The trace and the norm.

We start with a reminder of some results from the Linear algebra. Let K be a field. For any $n > 0$ we denote by $GL_n(K)$ the group of invertible $n \times n$ matrices and by $M_n(K)$ the ring of $n \times n$ matrices. In particular $GL_1(K)$ is equal to the multiplicative group $K^* := K - \{0\}$.

Claim 9.1. a) There exists a group homomorphism $Det : GL_n(K) \to K^*$ such that in the case when $A \in GL_n(K)$ is an upper or lower diagonal matrix $Det(A)$ is equal to the product of diagonal elements of A,

Let V be a finite-dimensional K-vector space and $A : V \to V$ a linear operator. Given a basis $\mathcal{B} = \{e_1, ..., e_n\}$ in V we denote by $A_{\mathcal{B}}$ the $n \times n$ matrix $A_{\mathcal{B}} := (t_{ij}), 1 \leq i, j \leq n$ such that

$$A(e_j) = \sum_{1 \leq i \leq n} t_{ij} e_i$$

b) The determinant $Det(A_{\mathcal{B}})$ does not depend on a choice of a basis $\mathcal{B}$. We denote it by $Det(A)$,

c) The trace $Tr(A_{\mathcal{B}})$ does not depend on a choice of a basis $\mathcal{B}$. We denote it by $Tr(A)$,

d) for any pair $A, B : V \to V$ of linear operators we have

$$Tr(A + B) = Tr(A) + Tr(B), Det(AB) = Det(A)Tr(B)$$

Definition 9.1. Let $L \supset K$ be a finite extension. We can consider L as a finite-dimensional K-vector space.

a) To any $\alpha \in L$ we associate a K-linear operator $A_\alpha : L \to L$ given by

$$A_\alpha(\beta) := \alpha\beta, \beta \in L$$

b) we define a map $N_{L/K} : L \to K$ by $N_{L/K}(\alpha) := Det(A_\alpha)$,

c) we define a map $Tr_{L/K} : L \to K$ by $Tr_{L/K}(\alpha) := Tr(A_\alpha)$.

Remark a) Since the trace map is linear we have $Tr_{L/K}(\alpha + \beta) = Tr_{L/K}(\alpha) + Tr_{L/K}(\beta)$,

b) Since the determinant map is a group homomorphism we have $N_{L/K}(\alpha\beta) = N_{L/K}(\alpha)N_{L/K}(\beta)$,

c) it follows from the definition that for any $\alpha \in K$ we have $Tr(\alpha) = [L : K]\alpha, N_{L/K}(\alpha) = \alpha^{[L:K]}$.

Lemma 9.1. Let $L \supset K$ be a finite extension, $\alpha \in L$ be such that $L = K(\alpha)$ and $p(t) = Irr(\alpha, K, t)$. Consider a decomposition

$$p(t) = \prod_{i=1}^{s} (t - \alpha_i)^{m_i}, \alpha_j \in \bar{K}$$

of $p(t)$ in the product of linear factors. Then

a) $Tr_{L/K}(\alpha) = \sum_{1 \leq i \leq s} m_j \alpha_j$,

b) $N_{L/K}(\alpha) = \prod_{1 \leq j \leq s} \alpha_j^{m_j}$.

Proof. Let us choose a basis $\mathcal{B} = \{e_i\}, 0 \leq i < n$ in $L = K(\alpha)$ where $e_i := \alpha^i, 0 \leq i < n$. Then $A^L_\alpha(e_i) = e_{i+1}$ if $, 0 \leq i < n-1$ and $A^L_\alpha(e_{n-1}) = \alpha^n = -\sum_{i=0}^{n-1} c_i \alpha^i$. So we have $\mathrm{Det}(A^L_\alpha) = (-1)^n c_0$ and $\mathrm{Tr}(A^L_\alpha) = -c_{n-1}$. But it is clear from the formula

$$p(t) = \prod_{i=1}^{s} (t - \alpha_i)^{m_i}, \alpha_j \in \bar{K}$$

that

$(-1)^n c_0 = (-1)^n \prod_{1 \leq j \leq s} \alpha_j^{m_j}$ and

$-c_{n-1} = -\sum_{1 \leq i \leq s} m_j \alpha_j$.$\square$

Theorem 9.1. Let K be a field, p an odd prime number, $a \in K - K^p$. Then for any $n > 0$ the polynomial $t^{p^n} - a \in K[t]$ is irreducible.

In the proof of the theorem we will use the following easy result. Please prove it yourself.

Lemma 9.2. Let K be a field, $p(t) \in K[t]$ a polynomial of positive degree, $\bar{K} \supset K$ be an algebraic closure of $K, \alpha \in \bar{K}$ an element such that $p(\alpha) = 0$. The polynomial $p(t) \in K[t]$ is irreducible iff $[K(\alpha) : K]$=deg$(p(t))$.

Proof of Theorem 9.1. In the case when $\mathrm{ch}(K) = p, n = 1$ the result follows from Lemma 3.5. The result for $\mathrm{ch}(K) = p, n > 1$ can be proven by exactly the same arguments. So we can assume that $\mathrm{ch}(K) \neq p$. We first consider the case when $n = 1$.

Let $\bar{K} \supset K$ be an algebraic closure of $K, \alpha \in \bar{K}$ an element such that $\alpha^p = a$. It is sufficient to show that $[K(\alpha) : K] = \deg(t^p - a)$. We show that the assumption $[K(\alpha) : K] < p$ leads to a contradiction.

So suppose that $d := [K(\alpha) : K] < p$. Let $b := N_{K(\alpha)/K}(\alpha) \in K$. Since $\alpha^p = a$ we have $b^p = N_{K(\alpha)/K}(a) = a^d$. Since d, p are relatively prime there exists $m, n \in \mathbb{Z}$ such that $md + np = 1$. Then we have

$$a = a^{md+np} = (a^d)^m (a^n)^p = (b^m)(a^n)^p \in K^p$$

This contradicts the assumption that $a \in K - K^p$.

Now we prove the theorem by induction in n. Suppose it is known for polynomials of the form $t^{p^{n-1}} - b$ for all the fields $L, b \in L - L^p$.

As before let $\bar{K} \supset K$ be an algebraic closure of $K, \alpha \in \bar{K}$ an element such that $\alpha^p = a$. We know that $[K(\alpha) : K] = p$. As follows from Lemma 9.1 we have $N_{K(\alpha)/K}(\alpha) = (-1)^{p-1}a = a$

I claim that there is no $\beta \in K(\alpha)$ such that $\alpha = \beta^p$. Really if $\alpha = \beta^p$ then $N_{K(\alpha)/K}(\alpha) = c^p, c \in K$ where $c := N_{K(\alpha)/K}(\beta)$. So $a = c^p$. But we assumed that $a \in K - K^p$.

Now we can finish the proof of the Theorem 9.1. Let $\gamma \in \bar{K}$ be a solution of the equation $\gamma^{p^{n-1}} = \alpha$. Since α is not a p-th power in $K(\alpha)$ we know [by the inductive assumption] that $[K(\gamma) : K(\alpha)] = p^{n-1}$. Therefore $[K(\gamma) : K] = p^n$.$\square$

Remark. One can show that a polynomial $t^{2^n} - a \in K[t], n > 1$ is irreducible iff $a \notin K^2$ and $a \notin -4K^4$.

The condition $a \notin -4K^4$ is necessary. Really for any $a = -4b^4, b \in K$ we have $t^4 - a = t^4 + 4b^4 = (t^2 + 2bt + 2b^2)(t^2 - 2bt + 2b^2)$

Corollary. Let K be a field, n an odd number, $a \in K$ such that $a \notin K^r$ for any divisor r of $n, r > 1$. Then $t^n - a$ is irreducible in $K[t]$.

Proof. Let's write n as a product of powers of prime numbers $n = \prod_{i=1}^{s} p_i^{r_i}$. Choose $\beta \in \bar{K}$ such that $\beta^n = a$. We have to show that $[K(\beta) : K] = n$.

We define $\alpha_i \in \bar{K}$ by $\alpha_i := \beta^{n/p_i^{r_i}}$. It is clear that $\alpha_i^{r_i} = a$. Therefore it follows from Theorem 9.1 that $[K(\alpha_i) : K] = p_i^{r_i}$. Since $K(\alpha_i) \subset K(\beta), 1 \leq i \leq s$ we see that $K(\beta)$ contains the composite field $K(\alpha_1)K(\alpha_2)...K(\alpha_s)$. Since the degrees $[K(\alpha_i) : K]$ are relatively prime we see that

$$[K(\alpha_1)K(\alpha_2)...K(\alpha_s) : K] = \prod_{i=1}^{s}[K(\alpha_i) : K] = n. \quad \square$$

Lemma 9.2 Let K be a field, $\mathrm{ch}(K) \neq 2$ and $a \in K - K^2$ such that $a \in L^2$ for non-trivial finite extension $L \supset K$. Then for any finite normal extension $M \supset K$ the group $Gal(M/K)$ is cyclic of order 2^r.

Example. $K = \mathbb{R}$.

Proof. If $M \neq K$ that by the assumption we can find $\alpha \in M$ such that $a = \alpha^2$. Let $G := Gal(M/K), G' := Gal(M/K(\alpha))$. Then $G/G' = Gal(/K(\alpha)/K) = \mathbb{Z}/2\mathbb{Z}$.

I claim that any element $g \in G - G'$ generates G. Really choose $g \in G - G'$ and denote by $H \subset G$ the subgroup generated by g. We want to show that $H = G$. By the Main theorem of Galois it is sufficient to check that $M^H = K$. Since $g(\alpha) = -\alpha$ we see that $\alpha \notin M^H$. But then it follows from our assumption that $M^H = K$. So we see that the group $Gal(M/K)$ is cyclic.

It is easy to see that for any cyclic group G of order $n \neq 2^r$ one can find $g \in G - G'$ which does not generate G where $G' \subset G$ is the unique subgroup of G of index 2.$\square$