210B worksheet 10

Question 1. Given a simple algebraic extension $F(\alpha)/F$ with α having minimal polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_0$ over F. Prove that

$$tr_{F(\alpha)/F}(\alpha) = -a_{n-1} \quad \text{and} \quad N_{F(\alpha)/F}(\alpha) = (-1)^n a_0.$$

With respect to the basis $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$, the element α has matrix given by its companion matrix

$$C(\alpha) = \begin{pmatrix} 0 & 0 & & 0 & -a_0 \\ 1 & 0 & & 0 & -a_1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \vdots & & 0 & \vdots \\ & & & 1 & -a_{n-1} \end{pmatrix}$$

Hence $tr_{F(\alpha)/\alpha}(\alpha) = -a_{n-1}$, $N_{F(\alpha)/\alpha} = (-1)^n a_0$

Question 2. Let E/F be a finite extension and $\alpha \in E$. Assume that $[E : F(\alpha)] = r$. Prove that

$$tr_{E/F}(\alpha) = r\, tr_{F(\alpha)/F}(\alpha) \quad \text{and} \quad N_{E/F}(\alpha) = N_{F(\alpha)/F}(\alpha)^r.$$

Let $u_1, \ldots, u_r$ be a basis for E over $F(\alpha)$. Then $\{u_i \alpha^j\}$ $i = 0, \ldots, r$, $j = 0, \ldots, n-1$ is a basis for E/F for some n (E/F finite extension). Then the matrix corresponding to α as a F-linear transformation is

$$[\alpha] = \begin{pmatrix} C(\alpha) & & \\ & C(\alpha) & 0 \\ & & \end{pmatrix}$$

$$[\alpha] = \begin{pmatrix} C(\alpha) & & 0 \\ & C(\alpha) & \\ & \cup & \ddots \\ 0 & & C(\alpha) \end{pmatrix}$$

ie, the block diagonal with companion matrices along the diagonal.

Hence $Tr_{E/F}(\alpha) = r\,Tr_{F(\alpha)/F}(\alpha)$, $N_{E/F}(\alpha) = N_{F(\alpha)/F}(\alpha)^r$

Question 3. Suppose E/F is a finite Galois extension. Show that for $\alpha \in E$ we have that

$$N_{E/F}(\alpha) = \prod_{\sigma \in Gal(E/F)} \sigma(\alpha), \quad tr_{E/F}(\alpha) = \sum_{\sigma \in Gal(E/F)} \sigma(\alpha).$$

Let $G = Gal(E/F)$, and $H = Fix(F(\alpha)) \leq G$.

Since E/F is a finite Galois extension, we can finitely partition G into left cosets.

$G = \bigsqcup_{i=1}^{n} \tau_i H$ with $|H| = r$

So $\prod_{\sigma \in G} \sigma(a) = \prod_{i=1}^{n} \tau_i(a)^r = \left(\prod_{i=1}^{n} \tau_i(a)\right)^r$

Since Galois extension, $\tau_i(a)$ are all the roots of the minimal poly of α. Hence $\prod_{i=1}^{n} \tau_i(a) = -a_{n-1}$

where $m_\alpha(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$.

Hence by the previous two questions

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

Similar logic works for the trace.

Question 4. Suppose we have an irreducible polynomial $f \in \mathbb{Q}[X]$ of degree p, where p is prime. Assume that f has $p-2$ real roots and 2 nonreal, complex roots. What is that Galois group of f?

Let $G = Gal(E/\mathbb{Q})$ where E splitting field of f. We have $G \hookrightarrow S_p$ given by the action of of G on the roots of f in E.

The complex roots must be conjugate and so we have $\tau \in G$ which is a transposition.

Similarly, let α be a root of f. Then $[\mathbb{Q}(\alpha):\mathbb{Q}] = p$ is prime and so by Galois Theory, $p \mid |G|$.

Hence by cauchy's theorem, there exists an element $\sigma \in G$ s.t $|\sigma| = p$. Since a transposition τ and element of order p, σ generate S_p we have $G = S_p$. ∎

Question 5. (Fall '16) Let $f \in F[X]$ be an irreducible polynomial of prime degree over a field F, and let K/F be the splitting field of f. Prove there is an element in the Galois group of K/F permuting cyclically all the roots of f in K.

Note: I forgot to include the condition f is

Note: I forgot to include the condition f is seperable. Let $G = Gal(K/F)$

Let $\alpha \in K$ be a root of f. Then $|F(\alpha)/F| = p$ and by Galois Th. $p \mid |G|$ and so by cauchy there exists $\sigma \in G$ s.t $|\sigma| = p$.

Consider $g(x) = \prod_{\beta \in \langle\sigma\rangle \cdot \alpha} (x - \beta)$ where $\langle\sigma\rangle \cdot \alpha$ is the orbit of the root α under $\langle\sigma\rangle$.

Since $\tau g(x) = g(x)$ for all $\tau \in G$ we must have $g(x) \in F(x)$ and as $g(\alpha) = 0$. Hence $g \mid f \Rightarrow f = g$ and we conclude σ permutes the roots of f cyclically.

Question 6. (Spring '18) let $\alpha \in \mathbb{C}$ and suppose that $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is finite and coprime to $n!$ for some integer $n > 0$. Show that $\mathbb{Q}(\alpha^n) = \mathbb{Q}(\alpha)$.

We have a tower of extensions $\mathbb{Q}(\alpha)/\mathbb{Q}(\alpha^n)/\mathbb{Q}$ and so $[\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^n)]$ is coprime to $n!$.

Since $f(x) = x^n - \alpha^n \in \mathbb{Q}(\alpha^n)[x]$ is such that $f(\alpha) = 0$, it follow that $[\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^n)] \leq n$ and so $[\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^n)] = 1$ ∎