MATH 470 Winter 2007

Graduate Algebra
Problem Set 2

1. Let $\mathbb{F}$ be a field of characteristic p and let $\mathbb{F} \subseteq \mathbb{E}$ be a normal extension. Define $\mathbb{F}_\infty \subseteq \mathbb{E}$ to be the subset

$$\mathbb{F}_\infty = \{ \ a \in \mathbb{E} \mid a^{p^n} \in \mathbb{F} \text{ for some } n \ \}.$$

Prove that $\mathbb{F}_\infty$ is a field, then $\mathbb{F} \subseteq \mathbb{F}_\infty$ is purely inseparable and the $\mathbb{F}_\infty \subseteq \mathbb{E}$ is separable.

Hint: recall that we have shown that if a is algebraic over $\mathbb{F}$, then the minimal polynomial can be written (over the algebraic closure of $\mathbb{F}$) as $h(x)^{p^n}$ for some separable polynomial $h(x)$. Show that $h(x) \in \mathbb{F}_\infty[x]$.

2. Continuing problem one, show that $\mathrm{Gal}(\mathbb{E}, \mathbb{F}) = \mathrm{Gal}(\mathbb{E}, \mathbb{F}_\infty)$. Conclude that the main theorem of Galois theory yields, for finite normal extensions, an anti-equivalence of between the lattice of subgroups of $\mathrm{Gal}(\mathbb{E}, \mathbb{F})$ and the subfields $\mathbb{F}_\infty \subseteq \mathbb{E}_0 \subseteq \mathbb{E}$.

3. Let $\mathbb{F}$ be a field of characteristic p and let $\mathbb{F} \subseteq \mathbb{E}$ be an algebraic extension. Let $\mathbb{F}_s$ be the set of elements in $\mathbb{E}$ which are the roots of separable polynomial.

i.) Prove that $\mathbb{F}_s$ is a field. As a hint, suppose $a, b \in \mathbb{F}_s$. What is the separable degree of $\mathbb{F}(a, b)$ over $\mathbb{F}$? What can you conclude about the separable degree of $\mathbb{F}(a + b)$?

ii.) Show that $\mathbb{F}_s \subseteq \mathbb{E}$ is purely inseparable. Hint: recall that we have shown that if a is algebraic over $\mathbb{F}$, then the minimal polynomial can be written (over the algebraic closure of $\mathbb{F}$) as $g(x^{p^n})$ for some separable polynomial. Show that $g(x)$ is a separable polynomial.

4. Display the Galois correspondence between subfields and subgroups for the splitting fields of the following polynomials over the rationals.

i.) $x^3 - 2$;
ii.) $(x^2 - 2)(x^2 - 3)$;
iii.) $x^6 - 1$;
iv.) $x^8 - 1$.

5. Let $\mathbb{F}$ be a field and G a finite group. If V is an $\mathbb{F}$-vector space, let $\mathrm{map}(G, V)$ be the set of set functions from G to V. (This is the product V^G.) The set $\mathrm{map}(G, V)$ is a vector space using addition and scalar multiplication in the target.

i.) If $g \in G$ and $\phi \in \mathrm{map}(G, V)$, define a new function $g\phi \in \mathrm{map}(G, V)$ by $g\phi(x) = \phi(xg)$. Prove that this is a left action and $\mathrm{map}(G, V)$ is a representation.

ii.) Define $\epsilon : \mathrm{map}(G, V) \to V$ by $\epsilon(\phi) = \phi(e)$. Show this map has the following universal property. Suppose W is any representation and $f : W \to V$ is $\mathbb{F}$-linear, then there is a morphism $g : W \to \mathrm{map}(G, V)$ of representations so that $\epsilon g = f$.

iii.) Show that there is an isomorphism of $\mathbb{F}[G] \to \mathrm{map}(G, \mathbb{F})$ but this map depends on choices.

6. (The Normal Basis Theorem. See Lang, p. 312.) Let $\mathbb{F} \subseteq \mathbb{E}$ be a finite Galois extension with Galois group G. Since G acts on $\mathbb{E}$ through $\mathbb{F}$-linear transformations $\mathbb{E}$ is representation of G over $\mathbb{F}$. The normal basis theorem, as usually phrased as $\mathbb{E} \cong \mathbb{F}[G]$, but there is no choice-free isomorphism. To get a canonical answer, it turns out to be easier to identity $\mathbb{E} \otimes_{\mathbb{F}} \mathbb{E}$.

i.) Regard $\mathbb{E}$ as an $\mathbb{F}$ vector space and consider the representation $\mathrm{map}(G, \mathbb{E})$ defined in the previous problem. Prove this an $\mathbb{E}$-algebra using multiplication in the target.

ii.) Define a G action on $\mathbb{E} \otimes_{\mathbb{F}} \mathbb{E}$ by $g(x \otimes y) = x \otimes gy$. Let $g : \mathbb{E} \otimes_{\mathbb{F}} \mathbb{E} \to \mathrm{map}(G, \mathbb{E})$ be the morphism of representations (5ii) so that $\epsilon g : \mathbb{E} \otimes_{\mathbb{F}} \mathbb{E} \to \mathbb{E}$ is multiplication. Show that this is an $\mathbb{E}$-algebra homomorphism that commutes with the G actions.

iii.) Show that is isomorphism. Conclude that $\mathbb{E} \otimes_{\mathbb{F}} \mathbb{E} \cong \mathbb{E}[G]$ as a representation.