu(\gamma) \in \mathbb{Q}(\gamma)$. Furthermore, since $\gamma^3 - 2 = 0$ we must have $0 = \mu(0) = \mu(\gamma^3 - 2) = \mu(\gamma)^3 - 2$, so $\mu(\gamma)$ is also a root of $x^3 - 2 \in \mathbb{Q}[x]$. But $\mathbb{Q}(\gamma) \subseteq \mathbb{R}$ and $x^3 - 2$ has only one real root (namely, γ). Hence the only choice is $\mu(\gamma) = \gamma$ and we conclude that μ is the identity map. In particular, we have $|\mathsf{Gal}(\mathbb{Q}(\gamma)/\mathbb{Q})| = 1 < [\mathbb{Q}(\gamma) : \mathbb{Q}] = 3$, which means that $\mathbb{Q}(\gamma)$ is not a splitting field for any polynomial in $\mathbb{Q}[x]$. (You can just quote this from class.)

So what is the splitting field of $x^3 - 2 \in \mathbb{Q}[x]$? The roots of $x^3 - 2$ are $\gamma, \omega\gamma, \omega^2\gamma$ (thought of as complex numbers), hence the splitting field is $K = \mathbb{Q}(\gamma, \omega\gamma, \omega^2\gamma) \subseteq \mathbb{C}$. Clearly $\gamma, \omega\gamma, \omega^2\gamma \in \mathbb{Q}(\gamma, \omega)$, hence $K \subseteq \mathbb{Q}(\gamma, \omega)$. Conversely, $\gamma \in K$ and $\omega = (\omega\gamma)/\omega \in K$ imply $\mathbb{Q}(\gamma, \omega) \subseteq K$, hence $K = \mathbb{Q}(\gamma, \omega)$.

You showed on Exam 2 that $[\mathbb{Q}(\gamma,\omega):\mathbb{Q}]=6$ so we expect a Galois group of size 6. Any element $\mu\in\mathsf{Gal}(\mathbb{Q}(\gamma,\omega)/\mathbb{Q})$ is determined by the two values $\mu(\gamma),\mu(\omega)\in\mathbb{Q}(\gamma,\omega)$. Furthermore, $\mu(\gamma)$ must be a root of x^3-2 and $\mu(\omega)$ must be a root of x^2+x+1. If we let σ denote the map $(\gamma,\omega)\mapsto(\omega\gamma,\gamma)$ and let ρ denote the map $(\gamma,\omega)\mapsto(\gamma,\omega^2)$ then we can generate all six group elements as in the following table:

1	σ	σ^2	ρ	$\rho\sigma$	$\rho\sigma^2$
$\gamma\mapsto\gamma$	$\gamma\mapsto\omega\gamma$	$\gamma\mapsto\omega^2\gamma$	$\gamma\mapsto\gamma$	$\gamma\mapsto\omega^2\gamma$	$\gamma\mapsto\omega\gamma$
$\omega\mapsto\omega$	$\omega\mapsto\omega$	$\omega\mapsto\omega$	$\omega\mapsto\omega^2$	$\omega\mapsto\omega^2$	$\omega\mapsto\omega^2$

(Here we use juxtaposition to denote composition; i.e. $\rho\sigma=\rho\circ\sigma$.) Note that the group is **not abelian** because $\rho\sigma$ sends $(\gamma,\omega)\mapsto(\omega^2\gamma,\omega^2)$, whereas $\sigma\rho$ sends $(\gamma,\omega)\mapsto(\omega\gamma,\omega^2)$. In fact, this shows that $\sigma\rho=\rho\sigma^2$. Recall the definition of the dihedral group D_3, the group of symmetries of an equilateral triangle. It is generated by a rotation R satisfying $R^3=1$, a flip F satisfying $F^2=1$, and the single relation $RF=FR^2$. Sending $\sigma\mapsto R$ and $\rho\mapsto F$ gives the desired group isomorphism $\mathsf{Gal}(\mathbb{Q}(\gamma,\omega)/\mathbb{Q})\xrightarrow{\sim}D_3$. We can also view this as a semi-direct product

$$\mathsf{Gal}(\mathbb{Q}(\gamma,\omega)/\mathbb{Q})=\langle\rho\rangle\ltimes\langle\sigma\rangle$$

where $\langle\sigma\rangle$ is a normal subgroup and the (non-normal) subgroup $\langle\rho\rangle$ **acts on** $\langle\sigma\rangle$ by conjugation, sending σ to $\rho\sigma\rho=\sigma^2$. $\square$

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. $z^{-1}=\bar{z}/|z|^2$.]

Proof. To show part (a), suppose $[K:F]=n$ and let $G=\{\sigma_1,\ldots,\sigma_n\}$. If $\mu\in G$, note that $G=\{\mu\sigma_1,\ldots,\mu\sigma_n\}$ is just a permutation of the group elements. Hence

$$\mu(\sigma_1(\alpha)\cdots\sigma_n(\alpha))=\mu\sigma_1(\alpha)\cdots\mu\sigma_n(\alpha)=\sigma_1(\alpha)\cdots\sigma_n(\alpha)\in K$$

and we conclude that $\mu(N_{K/F}(\alpha))=N_{K/F}(\alpha)$. Since this is true for all $\mu\in G$ we have that $N_{K/F}(\alpha)$ is an element of the fixed subfield $K^G\subseteq K$. By the Tower Law we have $[K:F]=[K:K^G]\cdot[K^G:F]$. We will see in class that $[K:K^G]=|G|=[K:F]$, which implies that $[K^G:F]=1$, or $K^G=F$. We conclude that $N_{K/F}(\alpha)\in F$.

Finally, part (b). Let's just write N for the norm $N_{\mathbb{Q}(\omega)/\mathbb{Q}}$. The Galois group $\mathsf{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ consists of the identity element 1 and the "conjugation" map σ defined by $\sigma(\omega):=\omega^2$. Note that $\sigma(a+b\omega)=\sigma(a)+\sigma(b)\sigma(\omega)=a+b\omega^2=a+b(-\omega-1)=(a-b)-b\omega$ for arbitrary $a,b\in\mathbb{Q}$. Thus we have

$$\begin{aligned}N(a+b\omega)&=1(a+b\omega)\sigma(a+b\omega)=(a+b\omega)(a+b\omega^2)\\&=a^2+ab(\omega+\omega^2)+b\omega^3=a^2-ab+b^2\in\mathbb{Q}.\end{aligned}$$

Finally we get

$$\frac{1}{a+b\omega}=\frac{1}{a+b\omega}\cdot\frac{\sigma(a+b\omega)}{\sigma(a+b\omega)}=\frac{(a-b)-b\omega}{a^2-ab+b^2}=\left(\frac{a-b}{a^2-ab+b^2}\right)-\left(\frac{b}{a^2-ab+b^2}\right)\omega.$$

More compactly, this is $(a+b\omega)^{-1}=\sigma(a+b\omega)/N(a+b\omega)$. Compare $z^{-1}=\bar{z}/|z|^2$. $\square$