

1. for $p = 2$ we have splitting field $\mathbb{Q}(\sqrt{2})$ which is a degree 2 extension. Now let $p > 2$, then the splitting field is $k := \mathbb{Q}(2^{1/p}, \zeta_p 2^{1/p}, \dots, \zeta_p^{p-1} 2^{1/p})$, then $\frac{\zeta_p 2^{1/p}}{2^{1/p}} = \zeta_p \in k$, hence $k \subset \mathbb{Q}(\zeta_p, 2^{1/p})$, and the reverse inclusion is obvious so they are equal. It follows that the degree of this extension is $p(p-1)$, since ζ_p has minimum polynomial $x^{p-1} + x^{p-2} + \dots + 1$ of degree $p-1$ in $\mathbb{Q}[x]$. And $2^{1/p}$ has minimum polynomial $x^p - 2$ (Gauss' lemma to reduce to \mathbb{Z} , then irreducible from Eisenstein) of degree p . Implying that $p, p-1 \mid [k : \mathbb{Q}]$, or equivalently $p(p-1) \mid [k : \mathbb{Q}]$. For equality, note that $[\mathbb{Q}(\zeta_p, 2^{1/p}) : \mathbb{Q}(\zeta_p)] \leq p$, since $2^{1/p}$ still satisfies $x^p - 2$, so that

$$p(p-1) \leq [k : \mathbb{Q}] = [\mathbb{Q}(\zeta_p, 2^{1/p}) : \mathbb{Q}(\zeta_p)][\mathbb{Q}(\zeta_p) : \mathbb{Q}] \leq p(p-1)$$

Proof that $x^{p-1} + x^{p-2} + \dots + 1$ is irreducible: We first note that $f(x)$ is irreducible in \mathbb{Q} when it is irreducible in \mathbb{Z} by Gauss' lemma. Then $f(x)$ is irreducible if and only if $f(x+1)$ is irreducible, one way to see this is $F : \mathbb{Z}[x] \rightarrow \mathbb{Z}[x], x \mapsto x+1$ is a \mathbb{Z} -module automorphism. Hence

$$f(x) = g(x)h(x) \iff f(F(x)) = F(f(x)) = F(g(x))F(h(x)) = g(F(x))h(F(x))$$

Then irreducibility follows from Eisenstein's criterion after the following computation;

$$\begin{aligned} \sum_{k=0}^{p-1} (x+1)^k &= \frac{(x+1)^p - 1}{(x+1) - 1} = x^{-1} \sum_{k=1}^p \binom{p}{k} x^k = \sum_1^p \binom{p}{k} x^{k-1} \\ &= x^{p-1} + \sum_{k=1}^{p-2} a_k x^k + p, \text{ where } p \mid a_k \end{aligned}$$

2. I claim that $z := \zeta_3 + 2^{1/3}$ is such a number, it will suffice to show that $\deg(\min(z, \mathbb{Q})) = 6 = [\mathbb{Q}(\zeta_3, 2^{1/3}) : \mathbb{Q}]$. But then since $\mathbb{Q}(z)$ is a subextension it has degree 2, 3 or 6 over \mathbb{Q} , so it is sufficient to show that $\deg \min(z, \mathbb{Q}) > 3$. Then we can take basis for $\mathbb{Q}(\zeta_3, 2^{1/3})/\mathbb{Q}$ to be $\{2^{1/3}\zeta_3, 2^{2/3}\zeta_3, 2^{1/3}\zeta_3^{-1}, 2^{2/3}\zeta_3^{-1}, \zeta_3, \zeta_3^{-1}\}$. We can see this is a basis, since it contains six elements, and $1 = 2(\zeta_3 + \zeta_3^{-1})$ is sufficient to check that it spans $\mathbb{Q}(\zeta_3, 2^{1/3})$ since this allows us to write the rest of the extension in terms of the basis. First we compute the powers of z up to 3.

$$\begin{aligned} z^2 &= \zeta_3^{-1} + 2\zeta_3 2^{1/3} + 2^{2/3} & z^3 &= 3(\zeta_3^{-1} 2^{1/3} + \zeta_3 2^{2/3} + 2(\zeta_3 + \zeta_3^{-1})) \\ 1 &= \zeta_3 + \zeta_3^{-1} & z &= \zeta_3 + 2^{1/3}\zeta_3 + 2^{1/3}\zeta_3^{-1} \end{aligned}$$

Now consider any degree ≤ 3 polynomial evaluated at z ,

$$\begin{aligned} p(z) &= az^3 + bz^2 + cz + d \\ &= (2b+c)(2^{1/3}\zeta_3) + 3a2^{2/3}\zeta_3 + (3a+c)(2^{1/3}\zeta_3^{-1}) + (6a+c+d)(\zeta_3) + (6a+b+d)(\zeta_3^{-1}) \end{aligned}$$

Then by linear independence of basis elements, $p(z)$ is equal to zero if and only if

$$\begin{aligned} 2b + c &= 0 \\ 3a + c &= 0 \\ 6a + c + d &= 0 \\ 6a + b + d &= 0 \end{aligned}$$

then from the second 2 equations we get $c = -b$, implying from the first equation that $c = b = 0$ which implies in the second equation $a = 0$, so that $a = b = c = 0$, which means d must be zero as well. So that $\deg \min(z, \mathbb{Q}) > 3$, which implies it must be 6 and we are done.

3. $[K : \mathbb{Q}] \in \{6, 3, 2, 1\}$, since $[K : \mathbb{Q}] | 6$. For a more detailed explanation, the largest irreducible factor of $f(x)$ may have degree 1, 2 or 3. The first case is the trivial case where f splits over \mathbb{Q} , so that $K = \mathbb{Q}$ is an extension of degree 1. In the second case $[K : \mathbb{Q}]$ has degree 2, since adjoining a root α of a quadratic polynomial gives a field extension of degree 2 containing the other root. Finally if f itself is irreducible, then $[K : \mathbb{Q}]$ may have degree 3 in the case where the extension is simple, or degree 6 otherwise no other values are possible, since when a root of degree 3 is adjoined, then the polynomial splits in the new field, or is a quadratic, so that the roots are contained in a degree 2 extension of the degree 3 extension, which has degree 6 over the original field.

Examples:

$$[K : \mathbb{Q}] = 1 \quad f(x) = (x - 1)^3 \quad K = \mathbb{Q}$$

$$[K : \mathbb{Q}] = 2 \quad f(x) = (x - 1)(x^2 - 2) \quad K = \mathbb{Q}(\sqrt{2})$$

$$[K : \mathbb{Q}] = 3 \quad f(x) = (x - (\zeta_7 + \zeta_7^{-1}))(x - (\zeta_7^3 + \zeta_7^4))(x - (\zeta_7^2 + \zeta_7^5)) = x^3 + x^2 - 2x - 1 \quad K = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$$

$$[K : \mathbb{Q}] = 6 \quad f(x) = x^3 - 2 \quad K = \mathbb{Q}(2^{1/3}, \zeta_3)$$

4. Let L be the algebraic closure containing N and L' be an algebraic closure of N' , then we have the embedding by the identity $E \rightarrow L'$. By the extension theorem, there exists an extension $\sigma : N \rightarrow L'$ which is identity on E and thus F . We first check that ${}^\sigma N$ is normal, if N is the splitting field of polynomials $\{f_i\}_i$, then ${}^\sigma N$ is the splitting field of $\{{}^\sigma f_i\}_i$, since if f_i has roots $\{\alpha_j\}_j$, then $\{{}^\sigma \alpha_j\}_j$ are the roots of ${}^\sigma f_i$. If ${}^\sigma N$ weren't the normal closure of E in L' , then there would exist $E \subset N'' \subsetneq {}^\sigma N$ normal. Then since σ is invertible on its image, we could take $E \subset \sigma^{-1} N'' \subsetneq N$, where once again the image would be normal, but this contradicts N being the normal closure. Hence ${}^\sigma N$ is the normal closure of E in L' , this implies that $E \subset {}^\sigma N \cap N' = {}^\sigma N$ since the intersection is normal. Hence $\sigma : N \rightarrow N'$ is an F homomorphism.

If $\sigma : N \rightarrow N'$ is an F homomorphism, then it must be injective. From the construction above we have identity on E , so that $E \subset {}^\sigma N \subset N'$, but then by hypothesis, there are no subextensions implying that $\sigma(N) = N'$ is an F -isomorphism.

5. E is contained in some algebraically closed field L , then σ can be seen as an embedding from K into L , so that there exists an embedding $\tau : E \rightarrow L$ extending σ by the extension theorem. Since E is normal this embedding is an automorphism on E (one of the three equivalent conditions for normal extensions - NOR 1 in Lang).