Trace and Norm

Let K be a normal finite-dimensional extension of F, with Galois group given by $\sigma_1, \ldots, \sigma_n$. For any $a \in K$, we define the trace and norm of a:

$$T(a) = \sigma_1(a) + \cdots + \sigma_n(a),$$

$$N(a) = \sigma_1(a) \ldots \sigma_n(a).$$

Clearly $T(a)$ and $N(a)$ both lie in F since they are fixed under all automorphisms of K/F and K/F is normal. Trace is additive and norm multiplicative:

$$T(a+b) = T(a) + T(b), \quad N(ab) = N(a)N(b).$$

For $a \in F$, $T(a) = na$ and $N(a) = a^n$.

Theorem. *Any distinct automorphisms of a field F are linearly independent.*

Remark. Linear independence of $\sigma_1, \ldots, \sigma_n$ over F means that if $a_1\sigma_1 + \cdots + a_n\sigma_n$ is identical to the zero homomorphism on F for some $a_1, \ldots, a_n \in F$, then all the a_i's must be zero.

proof of the theorem. Suppose on the contrary that $\sigma_1, \ldots, \sigma_n$ are linearly dependent over F. Among all dependence relations, pick one with as many zeroes as possible. Say this "shortest" relation is $a_1\sigma_1 + \ldots + a_r\sigma_r = 0$. Of course, we must have $r > 1$. Since σ_1 and σ_2 are distinct, there exists $b \in F$ with $\sigma_1(b) \neq \sigma_2(b)$. Then we have the following two equations:

$$a_1\sigma_1(x)\sigma_1(b) + a_2\sigma_2(x)\sigma_2(b) + \cdots + a_r\sigma_r(x)\sigma_r(b) = 0$$

and

$$a_1\sigma_1(x)\sigma_1(b) + a_2\sigma_2(x)\sigma_1(b) + \cdots + a_r\sigma_r(x)\sigma_1(b) = 0.$$

Subtracting, we get

$$a_2\sigma_2(x)\big(\sigma_1(b) - \sigma_2(b)\big) + \cdots + a_r\sigma_r(x)\big(\sigma_1(b) - \sigma_r(b)\big) = 0.$$

This is a shorter dependence relation, non-trivial since the coefficient of $\sigma_2(x)$ is not zero.

Lemma. *Let K be a normal and finite-dimensional extension over F. Then the trace mapping $T : K \longrightarrow F$, $a \longmapsto T(a)$ is a surjection.*

proof. *Left to the student!*

Exercise. Prove the above lemma.

Theorem. Let K be a normal extension over F with a Galois group which is cyclic of order n generated, say, by σ. Then an element $a \in K$ has trace 0 if and only if it is of the form $b - \sigma(b)$ for some $b \in K$.

proof. If $a = b - \sigma(b)$ for some $b \in K$, then

$$\begin{aligned} T(a) &= (1 + \sigma + \sigma^2 + \cdots + \sigma^{n-1})(a) \\ &= (b - \sigma(b)) + (\sigma(b) - \sigma^2(b)) + \cdots + (\sigma^{n-1}(b) - \underbrace{\sigma^n(b)}_{b}) \\ &= 0. \end{aligned}$$

Conversely, assume $T(a) = 0$. By above lemma, there exists $c \in F$ with $T(c) = 1$. Define $d_0 = ac$, $d_1 = (a + \sigma(a))\sigma(c)$, and in general

$$d_i = (a + \sigma(a) + \cdots + \sigma^i(a))\sigma^i(c)$$

for $0 \le i \le n-2$. Set $b = d_0 + d_1 + \cdots + d_{n-2}$. Since $\sigma(d_i) = (\sigma(a) + \sigma^2(a) + \cdots + \sigma^{i+1}(a))\sigma^{i+1}(c)$, we find $d_{i+1} - \sigma(d_i) = a\sigma^{i+1}(c)$ for $0 \le i \le n-3$. Also, $\sigma(d_{n-2}) = -a\sigma^{n-1}(c)$ since $T(a) = 0$. Hence

$$\begin{aligned} b - \sigma(b) &= d_0 + (d_1 - \sigma(d_0)) + (d_2 - \sigma(d_1)) + \cdots + (d_{n-2} - \sigma(d_{n-3})) - \sigma(d_{n-2}) \\ &= ac + a\sigma(c) + \cdots + a\sigma^{n-1}(c) \\ &= a \end{aligned}$$

since $T(c) = 1$.

Theorem. Let K be normal over F, where $[K:F]$ is a prime p which is also the characteristic of K. Then $K = F(u)$ where u is a root of an irreducible polynomial over F of the form $x^p - x - a$.

proof. The Galois group of K/F is cyclic of order p, say generated by σ. The element $T(1) = 0$ (since the characteristic of K, and hence of F, is p). Thus we can write $1 = \sigma(u) - u$ for some $u \in K$. We have $\sigma(u) = 1+u$, hence $\sigma(u^p) = (1+u)^p = 1+u^p$. It follows that $a = u^p - u$ is invariant under σ and hence lies in F. Since there are no fields properly between F and K, and u is not in F, we have $K = F(u)$. It follows that $x^p - x - a$ must be the minimal polynomial for u.

Theorem. (Hilbert) Let K be normal over F with a cyclic Galois group generated, say by σ. Then an element $a \in K$ has norm 1 if and only if it has the form $a = b/\sigma(b)$ for some $0 \neq b \in K$.

proof. If $a = b/\sigma(b)$, then

$$N(a) = a\sigma(a)\dots\sigma^{n-1}(a) = \frac{b}{\sigma(b)}\,\frac{\sigma(b)}{\sigma^2(b)}\cdots\frac{\sigma^{n-1}(b)}{\sigma^n(b)} = 1$$

since $\sigma^n = 1$.

Suppose conversely that $N(a) = 1$. Write $d_0 = ac$, $d_1 = a\sigma(a)\sigma(c)$ and in general

$$d_i = a\sigma(a)\dots\sigma^i(a)\sigma^i(c)$$

for $0 \leq i \leq n-1$. Note that $d_{n-1} = \sigma^{n-1}(c)$ since $N(a) = 1$. Note also that $d_{i+1} = a\sigma(d_i)$ for $0 < i \leq n-2$. Since $1, \sigma, \dots, \sigma^{n-1}$ are linearly independent, there must be a choice for $c \in K$ such that the sum $b = d_0 + d_1 + \cdots + d_{n-1}$

is not zero. Then

$$\sigma(b) = \sigma(d_0) + \sigma(d_1) + \cdots + \sigma(d_{n-1})$$
$$= \frac{1}{a}(d_1 + d_2 + \cdots + d_{n-1}) + c = \frac{d_0 + d_1 + \cdots + d_{n-1}}{a}$$
$$= \frac{b}{a}$$

since $\sigma^n = 1$ and $c = d_0/a$.

Theorem. Let K be normal over F with a Galois group which is cyclic of order n, say generated by σ. Assume that the characteristic is prime to n and that $x^n - 1$ factors completely in F. Then $K = F(u)$ where u is a root of an irreducible polynomial over F of the form $x^n - a$.

proof. There n distinct roots of $x^n - 1$ in F and they form a multiplicative group. Any finite multiplicative group in a field is cyclic. (why?) Let a generator be ε. We have $N(\varepsilon) = \varepsilon^n = 1$. By the above theorem, we can write $\varepsilon = \sigma(u)/u$ for a suitable $u \in K$. Then $\sigma(u) = \varepsilon u$, $\sigma(u^n) = \varepsilon^n u^n = u^n$. Hence $a = u^n$ is invariant under σ and lies in F. If n is prime, then we are done. Assume n is composite. Since $u, \sigma(u) = \varepsilon u, \sigma^2(u) = \varepsilon^2 u, \ldots, \sigma^{n-1}(u) = \varepsilon^{n-1} u$ form the set of all roots of $x^n - a$, $F(u)$ is a splitting field of $x^n - a$ over F and the automorphisms $1, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ send u into distinct elements in $F(u)$. This shows that $F(u)$

admits n automorphisms over F and $[F(u):F] \geq n$, whence $K = F(u)$. It follows that $x^n - a$ must be the minimal polynomial for u over F.

Exercise. Prove that any finite multiplicative group in a field is cyclic!