

(15.2.2) (Collaboration with Tiffany Jiang)

Since α is a root of f , we get

$$f(\alpha) = 0 = \alpha^n - a_{n-1}\alpha^{n-1} + \cdots \pm a_0.$$

We now get rid of the \pm in front of the constant term a_0 and simplify:

$$\begin{aligned} 0 &= \alpha^n - a_{n-1}\alpha^{n-1} + \cdots + (-1)^n a_0 \\ -(-1)^n a_0 &= \alpha^n - a_{n-1}\alpha^{n-1} + \cdots \\ -(-1)^n a_0 &= \alpha(\alpha^{n-1} - a_{n-1}\alpha^{n-2} + \cdots) \\ (-1)^n(-a_0) &= \alpha(\alpha^{n-1} - a_{n-1}\alpha^{n-2} + \cdots) \end{aligned}$$

By observation, the multiplicative inverse of $(-1)^n$ is still $(-1)^n$. We also know for sure the constant term $a_0 \neq 0$, because otherwise the polynomial f would be reducible. This gives us the existence of a_0^{-1} and:

$$1 = \alpha(\alpha^{n-1} - a_{n-1}\alpha^{n-2} + \cdots)(-1)^n(-a_0^{-1}).$$

Now multiply α^{-1} to both sides of the equation:

$$\alpha^{-1} = (\alpha^{n-1} - a_{n-1}\alpha^{n-2} + \cdots)(-1)^n(-a_0^{-1}).$$

(15.3.1) (Modified during seminar)

Suppose $[F(\alpha) : F] = 5$ and recall that since 5 is prime, if an element β of $F(\alpha)$ is not in F , then $[F(\beta) : F] = 5$ and $F(\alpha) = F(\beta)$. So what we really want to show here is $\alpha^2 \notin F$.

Suppose for the sake of a contradiction that $\alpha^2 \in F$, then there exists an additive inverse $\beta \in F$ for α^2 such that $\alpha^2 + \beta = 0$. This would make α a root of the polynomial $x^2 + \beta$, which is in $F[x]$. So α is algebraic over F , and $[F(\alpha) : F] \leq \deg(x^2 + \beta) = 2$.

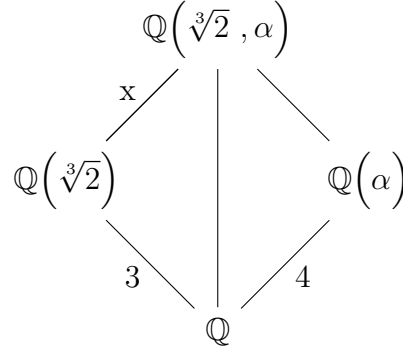
We have reached a contradiction with our initial assumption that $[F(\alpha) : F] = 5$.

Therefore, α^2 generates the same extension as α .

QED

(15.3.2) (Learned during seminar)

One way to show that the polynomial $x^4 + 3x + 3$ is irreducible over $\mathbb{Q}(\sqrt[3]{2})$ is to show that for a root α of $x^4 + 3x + 3$ in an extension field of $\mathbb{Q}(\sqrt[3]{2})$, the irreducible polynomial for α over $\mathbb{Q}(\sqrt[3]{2})$ is degree 4. We draw the following diagram:



We know $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ because $x^3 - 2$ is an integer polynomial that has $\sqrt[3]{2}$ as root.

We also know $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ because $x^4 + 3x + 3$ is irreducible over \mathbb{Q} by Eisenstein Criterion: 3 is the prime that does not divide the leading coefficient, but divides all other coefficients, and $3^2 = 9$ does not divide the constant term.

By the multiplicative property of the degree, it follows $4 \mid 3x$. Moreover, $x \leq 4$.

Hence it is only possible for $x = 4$.

Since $[\mathbb{Q}(\sqrt[3]{2}, \alpha) : \mathbb{Q}(\sqrt[3]{2})] = 4$ and α is algebraic over $\mathbb{Q}(\sqrt[3]{2})$, $x = 4$ is equal to the degree of the irreducible polynomial for α over $\mathbb{Q}(\sqrt[3]{2})$. This shows $x^4 + 3x + 3$ is irreducible over $\mathbb{Q}(\sqrt[3]{2})$.

QED

(15.4.1)

We determine the irreducible polynomial for $\gamma = 1 + \alpha^2$ over \mathbb{Q} by computing powers of γ and looking for a linear relation among them.

Notice that since α is a root of $x^3 - x - 1$, it must be $\alpha^3 - \alpha - 1 = 0$, and after rearranging gives us $\alpha^3 = \alpha + 1$. We will use this identity in both calculations below.

We first compute γ^2 :

$$\begin{aligned}\gamma^2 &= (1 + \alpha^2)^2 \\ &= 1 + 2\alpha^2 + \alpha^4 \\ &= 1 + 2\alpha^2 + \alpha^4 \\ &= 1 + 2\alpha^2 + \alpha \cdot \alpha^3 \\ &= 1 + 2\alpha^2 + \alpha(\alpha + 1) \\ &= 1 + \alpha + 3\alpha^2\end{aligned}\tag{1}$$

We then compute γ^3 :

$$\begin{aligned}\gamma^3 &= (1 + \alpha^2)(1 + \alpha + 3\alpha^2) \\ &= 1 + \alpha + 3\alpha^2 + \alpha^2 + \alpha^3 + 3\alpha^4 \\ &= 1 + \alpha + 4\alpha^2 + \alpha^3 + 3\alpha^4 \\ &= 1 + \alpha + 4\alpha^2 + \alpha + 1 + 3\alpha(\alpha + 1) \\ &= 2 + 5\alpha + 7\alpha^2\end{aligned}\tag{2}$$

We can now clear α and substitute in $\gamma - 1$ for α^2 and make everything in terms of γ :

$$\begin{aligned}\gamma^3 - 5\gamma^2 &= 2 + 5\alpha + 7\alpha^2 - 5(1 + \alpha + 3\alpha^2) \\ &= -3 - 8\alpha^2 \\ &= -3 - 8(\gamma - 1) \\ &= -3 - 8\gamma + 8 \\ &= -8\gamma + 5\end{aligned}$$

Hence $\gamma^3 - 5\gamma^2 + 8\gamma - 5 = 0$ and the irreducible polynomial for $\gamma = 1 + \alpha^2$ over \mathbb{Q} is $x^3 - 5x + 8x - 5$.