MATH 470 Winter 2007

Graduate Algebra
Problem Set 2 Annex

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.

Outline of proof of part (iii): We'd like to use the proof of Artin's theorem. Define

$$f : \mathbb{E} \longrightarrow \mathrm{map}(G, \mathbb{E})$$

by $y \mapsto f(y) = f_y$ with $f_y(\sigma) = \sigma(y)$. This is an $\mathbb{F}$-linear homomorphism and we're trying to show that the induced map

$$\begin{gathered} \mathbb{E} \otimes_{\mathbb{F}} \mathbb{E} \longrightarrow \mathrm{map}(G, \mathbb{E}) \\ x \otimes y \mapsto x f(y) \end{gathered}$$

is an isomorphism. This can be deduced from the following statement: if $x_1, \ldots, x_n$ is a basis for $\mathbb{E}$ as an $\mathbb{F}$-vector space, then $f_{x_1}, \ldots, f_{x_n}$ is a basis for $\mathrm{map}(G, \mathbb{E})$ as an $\mathbb{E}$-vector space.

It is sufficient to prove linear independence; thus we prove the contrapositive: if the f_{x_i} are linearly dependent over $\mathbb{E}$, the x_i are linearly dependent over $\mathbb{F}$. To prove this assume we have an equation

$$c_1 f_{x_1} + \cdots + c_n f_{x_n} = 0. \tag{1}$$

If $G = \{e = \sigma_1, \ldots, \sigma_n\}$ enumerates the elements of G, evaluating (1) at σ_j

givens an array of equations

$$\begin{aligned} c_1 x_1 + \cdots\cdots + c_n x_n &= 0 \\ c_1 \sigma_2(x_1) + \cdots + c_n \sigma_2(x_n) &= 0 \\ \cdots \\ c_1 \sigma_n(x_1) + \cdots + c_n \sigma_n(x_n) &= 0 \end{aligned}$$

If we can choose some $c_i \neq 0$ we can proceed as in the proof of Artin's theorem to show that all c_i can be chosen in $\mathbb{F}$.