Q1 Let K be a finite separable extension of F. Given $\alpha \in K$, the **norm** of α from K to F is defined as

$$N_{K/F}(\alpha) = \prod_{\substack{\varphi: K \to \overline{F} \\ F\text{-embedding}}} \varphi(\alpha).$$

For fields K and L containing F, we write

$$\mathrm{Emb}_F(K, L) = \{F\text{-embeddings } K \to L\}$$

to denote the set of F-embeddings from K to L.

(a) Show that $N_{K/F}(\alpha) \in F$.

Proof. Let L/F be the Galois closure of K/F, with $L \subseteq \overline{F}$. Each $\varphi \in \mathrm{Emb}_F(K, \overline{F})$ can be extended to an F-embedding $\sigma : L \to \overline{F}$, such that $\sigma|_K = \varphi$. And since L/F is normal, then $\sigma(L) = L$, meaning σ is an automorphism of L fixing F, i.e., $\sigma \in \mathrm{Gal}(L/F)$. Since

$$\varphi(K) = \sigma(K) \subseteq \sigma(L) = L,$$

then φ can be considered as an F-embedding from K to $L \subseteq \overline{F}$.

Given $\tau \in \mathrm{Gal}(L/F)$, we consider the map

$$\begin{gathered} \mathrm{Emb}_F(K, \overline{F}) \to \mathrm{Emb}_F(K, \overline{F}), \\ \varphi \mapsto \tau \circ \varphi. \end{gathered}$$

Since $\varphi(K) \subseteq L$ and τ fixes F, we know each $\tau \circ \varphi$ is an F-embedding $K \to \overline{F}$, i.e., this map is well-defined. We claim that this map is a bijection.

Suppose $\tau \circ \varphi_1 = \tau \circ \varphi_2$, for a pair $\varphi_1, \varphi_2 \in \mathrm{Emb}_F(K, \overline{F})$. Extend φ_1 and φ_2 to automorphisms $\sigma_1, \sigma_2 \in \mathrm{Gal}(L/F)$, respectively, so

$$\tau\sigma_1|_K = \tau \circ \varphi_1 = \tau \circ \varphi_2 = \tau\sigma_2|_K.$$

Composing with τ^{-1}, we obtain

$$\varphi_1 = \sigma_1|_K = \tau^{-1}\tau\sigma_1|_K = \tau^{-1}\tau\sigma_2|_K = \sigma_2|_K = \varphi_2,$$

which proves injectivity. Moreover, with the number of F-embeddings being finite, we conclude that the map is a bijection. Therefore,

$$\tau(N_{K/F}(\alpha)) = \prod_{\varphi \in \mathrm{Emb}_F(K, \overline{F})} (\tau \circ \varphi)(\alpha) = \prod_{\varphi \in \mathrm{Emb}_F(K, \overline{F})} \varphi(\alpha) = N_{K/F}(\alpha).$$

This proves that $N_{K/F}(\alpha)$ is fixed by every element of $\mathrm{Gal}(L/F)$, i.e.,

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

$\square$

(b) Suppose that $\alpha \in \overline{F}$ and $m_{\alpha,F}(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ is separable. Show that $N_{F(\alpha)/F}(\alpha) = (-1)^n a_0$.

Proof. Each element of $\mathrm{Emb}_F(F(\alpha), \overline{F})$ is completely determined by the image of α, which must be a root of $m_{\alpha,F}(x)$. In other words, there is an injection

$$\begin{aligned} \mathrm{Emb}_F(F(\alpha), \overline{F}) &\to \{\text{roots of } m_{\alpha,F}(x) \text{ in } \overline{F}\}, \\ \varphi &\mapsto \varphi(\alpha). \end{aligned}$$

To show it is a bijection, we show that the sets are the same size. Since $m_{\alpha,F}(x)$ is separable and degree n, it has exactly n distinct roots. Moreover, $F(\alpha)/F$ is a finite separable extension, giving us

$$|\,\mathrm{Emb}_F(F(\alpha), \overline{F})| = [F(\alpha) : F] = \deg m_{\alpha,F}(x) = n.$$

Hence, the above evaluation map is a bijection.

If S is the set of roots of $m_{\alpha,F}(x)$ in $\overline{F}$, then $m_{\alpha,F}(x) = \prod_{\beta \in S}(x - \beta)$, so

$$a_0 = m_{\alpha,F}(0) = \prod_{\beta \in S}(0 - \beta) = (-1)^n \prod_{\beta \in S} \beta.$$

Thus,

$$N_{F(\alpha)/F}(\alpha) = \prod_{\varphi \in \mathrm{Emb}_F(F(\alpha), \overline{F})} \varphi(\alpha) = \prod_{\beta \in S} \beta = (-1)^n a_0.$$

$\square$

Q2 Problem 14.7.4 Let $K = \mathbb{Q}(\sqrt[n]{a})$, where $a \in \mathbb{Q}$, $a > 0$ and suppose $[K : \mathbb{Q}] = n$ (i.e., $x^n - a$ is irreducible). Let E be any subfield of K and let $[E : \mathbb{Q}] = d$. Prove that $E = \mathbb{Q}(\sqrt[d]{a})$. [Consider $N_{K/E}(\sqrt[n]{a}) \in E$.]

Proof. Since $K/\mathbb{Q}$ is finite and $\mathbb{Q}$ is perfect, the extension is separable. Therefore, K/E is a finite separable extension, with

$$|\operatorname{Emb}_E(K, \overline{\mathbb{Q}})| = [K : E] = \frac{[K : \mathbb{Q}]}{[E : \mathbb{Q}]} = \frac{n}{d}.$$

In particular, note $n/d \in \mathbb{Z}_{>0}$. By Q1(a), we have

$$N_{K/E}(\sqrt[n]{a}) = \prod_{\varphi \in \operatorname{Emb}_E(K, \overline{\mathbb{Q}})} \varphi(\sqrt[n]{a}) \ \in E.$$

Note that $K = E(\sqrt[n]{a})$, so any E-embedding $K \to \overline{\mathbb{Q}}$ is completely determined by the image of $\sqrt[n]{a}$, which must be a root of $x^n - a$. Suppose $\operatorname{Emb}_E(K, \overline{\mathbb{Q}}) = \{\varphi_1, \ldots, \varphi_{n/d}\}$, and assume that $\varphi_j(\sqrt[n]{a}) = \sqrt[n]{a}\zeta_n^{r_j}$ for $0 \le r_j \le n$. Then

$$N_{K/E}(\sqrt[n]{a}) = \prod_{j=1}^{n/d} \varphi_j(\sqrt[n]{a}) = \sqrt[n]{a}^{n/d} \zeta_n^{r_1} \cdots \zeta_n^{r_{n/d}} = \sqrt[d]{a}\zeta_n^{r_1 + \cdots + r_{n/d}} \in E.$$

Since $E \subseteq K = \mathbb{Q}(\sqrt[n]{a}) \subseteq \mathbb{R}$ and $\sqrt[d]{a} \in \mathbb{R}$, then

$$\zeta_n^{r_1 + \cdots + r_{n/d}} = \sqrt[d]{a}^{-1} N_{K/E}(\sqrt[n]{a}) \in \mathbb{R},$$

so $\zeta_n^{r_1 + \cdots + r_{n/d}} = \pm 1$. Hence, $N_{K/E}(\sqrt[n]{a}) = \pm\sqrt[d]{a} \in E$.

Since $\mathbb{Q}(\sqrt[d]{a}) \subseteq E$,

$$[\mathbb{Q}(\sqrt[d]{a}) : \mathbb{Q}] \le [E : \mathbb{Q}] = d.$$

To prove $E = \mathbb{Q}(\sqrt[d]{a})$, it remains to show the opposite inequality.

Since the polynomial $x^{n/d} - \sqrt[d]{a} \in (\mathbb{Q}(\sqrt[d]{a}))[x]$ has a root of $\sqrt[n]{a}$, it has as a factor the minimal polynomial of $\sqrt[n]{a}$ over $\mathbb{Q}(\sqrt[d]{a})$. Then

$$[K : \mathbb{Q}(\sqrt[d]{a})] = [(\mathbb{Q}(\sqrt[d]{a}))(\sqrt[n]{a}) : \mathbb{Q}(\sqrt[d]{a})] = \deg m_{\sqrt[n]{a}, \mathbb{Q}(\sqrt[d]{a})}(x) \le \frac{n}{d},$$

giving us

$$[\mathbb{Q}(\sqrt[d]{a}) : \mathbb{Q}] = \frac{[K : \mathbb{Q}]}{[K : \mathbb{Q}(\sqrt[d]{a})]} = \frac{n}{[K : \mathbb{Q}(\sqrt[d]{a})]} \ge \frac{n}{n/d} = d.$$

Hence, $[\mathbb{Q}(\sqrt[d]{a}) : \mathbb{Q}] = d$, implying that $E = \mathbb{Q}(\sqrt[d]{a})$.

$\square$

Q3 Problem 14.7.5 Let K be as in the previous exercise. Prove that if n is odd then K has no nontrivial subfields which are Galois over $\mathbb{Q}$ and if n is even then the only nontrivial subfield of K which is Galois over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{a})$.

Proof. Suppose E is a subfield of K which is Galois over $\mathbb{Q}$. By Q2, we know $E = \mathbb{Q}(\sqrt[d]{a})$ for some $d \mid n$. Since $\mathbb{Q}(\sqrt[d]{a})/\mathbb{Q}$ is Galois, it must be the splitting field of $m_{\sqrt[d]{a},\mathbb{Q}}(x) = x^d - a$. Therefore, E contains the d-th roots of unity. But unless d is 1 or 2, the d-th roots of unity are not contained in $\mathbb{R}$. Since $E \subseteq K \subseteq \mathbb{R}$, the it must be the case that $d = 1$ or $d = 2$.

If n is odd, then $d \mid n$ implies $d = 1$, so $E = \mathbb{Q}(a) = \mathbb{Q}$. That is, K has not nontrivial subfields which are Galois over $\mathbb{Q}$.

Suppose n is even. As before, $d = 1$ implies $E = \mathbb{Q}$. That is, E is nontrivial only if $d = 2$; we check that $\mathbb{Q}(\sqrt{a})$ is as desired. Since n is even, then $n/2 \in \mathbb{Z}$, so $\sqrt{a} = \sqrt[n]{a}^{n/2} \in K$, i.e., $\mathbb{Q}(\sqrt{a}) \subseteq K$. Moreover, $\mathbb{Q}(\sqrt{a})/\mathbb{Q}$ is Galois, as the splitting field of $x^2 - a \in \mathbb{Q}[x]$. Additionally, $\mathbb{Q}(\sqrt{a}) \neq \mathbb{Q}$ since, from Q2, we know $[\mathbb{Q}(\sqrt{a}) : \mathbb{Q}] = 2$. Hence, $\mathbb{Q}(\sqrt{a})/\mathbb{Q}$ is in fact a nontrivial Galois subextension of $K/\mathbb{Q}$.

$\square$

Q4 Problem 14.7.6 Let L be the Galois closure of K is the previous two exercises (i.e., the splitting field of $x^n - a$). Prove that $[L : \mathbb{Q}] = n\varphi(n)$ or $\frac{1}{2}n\varphi(n)$. [Note that $\mathbb{Q}(\zeta_n) \cap K$ is a Galois extension of $\mathbb{Q}$.]
(Here $\varphi(n)$ is Euler's totient function. It counts the number of integers between 1 and n coprime to n. For $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, $\varphi(n) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \cdots (p_r^{k_r} - p_r^{k_r-1})$. You can use the fact that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.)

Proof. Since $x^n - a$ splits over L, then L contains all n-th roots of unity, i.e., $\mathbb{Q}(\zeta_n) \subseteq L$, so

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\zeta_n)][\mathbb{Q}(\zeta_n) : \mathbb{Q}] = [L : \mathbb{Q}(\zeta_n)]\varphi(n).$$

Let $F = \mathbb{Q}(\zeta_n)$, then $x^n - 1$ splits over F and $L = F(\sqrt[n]{a})$. Therefore, $m = [F(\sqrt[n]{a}) : F]$, where m is the minimum positive integer such that $\sqrt[n]{a}^m \in F$.

We consider the extension $\mathbb{Q}(\sqrt[n]{a}^m)/\mathbb{Q}$. By assumption, F contains $\sqrt[n]{a}^m$, so $\mathbb{Q}(\sqrt[n]{a}^m)/\mathbb{Q}$ is a subextension of $F/\mathbb{Q}$. By the fundamental theorem,

$$\mathrm{Gal}(F/\mathbb{Q}(\sqrt[n]{a}^m)) \leq \mathrm{Gal}(F/\mathbb{Q}).$$

Moreover, since $\mathrm{Gal}(F/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ is abelian, then every subgroup is a normal subgroup, implying that $\mathbb{Q}(\sqrt[n]{a}^m)/\mathbb{Q}$ is a Galois extension. Since $\sqrt[n]{a} \in K$, then $\mathbb{Q}(\sqrt[n]{a}^m) \subseteq K$, i.e., $\mathbb{Q}(\sqrt[n]{a}^m)/\mathbb{Q}$ is a Galois subextension of $K/\mathbb{Q}$. By Q3, we now consider two possible cases: n is odd and n is even.

If n is odd, then we must have $\mathbb{Q}(\sqrt[n]{a}^m) = \mathbb{Q}$, i.e., $\sqrt[n]{a}^m \in \mathbb{Q}$. But we know that n is the minimum positive integer such that $\sqrt[n]{a}^n = a \in \mathbb{Q}$, implying that $m \geq n$. By assumption, m was chosen to the the minimum positive integer such that $\sqrt[n]{a}^m \in F$. Since $\sqrt[n]{a}^n \in \mathbb{Q} \subseteq F$, we know n suffices, implying $m \leq n$. Hence,

$$n = m = [F(\sqrt[n]{a}) : F] = [L : \mathbb{Q}(\zeta_n)],$$

so

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\zeta_n)]\varphi(n) = n\varphi(n).$$

If n is even, then either $\mathbb{Q}(\sqrt[n]{a}^m) = \mathbb{Q}$ (handled in the odd case) or $\mathbb{Q}(\sqrt[n]{a}^m) = \mathbb{Q}(\sqrt{a})$. Assuming the latter is true, we claim that $m = n/2$. Consider the norm

$$N_{\mathbb{Q}(\sqrt[n]{a}^m)/\mathbb{Q}}(\sqrt[n]{a}^m) = \prod_{\varphi \in \mathrm{Emb}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[n]{a}^m), \overline{\mathbb{Q}})} \varphi(\sqrt[n]{a}^m) \in \mathbb{Q}.$$

Since $\mathbb{Q}(\sqrt[n]{a}^m) = \mathbb{Q}(\sqrt{a})$ is separable over $\mathbb{Q}$,

$$|\mathrm{Emb}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[n]{a}^m), \overline{\mathbb{Q}})| = [\mathbb{Q}(\sqrt[n]{a}^m) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{a}) : \mathbb{Q}] = 2.$$

If $\mathrm{Emb}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[n]{a}^m), \overline{\mathbb{Q}}) = \{\varphi_1, \varphi_2\}$, then

$$N_{\mathbb{Q}(\sqrt[n]{a}^m)/\mathbb{Q}}(\sqrt[n]{a}^m) = \varphi_1(\sqrt[n]{a}^m)\varphi_2(\sqrt[n]{a}^m) \in \mathbb{Q}.$$

Both $\mathbb{Q}$-embeddings φ_1, φ_2 can be extended to $\sigma_1, \sigma_2 \in \mathrm{Gal}(L/\mathbb{Q})$ such that $\sigma_j|_{\mathbb{Q}(\sqrt[n]{a}^m)} = \varphi_j$, for $j = 1, 2$. Then suppose $\sigma_j(\sqrt[n]{a}) = \sqrt[n]{a}\zeta_n^{r_j}$, so

$$\varphi_1(\sqrt[n]{a}^m)\varphi_2(\sqrt[n]{a}^m) = \sigma_1(\sqrt[n]{a}^m)\sigma_2(\sqrt[n]{a}^m) = (\sqrt[n]{a}\zeta_n^{r_1})^m(\sqrt[n]{a}\zeta_n^{r_2})^m = \sqrt[n]{a}^{2m}\zeta_n^{(r_1+r_2)m}.$$

Since this is an element of $\mathbb{Q} \subseteq \mathbb{R}$, then it must be $\pm\sqrt[n]{a}^{2m}$, i.e., we have that $\sqrt[n]{a}^{2m} \in \mathbb{Q}$. As previously noted, n is the minimum positive integer such that $\sqrt[n]{a}^n \in \mathbb{Q}$, which implies that $m \geq n/2$. On the other hand, by assumption, we have $\mathbb{Q}(\sqrt[n]{a}^m) = \mathbb{Q}(\sqrt{a}) \subseteq F$; in particular, $\sqrt{a} \in F$, so

$$\sqrt[n]{a}^{n/2} = \sqrt{a} \in F.$$

Since m was chosen to be the minimum positive integer such that $\sqrt[n]{a}^m \in F$, this implies $m \leq n/2$. Hence,

$$\frac{n}{2} = m = [F(\sqrt[n]{a}) : F] = [L : \mathbb{Q}(\zeta_n)],$$

so

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\zeta_n)]\varphi(n) = \tfrac{1}{2}n\varphi(n).$$

$\square$

Q5 Problem 14.7.18 Let $D \in \mathbb{Z}$ be a squarefree integer and let $a \in \mathbb{Q}$ be a nonzero rational number. Prove that if $\mathbb{Q}(\sqrt{a\sqrt{D}})$ is Galois over $\mathbb{Q}$ [and $D \neq 1$] then $D = -1$.

Proof. Immediately, we can deduce two facts about the squarefree integer D. First, $D \neq 0$, as zero is trivially divisible by any square integer. Second, D is not the square of any rational number; one can check that $p \in \mathbb{Q}$ and $p^2 \in \mathbb{Z}$ imply that $p \in \mathbb{Z}$.

Our first main step is determining the minimal polynomial of $\sqrt{a\sqrt{D}}$ over $\mathbb{Q}$.

Consider the extension $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$, which is the splitting field of the irreducible separable polynomial $x^2 - D \in \mathbb{Q}[x]$. The irreducibility over $\mathbb{Q}$ follows from the fact that D is not the square of any rational number (i.e., $x^2 - D$ has no roots in $\mathbb{Q}$), implying $m_{\sqrt{D},\mathbb{Q}}(x) = x^2 - D$. The separability follows from the factorization in $\overline{\mathbb{Q}}[x]$, given by

$$x^2 - D = (x - \sqrt{D})(x + \sqrt{D}),$$

in which $D \neq 0$ implies $\sqrt{D} \neq -\sqrt{D}$. Hence, $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$ is a Galois extension with

$$[\mathbb{Q}(\sqrt{D}) : \mathbb{Q}] = \deg m_{\sqrt{D},\mathbb{Q}}(x) = \deg(x^2 - D) = 2.$$

Now, let $F = \mathbb{Q}(\sqrt{D}) = \{p + q\sqrt{D} \mid p, q \in \mathbb{Q}\}$, where 1 and $\sqrt{D}$ form a basis of F over $\mathbb{Q}$. It can be seen that $F/\mathbb{Q}$ is a subextension of $\mathbb{Q}(\sqrt{a\sqrt{D}})/\mathbb{Q}$, since

$$\sqrt{D} = a^{-1}\sqrt{a\sqrt{D}}^2 \in \mathbb{Q}(\sqrt{a\sqrt{D}}).$$

In particular, $\sqrt{a\sqrt{D}}$ generates the same field over both $\mathbb{Q}$ and F, so it makes sense to define

$$K = F(\sqrt{a\sqrt{D}}) = \mathbb{Q}(\sqrt{a\sqrt{D}}).$$

Since the polynomial $x^2 - a\sqrt{D} \in F[x]$ has $\sqrt{a\sqrt{D}}$ as a root, then the degree of K/F is at most 2. To show it is exactly 2, it suffices to show $\sqrt{a\sqrt{D}} \notin F$; in which case, $x^2 - a\sqrt{D}$ has no roots in F, and is therefore irreducible in $F[x]$. Assume, in contradiction, that there exist $p, q \in \mathbb{Q}$ such that, in F, we have

$$\sqrt{a\sqrt{D}} = p + q\sqrt{D} \implies a\sqrt{D} = p^2 + q^2 D + 2pq\sqrt{D}.$$

As mentioned above, 1 and $\sqrt{D}$ form a basis for F, so in particular, $p^2 + q^2 D = 0$. It must be the case that q is nonzero; otherwise, $\sqrt{D} = a^{-1}p^2 \in \mathbb{Q}$, which is false. Then we can write

$$-D = \frac{p^2}{q^2} = \left(\frac{p}{q}\right)^2 \in \mathbb{Z},$$

which implies $p/q \in \mathbb{Z}$ with $(p/q)^2 \mid D$, contradicting the fact that D is a squarefree integer (unless $p/q = 1$, in which case we are done). Hence, $\sqrt{a\sqrt{D}} \notin F$, and we conclude that that

$x^2 - a\sqrt{D}$ is irreducible in $F[x]$. This means $x^2 - a\sqrt{D}$ is the minimal polynomial of $\sqrt{a\sqrt{D}}$ over F, so

$$[K : F] = \deg m_{\sqrt{a\sqrt{D}},F}(x) = \deg(x^2 - a\sqrt{D}) = 2.$$

Thus, we now have

$$[K : \mathbb{Q}] = [K : F][F : \mathbb{Q}] = 2 \cdot 2 = 4.$$

Since $\sqrt{a\sqrt{D}}$ is a root of the degree 4 monic polynomial $x^4 - a^2D \in \mathbb{Q}[x]$, its minimal polynomial over $\mathbb{Q}$ must precisely be $x^4 - a^2D$. Therefore, since $K/\mathbb{Q}$ is Galois, we conclude that it is the splitting field of

$$x^4 - a^2D = \left(x - \sqrt{a\sqrt{D}}\right)\left(x + \sqrt{a\sqrt{D}}\right)\left(x - i\sqrt{a\sqrt{D}}\right)\left(x + i\sqrt{a\sqrt{D}}\right).$$

Notice that $i = \sqrt{a\sqrt{D}}^{-1} \cdot i\sqrt{a\sqrt{D}} \in K$, implying $F(i)/F$ is a subextension of K/F with

$$[K : F(i)][F(i) : F] = [K : F] = 2.$$

This means that either $K = F(i)$ or $F(i) = F$, exclusively. We will show that the latter case is equivalent to $D = -1$, then that the the former case is not possible.

Clearly, if $D = -1$, then $F = \mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i) = \mathbb{Q}(i, i) = F(i)$. To see the opposite implication, suppose $F(i) = F$, so $i \in F$. Then there exist $p, q \in \mathbb{Q}$ such that, in F, we have

$$i = p + q\sqrt{D} \implies -1 = p^2 + q^2D + 2pq\sqrt{D}.$$

It must be the case that q is nonzero; otherwise, $i = p \in \mathbb{Q}$, which is false. Recall that 1 and $\sqrt{D}$ form a basis for F over $\mathbb{Q}$, so $2pq = 0$ implies $p = 0$. Then we can write

$$-D = \frac{1}{q^2} = \left(\frac{1}{q}\right)^2 \in \mathbb{Z},$$

which implies $1/q \in \mathbb{Z}$ with $(1/q)^2 \mid D$. This can only be true if $1/q^2 = 1$, so in fact $D = -1$. Thus, $D = -1$ if and only if $F(i) = F$, and remains to prove $K \neq F(i)$.

Assume, in contradiction, that $K = F(i)$ (which implies $D \neq -1$). In particular, there exist $u, v \in F$ such that, in $F(i)$, we have

$$\sqrt{a\sqrt{D}} = u + vi \implies a\sqrt{D} = u^2 - v^2 + 2uvi.$$

It must be the case that v is nonzero; otherwise, $\sqrt{a\sqrt{D}} = u \in F$, which is false. Since $[F(i) : F] = [K : F] = 2$, then 1 and i form a basis of $F(i)$ over F, so $2uv = 0$ implies $u = 0$. Then we can write

$$\sqrt{a\sqrt{D}} = vi \implies -a\sqrt{D} = v^2.$$

Since $v \in F$, there exist $p, q \in \mathbb{Q}$ such that $v = p + q\sqrt{D}$, then

$$-a\sqrt{D} = (p + q\sqrt{D})^2 = p^2 + q^2D + 2pq\sqrt{D}.$$

It must be the case that q is nonzero; otherwise, $\sqrt{D} = -a^{-1}p^2 \in \mathbb{Q}$, which is false. Then

$$p^2 + q^2 D = 0 \implies -D = \frac{p^2}{q^2} = \left(\frac{p}{q}\right)^2 \in \mathbb{Z},$$

which implies $p/q \in \mathbb{Z}$ with $(p/q)^2 \mid D$. If $p/q \neq 1$, then this contradicts the fact that D is a squarefree integer. If $p/q = 1$, then this contradicts the fact that $D \neq -1$. Either way, we have reached a contradiction, so $K \neq F(i)$, implying $D = -1$.

$\square$