Math 505 HW5

Anonymous

February 12, 2024

Lemma 3.

By definition the Galois group is the group of automorphisms of K that fix k, so $\mathrm{Gal}(K/k) = \Sigma$ which shows the two above equalities.

Proposition 4.

(1) We need only show that $N_{K/k}(\alpha)$ is fixed by every element of the Galois group. Let $\tau \in \mathrm{Gal}(K/k)$, and notice that

$$\tau\left(\prod_{\sigma \in \mathrm{Gal}(K/k)} \sigma(\alpha)\right) = \prod_{\sigma \in \mathrm{Gal}(K/k)} (\tau \circ \sigma)(\alpha)$$

Since left multiplication by an element of a group is a permutation, it follows immediately that

$$\{\, \tau \circ \sigma \mid \sigma \in \mathrm{Gal}(K/k) \,\} = \tau \mathrm{Gal}(K/k) = \mathrm{Gal}(K/k)$$

Which shows that τ fixes $N_{k/k}(\alpha)$ for every $\tau \in \mathrm{Gal}(K/k)$, completing the proof.

(2) Notice that

$$\tau\left(\sum_{\sigma \in \mathrm{Gal}(K/k)} \sigma(\alpha)\right) = \sum_{\sigma \in \mathrm{Gal}(K/k)} (\tau \circ \sigma)(\alpha)$$

So for the same reasons as before $\mathrm{Tr}_{K/k}(\alpha) \in k$.

Proposition 5.

Notice that

$$N_{K/k}(\alpha\beta) = \prod_{\sigma\in\mathrm{Gal}(K/k)} \sigma(\alpha\beta) = \prod_{\sigma\in\mathrm{Gal}(K/k)} \sigma(\alpha)\sigma(\beta) = \prod_{\sigma\in\mathrm{Gal}(K/k)} \sigma(\alpha) \cdot \prod_{\sigma\in\mathrm{Gal}(K/k)} \sigma(\beta)$$
$$= N_{K/k}(\alpha) \cdot N_{K/k}(\beta)$$

Proposition 5.

Once again,

$$\mathrm{Tr}_{K/k}(\alpha+\beta) = \sum_{\sigma\in\mathrm{Gal}(K/k)} \sigma(\alpha+\beta) = \sum_{\sigma\in\mathrm{Gal}(K/k)} \sigma(\alpha)+\sigma(\beta) = \sum_{\sigma\in\mathrm{Gal}(K/k)} \sigma(\alpha) + \sum_{\sigma\in\mathrm{Gal}(K/k)} \sigma(\beta)$$
$$= \mathrm{Tr}_{K/k}(\alpha) + \mathrm{Tr}_{K/k}(\beta)$$

Example 7.

(1) Since the minimal polynomial of D is $x^2 - D$ which has degree 2, the Galois group has order 2. We claim that it is generated by the automorphism

$$\varphi : \sqrt{D} \mapsto -\sqrt{D}$$

Since $\sqrt{D} \notin k$, this map fixes k, and hence is an automorphism of k sending $\sqrt{D}$ to another root of $x^2 - D$. Clearly it has order 2, which shows that the Galois group is just $\langle\varphi\rangle$. Then

$$N_{k(\sqrt{D})/k} = (a + b\sqrt{D})\varphi\left(a + b\sqrt{D}\right) = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2$$

(2) Similarly,

$$\mathrm{Tr}_{k(\sqrt{D})/k} = a + b\sqrt{D} + \varphi\left(a + b\sqrt{D}\right) = a + b\sqrt{D} + a - b\sqrt{D} = 2a$$

Proposition 8.

(1) Let $\alpha_2, \ldots, \alpha_d$ be the other $d-1$ roots of f. We claim that for any α_i, there are precisely n/d $\sigma \in \mathrm{Gal}(K/k)$ such that $\sigma(\alpha) = \alpha_i$. This was actually shown on homework 2, because each $\sigma \in \mathrm{Gal}(K/k)$ sending α to α_i is just an extension of $\tau : k(\alpha) \to \bar{k}$ with

$\tau(\alpha) = \alpha_i$, and I showed on HW2 that

$$\left|\left\{ \begin{array}{l} \text{extensions of } \tau \text{ to} \\ \text{embeddings } E \hookrightarrow L' \end{array} \right\}\right| = \left|\left\{ \begin{array}{l} \text{extensions of } \sigma \text{ to} \\ \text{embeddings } E \hookrightarrow L \end{array} \right\}\right|$$

Where E/F is an extension and $\tau : F \to L'$ and also $\sigma : F \to L$ with L, L' (possibly distinct) algebraic closures of F. Taking $L = L' = \overline{k}$, $F = k(\alpha)$, $E = K$, $\sigma = \mathrm{id}_F$, and τ as above will show that the number of $\sigma \in \mathrm{Gal}(K/k)$ sending α to α_i are in bijection with the number of $\sigma \in \mathrm{Gal}(K/k)$ that send α to α, which is precisely the (separable) degree of $K/k(\alpha)$, which, by the following diagram,

$$\begin{tikzcd} K \arrow[d, dash, "n/d"] \arrow[dd, dash, bend right, "n"'] \\ k(\alpha) \arrow[d, dash, "d"] \\ k \end{tikzcd}$$

Is just n/d. Thus, in the product

$$N_{K/k}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(K/k)} \sigma(\alpha)$$

precisely n/d of the terms are α_i for each i. So, let $\beta = \prod_{i=1}^{d} \alpha_i$ (taking $\alpha_1 = \alpha$) and we get that

$$N_{K/k}(\alpha) = \beta^{n/d}$$

By the formulas for symmetric polynomials, the product of the roots β is precisely $(-1)^n a_0$. If n is odd, then n^2/d is odd, so $(-1)^n = (-1)^{n^2/d}$. Similarly, if n is even then $(-1)^n = (-1)^{n^2/d}$. We have concluded that

$$N_{K/k}(\alpha) = \beta^{n/d} = (-1)^{n \cdot n/d} a_0^{n/d} = (-1)^n a_0^{n/d}$$

(2) Once again, precisely n/d of the terms of

$$\mathrm{Tr}_{K/k}(\alpha) = \sum_{\sigma \in \mathrm{Gal}(K/k)} \sigma(\alpha)$$

are α_i for each i. Thus,

$$\mathrm{Tr}_{K/k}(\alpha) = \frac{n}{d}\sum_{i=1}^{d}\alpha_i$$

Once again by the explicit formulas for symmetric polynomials, the sum of the roots is just $-a_{d-1}$, whence,

$$\mathrm{Tr}_{K/k}(\alpha) = -\frac{n}{d}a_{d-1}$$

Proposition 9

(1) Since $a \in k$, for any $\sigma \in \mathrm{Gal}(K/k)$ $\sigma(a) = a$. Thus,

$$N(a\alpha) = \prod_{\sigma\in\mathrm{Gal}(K/k)}\sigma(a\alpha) = \prod_{\sigma\in\mathrm{Gal}(K/k)} a\sigma(\alpha) = a^n \prod_{\sigma\in\mathrm{Gal}(K/k)}\sigma(\alpha) = a^n N_{K/k}(\alpha)$$

(2) Similarly,

$$\mathrm{Tr}_{K/k}(a\alpha) = \sum_{\sigma\in\mathrm{Gal}(K/k)}\sigma(a\alpha) = \sum_{\sigma\in\mathrm{Gal}(K/k)} a\sigma(\alpha) = a\sum_{\sigma\in\mathrm{Gal}(K/k)}\sigma(\alpha) = a\,\mathrm{Tr}_{K/k}(\alpha)$$

Theorem 10.

Let $0 \neq \beta \in K$, and write $\alpha = \frac{\beta}{\sigma(\beta)}$. Note that $N_{K/k}(1) = \prod_{\sigma\in\mathrm{Gal}(K/k)}\sigma(1) = 1^n = 1$. This shows that $N_{K/k}(a/b) = N_{K/k}(a)/N_{K/k}(b)$. We showed in Proposition 4 that $\sigma(N_{K/k}(\alpha)) = N_{K/k}(\alpha)$ for each σ. Similarly, since $\mathrm{Gal}(K/k)\tau = \mathrm{Gal}(K/k)$, we also have that $N_{K/k}(\tau(\alpha)) = N_{K/k}(\alpha)$ for each $\tau \in \mathrm{Gal}(K/k)$. Equivalently, since right multiplication by an element of a group is a permutation of that group, $\{\, \sigma\circ\tau \mid \sigma \in \mathrm{Gal}(K/k)\,\} = \mathrm{Gal}(K/k)$. Thus immediately from the definition,

$$N_{K/k}(\tau(\alpha)) = \prod_{\sigma\in\mathrm{Gal}(K/k)}\sigma\circ\tau(\alpha) = N_{K/k}(\tau)$$

Thus,

$$N_{K/k}\left(\frac{\beta}{\sigma(\beta)}\right) = \frac{N_{K/k}(\beta)}{N_{K/k}(\beta)} = 1$$

We provide a different proof of the case $n = 2$. Let $K = k(\sqrt{D})$ with $\sqrt{D}$ a solution to (by hypothesis, the irreducible) $X^2 - D = 0$. The only nontrivial automorphism in the Galois group is $\sigma : x + y\sqrt{D} \mapsto x - y\sqrt{D}$. Thus, for α of norm 1, we want to find a solution to

$$\alpha(x - y\sqrt{D}) = x + y\sqrt{D}$$
$$(\alpha - 1)x = y\sqrt{D}(\alpha + 1)$$

Notice that

$$\sigma\left(\frac{\sqrt{D}(\alpha+1)}{\alpha-1}\right) = \frac{-\sqrt{D}(\alpha^{-1}+1)}{\alpha^{-1}-1} = \frac{-\sqrt{D}(1+\alpha)}{1-\alpha}$$

Since α has norm 1 we have that $\alpha\sigma(\alpha) = 1$, thus $\sigma(\alpha) = \alpha^{-1}$ (I am a little confused by your question... α is an element of a field so it has an inverse). Thus the coefficient of y is fixed by every element of the Galois group and hence this is an equation in two variables in k, thus the kernel of its corresponding linear transformation has dimension at least 1, so there is a (necessarily nonzero) solution.

In the general case we use linear independence of characters. Recall that $\sigma^{(i)}(x) = (\underbrace{\sigma \circ \cdots \circ \sigma}_{i \text{ times}})(x)$. Notice that $\sigma\big|_{K^\times} : K^\times \to K^\times$ is a homomorphism of groups, and hence a character of $K^\times$. Notice also that

$$\mathcal{S} = \left\{ \sigma^{(0)} = \mathrm{id}, \sigma, \sigma^{(2)}, \ldots, \sigma^{(n-1)} \right\}$$

is a set of distinct characters since σ has order n. Thus there is a $\gamma \in K$ so that

$$\beta = \alpha\sigma^{(0)}(\gamma) + \alpha\sigma(\alpha)\sigma^{(1)}(\gamma) + \cdots + \underbrace{\left(\prod_{i=0}^{n-1} \sigma^{(i)}(\alpha)\right)}_{1}\sigma^{(n-1)}(\gamma) \neq 0$$

since $\mathcal{S}$ is linearly independent by linear independence of characters. We see that,

$$\frac{\beta}{\sigma(\beta)} = \frac{\alpha\sigma^{(0)}(\gamma) + \alpha\sigma(\alpha)\sigma^{(1)}(\gamma) + \cdots + \sigma^{(n-1)}(\gamma)}{\sigma(\alpha)\sigma^{(1)}(\gamma) + \sigma(\alpha)\sigma^{(2)}(\alpha)\sigma^{(2)}(\gamma) + \cdots + \prod_{i=1}^{n-1}\sigma^{(i)}(\alpha)\sigma^{(n-1)}(\gamma) + \sigma^{(0)}(\gamma)}$$

Where the coefficient of the last term is 1 precisely because $N(\alpha) = 1$. After moving the last term on the bottom to the beginning, and multiplying by α/α, we can see that this quantity is going to equal α, which completes the proof.