José Alberto Hoces Castro

Exercise 1. Find the monic irreducible polynomial with rational coefficients which has as zero $\alpha = \sqrt{3} + \sqrt[3]{5}$

Using Eisenstein's criterion:

•) $x^2 - 3$, we use $p = 3 \Rightarrow 3 \nmid 1, 9 \nmid 3 \Rightarrow$ Irreducible in $\mathbb{Q}[x]$

•) $x^3 - 5$, we use $p = 5 \Rightarrow 5 \nmid 1, 25 \nmid 5 \Rightarrow$ Irreducible in $\mathbb{Q}[x]$

Because of this, separate field degrees are:

$$[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \qquad [\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 3$$

This case is simpler than the case of two square roots, since the degree $[\mathbb{Q}(\sqrt{3}, \sqrt[3]{5}) : \mathbb{Q}]$ of any compositum is divisible by $2 = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]$ and $3 = [\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}]$, so is divisible by $6 = \mathrm{lcm}(2,3)$. On the other hand, it is at most the product $6 = 2 \cdot 3$ of the two degrees, so is exactly 6. Let's find a sextic over $\mathbb{Q}$ satisfied by α:

$$(\alpha - \sqrt{3})^3 = 5$$

$$\alpha^3 - 3\sqrt{3}\alpha^2 + 3 \cdot 3\alpha - 3\sqrt{3} = 5$$

We move all the square roots to one side,

$$\alpha^3 + 9\alpha - 5 = \sqrt{3} \cdot 3 \cdot (\alpha^2 + 1)$$

And we square both sides:

$$\alpha^6 + 81\alpha^2 + 25 + 18\alpha^4 - 10\alpha^3 - 90\alpha = 27(\alpha^4 + 2\alpha^2 + 1)$$

Rearrange

$$\alpha^6 - 9\alpha^4 - 10\alpha^3 + 27\alpha^2 - 90\alpha - 2 = 0$$

Since α is of degree 6 over $\mathbb{Q}$, the polynomial

$$x^6 - 9x^4 - 10x^3 + 27x^2 - 90x - 2$$

of which α is a zero is irreducible.

Exercise 2. The 5^{th} cyclotomic polynomial $\phi_5(x)$ factors into two irreducible quadratic factors over $\mathbb{Q}(\sqrt{5})$. Find the two irreducible factors.

In the example 19.3.1. it was shown that $\sqrt{5}$ occurs inside $\mathbb{Q}(\zeta)$ with ζ being a primitive fifth root of unity. The discussion of Gauss sums in the proof of quadratic reciprocity gives us: $\zeta - \zeta^2 - \zeta^3 + \zeta^4 = \sqrt{5}$.

We also have that $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$ because $x^2 - 5$ is irreducible in $\mathbb{Q}[x]$ using Eisenstein's criterion and Gauss lemma. We also have that $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$ since $\phi_5(x)$ is irreducible in $\mathbb{Q}[x]$ of degree $5 - 1 = 4$ because of what we saw in 19.3:

In particular, for prime $n = p$, we have already seen that Eisenstein's criterion proves that the p^{th} cyclotomic polynomial $\Phi_p(x)$ is irreducible of degree $\varphi(p) = p - 1$, so

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$$

Now, by multiplicativity of degrees in towers of fields, $[\mathbb{Q}(\zeta) : \mathbb{Q}(\sqrt{5})] = 2$.

Thus, since none of the 4 primitive fifth roots of 1 lies in $\mathbb{Q}(\sqrt{5})$, each is necessarily quadratic over $\mathbb{Q}(\sqrt{5})$, so has a minimal polynomial over $\mathbb{Q}(\sqrt{5})$ which is quadratic. Then, the 4 primitive fifth roots break up into two (disjoint) bunches of 2, grouped by being the 2 roots of the same quadratic over $\mathbb{Q}(\sqrt{5})$. This means that $\phi_5(x)$ factors as the product of those two minimal polynomials (which are necessarily irreducible over $\mathbb{Q}(\sqrt{5})$). To determine the two quadratic polynomials, we start with:

divide through ζ^2

$$\zeta^4+\zeta^3+\zeta^2+\zeta+1=0$$

$$\zeta^2+\zeta+1+\zeta^{-1}+\zeta^{-2}=0$$

regrouping

$$\left(\zeta+\frac{1}{\zeta}\right)^2+\left(\zeta+\frac{1}{\zeta}\right)-1=0$$

Thus, $\varepsilon=\zeta+\dfrac{1}{\zeta}$ satisfies the equation $x^2+x-1=0$, so $\varepsilon=(-1\pm\sqrt{5})/2$. Then,

$$\zeta+\frac{1}{\zeta}=\frac{-1\pm\sqrt{5}}{2}$$

$$\zeta^2-\frac{-1\pm\sqrt{5}}{2}\zeta+1=0$$

So we conclude that:

$$x^4+x^3+x^2+x+1=\left(x^2-\frac{-1+\sqrt{5}}{2}x+1\right)\left(x^2-\frac{-1-\sqrt{5}}{2}x+1\right)$$