The splitting field of $X^n - a$

Consider the polynomial $f(X) := X^n - a$ ($a \neq 0$) over a field K whose characteristic does not divide n. Then the derivative $f'(X) = nX^{n-1}$ does not vanish at any root of f, so f is separable.

Let $L \supset K$ be a splitting field of f. If α and β are roots, then $(\beta/\alpha)^n = a/a = 1$, and so $\beta = \xi\alpha$ where $\xi^n = 1$, i.e., $\xi \in L$ is an n-th root of unity. Fixing α, we have, in L, n distinct β, and hence n distinct ξ; and the roots of f are given by $\xi\alpha$ as ξ runs through these n-th roots of unity. Thus L contains a splitting field $L_1 \supset K$ of $X^n - 1$. The n-th roots of unity form a multiplicative group, of order n, which by a previous result is cyclic; and if ζ is a generator of this group then $L_1 = K(\zeta)$. Hence, $L = K(\zeta, \alpha)$.

Exercise. To each $\theta \in G := \mathrm{Aut}_K L$ associate the pair (k, ℓ) such that

$$\theta\alpha = \zeta^k\alpha, \quad \theta\zeta = \zeta^\ell \qquad \big(0 \le k < n,\ 1 \le \ell < n,\ (\ell, n) = 1\big).$$

Show that this gives an injective group homomorphism $G \hookrightarrow \mathbb{Z}_n \rtimes_\psi \mathbb{Z}_n^*$, where for $\ell \in \mathbb{Z}_n^*$, $\psi(\ell)$ is multiplication in $\mathbb{Z}_n$ by ℓ. Is G solvable?

Assume now that $\zeta \in K$, so that $K(\zeta) = K$.

Any $\nu \in G := \mathrm{Aut}_K L$ is determined by $\nu(\alpha)$, which is $\zeta^k\alpha$ for some $k \in [0, n-1]$, and accordingly we denote that ν by ν_k. The mapping $G \to \mathbb{Z}_n$ given by sending ν_k to k is easily seen to be an injective homomorphism. So G, being isomorphic to a subgroup of $\mathbb{Z}_n$, is cyclic, of order, say, n/e, generated by ν_e.

Then $b := \alpha^{n/e}$ is G-invariant, so lies in K; and $a = b^e$. In fact e is characterized by the property that its divisors are precisely those divisors f of n such that $a = c^f$ for some $c \in K$ (see below).

The fields between L and K correspond one-one to subgroups of the cyclic group G, hence to divisors d of n/e. The unique subgroup $G_d < G$ of index d is generated by ν_{ed}. *The corresponding field is $K(\alpha^{n/ed})$.* Indeed,

$$\nu_k(\alpha^{n/ed}) = \alpha^{n/ed} \iff (\zeta^k\alpha)^{n/ed} = \alpha^{n/ed} \iff (\zeta^k)^{n/ed} = 1 \iff k = med \text{ for some } m \iff \nu_k = \nu_{de}^m.$$

In other words, $\mathrm{Aut}_{K(\alpha^{n/ed})} L = G_d$, whence the assertion.

The G-orbit of $\alpha^{n/ed}$ over K consists of the d elements $\zeta^{in/d}\alpha^{n/ed}$ $(0 \le i < d)$, which are just the roots of $X^d - b$. Hence $K(\alpha^{n/ed})$ is the splitting field of $X^d - b$ over K, and $X^d - b$ is irreducible over K. In particular, $X^{n/e} - b$ is irreducible over K.

The same argument shows that $X^{n/e} - (\zeta^k\alpha)^{n/e} = X^{n/e} - \zeta^{kn/e}b$ is irreducible over K for $1 \le k \le e$. It follows that *over K, the factorization of $X^n - a$ into monic irreducible polynomials is*

$$X^n - a = \prod_{k=1}^{e} (X^{n/e} - \zeta^{kn/e}b).$$

Furthermore, *e is divisible by every divisor f of n such that a is an f-th power in K.* For if $f|n$ and $a = c^f$ then over K,

$$X^n - a = \prod_{i=1}^{f} (X^{n/f} - \zeta^{in/f}c),$$

so that each factor $X^{n/f} - \zeta^{in/f}c$ is a product of polynomials of the form $X^{n/e} - \zeta^{kn/e}b$, whence $f|e$.