Math 114 Homework 4

Michael Knopf

February 26, 2014

Note: When an extension K/F is Galois, its automorphism group $\operatorname{Aut} K/F$ is called the *Galois group* of K/F and is denoted $\operatorname{Gal} K/F$. The *Galois group* of a separable polynomial $p(X)$ over a field F is defined to be the Galois group of any splitting field of $p(X)$ over F. (See pp. 562-563 of DF.)

1. (Exercise 1 in DF §14.1.) Let K/F be a finite extension.

   (a) Show that if the field K is generated over F by the elements $\alpha_1, \ldots, \alpha_n \in K$, then an automorphism σ of K fixing F is uniquely determined by $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$. (That is, the values $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$ determine the value of $\sigma(\alpha)$ for every $\alpha \in K$.)

   In particular, show that an automorphism of K fixes K if and only if it fixes a set of generators for K over F.

   Proof. Suppose $\sigma \in \operatorname{Aut}(K/F)$. Since K/F is a finite extension, it is algebraic. Thus, for each i, α_i has some finite degree k_i, and a basis for K over F is $\{\alpha_1, \alpha_1^2, \ldots, \alpha_1^{k_1}, \ldots, \alpha_n, \alpha_n^2 \ldots, \alpha_n^{k_n}\}$.

   Let $\alpha \in K$. Then there exist constants $a_{11}, a_{12}, \ldots, a_{1k_1}, \ldots, a_{n1}, a_{n2}, \ldots, a_{nn_k}$ such that $\alpha = a_{11}\alpha_1 + a_{12}\alpha_1^2 + \cdots + a_{1k_1}\alpha_1^{k_1} + \cdots + a_{n1}\alpha_n + a_{n2}\alpha_n^2 + \cdots + a_{nk_n}\alpha^{k_n}$. Therefore, since σ is an automorphism fixing K, we must have

$$\begin{aligned}\sigma(\alpha) &= \sigma(a_{11}\alpha_1 + a_{12}\alpha_1^2 + \cdots + a_{1k_1}\alpha_1^{k_1} + \cdots + a_{n1}\alpha_n + a_{n2}\alpha_n^2 + \cdots + a_{nk_n}\alpha^{k_n}) \\ &= a_{11}\sigma(\alpha_1) + a_{12}\sigma(\alpha_1)^2 + \cdots + a_{1k_1}\sigma(\alpha_1)^{k_1} + \cdots + a_{n1}\sigma(\alpha_n) + a_{n2}\sigma(\alpha_n)^2 + \cdots + a_{nk_n}\sigma(\alpha)^{k_n}.\end{aligned}$$

   So σ is completely determined by its action on $\alpha_1, \ldots, \alpha_n$. If σ fixes $\alpha_1, \ldots, \alpha_n$, then $\sigma(\alpha) = \alpha$ for this arbitrary α, thus σ fixes K. Clearly, if σ does not fix some α_i then it does not fix K.

   □

   (b) Let $G \leq \operatorname{Gal}(K/F)$ be a subgroup of the Galois group of the extension K/F and suppose $\sigma_1, \ldots, \sigma_k$ are generators for G (i.e., $G = \langle \sigma_1, \ldots, \sigma_k \rangle$). Show that if E is an intermediate subfield ($F \subset E \subset K$), then E is fixed by G if and only if it is fixed by the generators $\sigma_1, \ldots, \sigma_k$.

   Proof. Clearly, if some σ_i does not fix E then G does not fix E, since $\sigma_i \in G$. Now, suppose σ_i fixes E for all i, and let $\sigma \in G$. Then $\sigma = \sigma_1^{n_1} \circ \cdots \circ \sigma_k^{n_k}$ for some $n_1, \ldots, n_k$. Then for any $\alpha \in E$, we have

$$\begin{aligned}\sigma(\alpha) = \sigma_1^{n_1} \circ \cdots \circ \sigma_k^{n_k}(\alpha) &= \sigma_1^{n_1} \circ \cdots \circ \sigma_{k-1}^{n_{k-1}}(\sigma_n^{n_k}(\alpha)) \\ &= \sigma_1^{n_1} \circ \cdots \circ \sigma_{k-1}^{n_{k-1}}(\mathrm{id}(\alpha)) = \sigma_1^{n_1} \circ \cdots \circ \sigma_{k-1}^{n_{k-1}}(\alpha) \\ &= \cdots = \sigma_1^{n_1}(\alpha) = \alpha.\end{aligned}$$

   So an arbitrary $\sigma \in G$ fixes an arbitrary $\alpha \in E$, thus G fixes E. □

2. (Exercise 3 in DF §14.2.) Determine the Galois group of the polynomial $(X^2-2)(X^2-3)(X^2-5)$ over $\mathbf{Q}$. Let K be a splitting field for this polynomial over $\mathbf{Q}$; determine all the subfields of K. (You may use the Galois correspondence, Theorem 14, although we haven't proved it in class yet.)

   Proof. Let $p(x) = (x^2-2)(x^2-3)(x^2-5)$. The splitting field K for $p(x)$ over $\mathbb{Q}$ is $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. A basis for K as a vector space over $\mathbb{Q}$ is $\{1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{10}, \sqrt{15}, \sqrt{30}\}$, therefore $[K : \mathbb{Q}] = 8$. Therefore, $\operatorname{Gal}(K/F) = <\sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto -\sqrt{3}, \sqrt{5} \mapsto -\sqrt{5}>$, because this group has order 8 and we know that the maps generated by these are the only possible automorphisms of K fixing $\mathbb{Q}$, since these are the only automorphisms that permute the roots of the irreducible polynomials x^2-2, x^2-3, and x^2-5. The lattice of subfields of K is drawn below.

   □

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[d, dash] \arrow[dr, dash] & \mathbb{Q}(\sqrt{2}\sqrt{5}) \arrow[dl, dash] \arrow[dr, dash] & \mathbb{Q}(\sqrt{3}, \sqrt{5}) \arrow[dl, dash] \arrow[d, dash] \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{3}) \arrow[d, dash] & \mathbb{Q}(\sqrt{5}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

3. (Exercise 4 in DF §14.2.) Let p be a prime. Determine the Galois group of $X^p - 2$ over $\mathbf{Q}$. (Hint: the example on p. 541 in §13.4 discusses the splitting field of this polynomial. The example on pp. 577-579 in §14.2 may be useful as a model.)

Proof. The splitting field for $x^p - 2$ over $\mathbb{Q}$ is $K = \mathbb{Q}(\zeta_p, \sqrt[p]{2})$, which has already been shown in the example on page 541. This extension has degree $p(p-1)$.

Since $\mathbb{Q}(\zeta_p)$ is the splitting field for the separable polynomial $x^{p-1} + x^{p-2} + \cdots + x + 1$ over $\mathbb{Q}$, we know that it is Galois. It is an extension of order $p - 1$, since this polynomial is irreducible, thus its Galois group H has order $p - 1$. There are only $p - 1$ automorphisms of this field that fix $\mathbb{Q}$, which are $\zeta_p \mapsto (\zeta_p)^k$ for $0 < k < p$. Thus $H = \{\zeta_p \mapsto (\zeta_p)^k : 0 \leq k < p - 1\}$. Since H is a subgroup of $G = \mathrm{Gal}(K/F)$, all of these automorphisms must be in G.

By Theorem 14, we know that K is Galois over $\mathbb{Q}(\zeta_p)$. Since $[K : \mathbb{Q}(\zeta_p)] = p$, $\mathrm{Gal}(K/\mathbb{Q}(\zeta_p))$ has order p. The only possible automorphisms of K fixing $\mathbb{Q}$ are those which permute the roots of $x^p - 2$. However, any element of $\mathrm{Gal}(K/\mathbb{Q}(\zeta_p))$ must also fix the pth roots of unity. So $\mathrm{Gal}(K/\mathbb{Q}(\zeta_p)) \subseteq \{\sqrt[p]{2} \mapsto (\sqrt[p]{2})^k : 0 \leq k < p\}$. However, this set (which is a cyclic group of order p) has the same number of elements as $\mathrm{Gal}(K/\mathbb{Q}(\zeta_p))$, thus this is the full group.

Thus, $\mathrm{Gal}(K/\mathbb{Q})$ contains both $\{\zeta_p \mapsto (\zeta_p)^k : 0 \leq k < p-1\}$ and $\{\sqrt[p]{2} \mapsto (\sqrt[p]{2})^k : 0 \leq k < p\}$. But the group generated by these two sets has order $p(p-1)$. It is the group of automorphisms $\sigma_{ij} : K \to K$ defined by

$$\zeta_p \mapsto (\zeta_p)^j$$
$$\sqrt[p]{2} \mapsto (\sqrt[p]{2})^k$$

for $0 \leq j < p - 1$ and $0 \leq k < p$, since a map of the form $\zeta_p \mapsto (\zeta_p)^j$ fixes any element that one of the form $\sqrt[p]{2} \mapsto (\sqrt[p]{2})^k$ does not, thus their composition must be of the form given above. So the full Galois group is $\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_{ij} : 0 \leq j < p - 1, 0 \leq k < p\}$.

$$\begin{tikzcd}
 & \mathbb{Q}(\zeta_p, \sqrt[p]{2}) \arrow[dl, dash, "p"'] \arrow[dr, dash, "p-1"] & \\
\mathbb{Q}(\zeta_p) \arrow[dr, dash, "p-1"'] & & \mathbb{Q}(\sqrt[p]{2}) \arrow[dl, dash, "p"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

$\square$

4. (Exercise 9 in DF §14.2.) Give (with proof) an example of fields F_1, F_2, F_3 with $F_0 := \mathbf{Q} \subset F_1 \subset F_2 \subset F_3$, such that $[F_3 : \mathbf{Q}] = 8$, $F_2/\mathbf{Q}$ is not Galois, but F_i/F_j is Galois for every $i > j$ other than $(i, j) = (2, 0)$.

Proof. Let $F_1 = \mathbb{Q}(\sqrt{2}), F_2 = \mathbb{Q}(\sqrt[4]{2}), F_3 = \mathbb{Q}(\sqrt[4]{2}, i)$. Then clearly $\mathbb{Q} \subset F_1 \subset F_2 \subset F_3$. Also, $F_2 \cong \mathbb{Q}/(x^4-2)$, which has degree 4 over $\mathbb{Q}$ because $x^4 - 2$ is irreducible over $\mathbb{Q}$, and $F_3 = F_2(i) \cong F_2/(x^2+1)$, which has degree 2 over F_2 because $x^2 + 1$ is irreducible over F_2. Thus $[F_3 : \mathbb{Q}] = [F_3 : F_2][F_2 : \mathbb{Q}] = 2 \cdot 4 = 8$.

F_1 is the splitting field for the polynomial $x^2 - 2$ over $\mathbb{Q}$. F_2 is the splitting field for the polynomial $x^2 - \sqrt{2}$ over F_1. F_3 is the splitting field for the polynomial $x^4 - 2$ over $\mathbb{Q}$, F_1, and F_2. Thus, F_i/F_j is Galois for every $i > j$ other than $(i, j) = (2, 0)$.

However, $F_2/\mathbb{Q}$ is not Galois. Since F_2 contains a root of the irreducible polynomial $x^4 - 2$, if it were Galois then it would contain all the roots. However, it does not contain the root $i\sqrt[4]{2}$.

□

5. (Exercise 14 in DF §14.2.) Show that $\mathbf{Q}(\sqrt{2+\sqrt{2}})$ is a cyclic quartic field, i.e., is a Galois extension of degree 4 over $\mathbf{Q}$ with cyclic Galois group.

Proof. First, note that $\sqrt{2+\sqrt{2}}$ is a root of $p(x) = x^4 - 4x^2 + 2$:

$$\begin{aligned} p\left(\sqrt{2+\sqrt{2}}\right) &= \left(\sqrt{2+\sqrt{2}}\right)^4 - 4\left(\sqrt{2+\sqrt{2}}\right)^2 + 2 \\ &= \left(2+\sqrt{2}\right)^2 - 4\left(2+\sqrt{2}\right) + 2 \\ &= 6 + 4\sqrt{2} - 8 - 4\sqrt{2} + 2 \\ &= 0. \end{aligned}$$

Also, $p(x)$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion, since $2 \mid 2$ and $2 \mid 4$, but $2^2 \nmid 1$. We can also check that $\sqrt{2-\sqrt{2}}$ is a root:

$$\begin{aligned} p\left(\sqrt{2-\sqrt{2}}\right) &= \left(\sqrt{2-\sqrt{2}}\right)^4 - 4\left(\sqrt{2-\sqrt{2}}\right)^2 + 2 \\ &= \left(2-\sqrt{2}\right)^2 - 4\left(2-\sqrt{2}\right) + 2 \\ &= 6 - 4\sqrt{2} - 8 + 4\sqrt{2} + 2 \\ &= 0. \end{aligned}$$

Since $p(x)$ is an even function, the other two roots are $-\sqrt{2+\sqrt{2}}$ and $-\sqrt{2-\sqrt{2}}$. Therefore, if we can show that $\sqrt{2-\sqrt{2}} \in \mathbb{Q}(\sqrt{2+\sqrt{2}})$, we will have shown that the extension is a splitting field for the separable polynomial $p(x)$, thus it is Galois, since it will necessarily contain the negative roots as well by closure.

Note that

$$\begin{aligned} \frac{\sqrt{2-\sqrt{2}}}{\sqrt{2+\sqrt{2}}} &= \frac{\sqrt{2-\sqrt{2}}}{\sqrt{2+\sqrt{2}}} \cdot \frac{\sqrt{2+\sqrt{2}}}{\sqrt{2+\sqrt{2}}} = \frac{\sqrt{4-2}}{2+\sqrt{2}} = \frac{\sqrt{2}}{2+\sqrt{2}} \cdot \frac{2-\sqrt{2}}{2-\sqrt{2}} \\ &= \frac{2\sqrt{2}-2}{4-2} = \frac{2\sqrt{2}-2}{2} = \sqrt{2} - 1. \end{aligned}$$

Also, $\left(\sqrt{2+\sqrt{2}}\right)^2 - 3 = 2 + \sqrt{2} - 3 = \sqrt{2} - 1 \in \mathbb{Q}(\sqrt{2+\sqrt{2}})$. Therefore, $\sqrt{2-\sqrt{2}} = (\sqrt{2}-1)\sqrt{2+\sqrt{2}} =\in \mathbb{Q}(\sqrt{2+\sqrt{2}})$. So $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ is Galois.

Since the Galois group has order 4, and there are 4 possible images for any given root, it must be that the action of an automorphism σ on one root determines the entire map. So consider the action of σ on the root $\sqrt{2+\sqrt{2}}$.

First, note that

$$\left(\sqrt{2+\sqrt{2}}\right)\left(\sqrt{2-\sqrt{2}}\right) = \sqrt{2}.$$

Now, define σ by $\sqrt{2+\sqrt{2}} \mapsto \sqrt{2-\sqrt{2}}$. Then $\left(\sqrt{2+\sqrt{2}}\right)^2 = 2+\sqrt{2} \mapsto 2+\sigma(\sqrt{2}) = \left(\sqrt{2-\sqrt{2}}\right)^2 = 2-\sqrt{2}$, so $\sqrt{2} \mapsto -\sqrt{2}$. Thus,

$$\sigma\left(\sqrt{2-\sqrt{2}}\right) = \frac{\sigma\left(\sqrt{2+\sqrt{2}}\right)}{\sigma(\sqrt{2})} = \frac{\sqrt{2-\sqrt{2}}}{-\sqrt{2}} = -\sqrt{2+\sqrt{2}}.$$

So σ rotates the roots of $p(x)$. Therefore, it cannot be that σ^2 is the identity, since $\sigma^2(\sqrt{2+\sqrt{2}}) = \sigma(\sqrt{2-\sqrt{2}} = -\sqrt{2+\sqrt{2}}$. Since σ is nontrivial and does not have order 2, it must have order 4. So $\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)\right)$ contains an element of order 4, thus it is a cyclic group of order 4. $\square$

6. (Adapted from Exercise 17 in DF §14.2.) Let K/F be a (finite) Galois extension. For each $\alpha \in K$, define the *norm* of α to be

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

(a) Prove that $N_{K/F}(\alpha) \in F$ for any $\alpha \in K$.

Proof. Let $\tau \in \mathrm{Gal}(K/F)$. Then τ acts on $\mathrm{Gal}(K/F)$ as a permutation. Therefore, as a group action, $\tau : \mathrm{Gal}(K/F) \to \mathrm{Gal}(K/F)$ is a bijection. Thus $\{\tau \circ \sigma : \sigma \in \mathrm{Gal}(K/F)\} = \mathrm{Gal}(K/F)$. So

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

Since an arbitrary $\tau \in \mathrm{Gal}(K/F)$ fixes the $N_{K/F}(\alpha)$, we know that $N_{K/F}(\alpha)$ is in the fixed field of $\mathrm{Gal}(K/F)$, which is F.

$\square$

(b) Prove that $N_{K/F}(\alpha\beta) = N_{K/F}(\alpha)N_{K/F}(\beta)$ for any $\alpha, \beta \in K$.

Proof. This follows easily from the fact that σ is an automorphism.

$$\begin{aligned} N_{K/F}(\alpha\beta) &= \prod_{\sigma \in \mathrm{Gal}(K/F)} \sigma(\alpha\beta) = \prod_{\sigma \in \mathrm{Gal}(K/F)} \sigma(\alpha)\sigma(\beta) \\ &= \prod_{\sigma \in \mathrm{Gal}(K/F)} \sigma(\alpha) \prod_{\sigma \in \mathrm{Gal}(K/F)} \sigma(\beta) = N_{K/F}(\alpha)N_{K/F}(\beta) \end{aligned}$$

$\square$

(c) Assume in addition that $[K : F] = 2$. Show that there exists $\gamma \in K$ such that $K = F(\gamma)$ and $\gamma^2 \in F$. Let $D = \gamma^2$. Show that for any $a, b \in F$, $N_{K/F}(a + b\gamma) = a^2 - Db^2$.

Proof. For the first part, we need to assume that F has characteristic > 2. Let $p(x) = ax^2 + bx + c$ be the minimum polynomial of α. Then some $\alpha \in K$ is a root of $p(x)$. So $\alpha^2 = \dfrac{b\alpha + c}{a}$.

Let $\gamma = 2a\alpha + b$. Since $\gamma \in K$, we know that $F(\gamma) \subseteq K$. Since the field has characteristic greater than 2, we have $\alpha = \dfrac{\gamma - b}{2a} \in F(\gamma)$, so $K \subseteq F(\gamma)$. Thus $K = F(\alpha)$. Also, $\gamma^2 = 4a^2\alpha^2 + 4ab\alpha + b^2 = 4a^2\left(\dfrac{b\alpha + c}{a}\right) + 4ab\alpha + b^2 = b^2 - 4ac \in F$. So $D = b^2 - 4ac$ suffices.

Now, let a and b be arbitrary elements of F. Note that $a + b\gamma$ and $a - b\gamma$ are roots of the separable polynomial $x^2 - 2ax + a^2 - Db^2$. Since these roots are not in F, the polynomial is irreducible. Thus the Galois group of K must permute its roots.

Since $\mathrm{Gal}(K/F)$ has order 2, and the automorphisms are defined by their action on γ, the only nontrivial automorphism is the one that takes $a + b\gamma$ to $a - b\gamma$. Therefore,

$$N_{K/F}(a + b\gamma) = \prod_{\sigma \in \mathrm{Gal}(K/F)} \sigma(a + b\gamma) = (a + b\gamma)(a - b\gamma) = a^2 - \gamma^2 b^2 = a^2 - Db^2.$$

□

(d) Given $\alpha \in K$, let $m_\alpha(X) = X^d + a_{d-1}X^{d-1} + \ldots + a_1 X + a_0 \in F[X]$ be the minimal polynomial for α over F. Let $n = [K : F]$. Prove that (i) d divides n, (ii) there are d distinct Galois conjugates of α (that is, the set $\{\sigma(\alpha) : \sigma \in \mathrm{Gal}(K/F)\}$ has d elements), and (iii) each Galois conjugate (i.e. each element of the aforementioned set) appears n/d times in the product defining $N_{K/F}(\alpha)$. Deduce that $N_{K/F}(\alpha) = (-1)^n a_0^{n/d}$.

(Hint: for (iii), use the Galois correspondence (Theorem 14 in §14.2).)

Proof. It is clear that d divides n. d is, by definition, the degree of the extension $F(\alpha)$, and $F \subseteq F(\alpha) \subseteq K$. So by corollary 15 on pg. 524, d must divide n.

Let $\sigma \in \mathrm{Gal}(K/F) = G$. By Theorem 13, m_α is separable, and thus has distinct roots $\alpha_1, \ldots, \alpha_d \in K$, where $\alpha_1 = \alpha$. We can now construct an automorphism σ that takes α to any arbitrary α_i:

Define a homomorphism σ fixing F on $F(\alpha, \alpha_i)$ partially by $\sigma(\alpha) = \alpha_i$, so that $\sigma(a_0 + a_1\alpha + \cdots + a_d\alpha^d) = a_0 + a_1\alpha_i + \cdots + a_d\alpha_i^d$. If α_i is generated by α over F, then σ is completely defined on $F(\alpha, \alpha_i)$. Otherwise, if α_i is not generated by α over F, then define $\sigma(\alpha_i) = \alpha$. This cannot contradict the fact that σ is a homomorphism, since its action on α_i was undetermined. By Theorem 13.27, we know that σ can be extended to an automorphism τ on all of K, since K is the splitting field of some polynomial over $F(\alpha, \alpha_i)$. Therefore, $\tau \in \mathrm{Gal}(K/F)$ takes α to an arbitrary α_i, thus every α_i is a conjugate of α.

Let $E = F(\alpha_1, \ldots, \alpha_d)$, and let $H = \mathrm{Gal}(E/F)$ (since E is the splitting field for the separable polynomial $m_\alpha(x)$, we know it is Galois). By part (iii) of Galois correspondence, $\mathrm{Gal}(E/F) \cong G/H$, thus $|\mathrm{Gal}(E/F)| = \dfrac{|G|}{|H|} = \dfrac{n}{d}$. By the statements in the proof of Galois correspondence, two automorphisms $\sigma_1, \sigma_2 \in G$ restrict to the same embedding of E if and only if they are representatives of the same coset of H in G. Each coset contains n/d elements, and there are d cosets. Let $H_1, \ldots, H_d$ be these cosets, where H_i is such that $\sigma(\alpha) = \alpha_i$ for all $\sigma \in H_i$. Then we have

$$N_{K/F}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(K/F)} \sigma(\alpha) = \prod_{i=1}^{d} \prod_{\sigma \in H_i} \sigma(\alpha) = \prod_{i=1}^{d} \alpha_i^{n/d}$$

since there are n/d elements in H_i, all of which map α to α_i. So each α_i appears n/d times in the product.

Now, the minimal polynomial of α can be expanded as

$$\begin{aligned} m_\alpha(x) &= (x - \alpha_1) \cdots (x - \alpha_d) \\ &= x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + (-1)^d \prod_{i=1}^{d} \alpha_i \\ &= x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 \end{aligned}$$

therefore $a_0 = (-1)^d \prod_{i=1}^{d} \alpha_i$, thus dividing by $(-1)^d$ gives $\prod_{i=1}^{d} \alpha_i = (-1)^d a_0$. So

$$N_{K/F}(\alpha) = \prod_{i=1}^{d} \alpha_i^{n/d} = \left(\prod_{i=1}^{d} \alpha_i \right)^{n/d} = ((-1)^d a_0)^{n/d} = (-1)^n (a_0)^{n/d}.$$

□