HW 11 Solutions

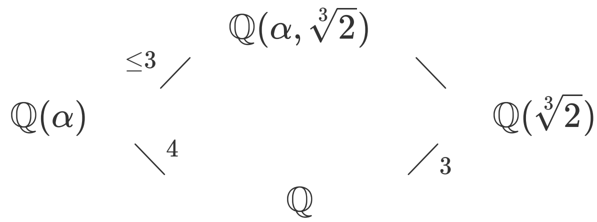
3rd May 2019 at 11:11am

1.

Prove that the polynomial $x^4 + 3x + 3$ is irreducible polynomial over the field $\mathbb{Q}[\sqrt[3]{2}]$. (Hint: Use multiplicative property of degree. In class, we proved $x^3 - 2$ is irreducible in $\mathbb{Q}[\sqrt{2}]$. Similar argument also works here.)

Solution.

Let α be a root of $x^4 + 3x + 3$ in $\mathbb{C}$. Consider the diamond of field extensions:



The polynomials $x^3 - 2$ and $x^4 + 3x + 3$ are irreducible over $\mathbb{Q}$ by Eisenstein's criterion, so

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4, \ [\mathbb{Q}(\sqrt[3]{2})] = 3.$$

These two numbers divide $[\mathbb{Q}(\alpha, \sqrt[3]{2}) : \mathbb{Q}]$, and so $[\mathbb{Q}(\alpha, \sqrt[3]{2}) : \mathbb{Q}] \geq 12.$

On the other hand, the minimal polynomial (aka irreducible polynomial) of α over $\mathbb{Q}(\sqrt[3]{2})$ divides $x^4 + 3x + 3$ and so has degree ≤ 4. Therefore

$$[\mathbb{Q}(\alpha, \sqrt[3]{2}) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\alpha, \sqrt[3]{2}) : \mathbb{Q}] \leq 3 \cdot 4 = 12.$$

So

$$[\mathbb{Q}(\alpha, \sqrt[3]{2}) : \mathbb{Q}] = 12$$

and therefore

$$[\mathbb{Q}(\alpha, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})] = 4.$$

So $x^4 + 3x + 3$ is irreducible over the field $\mathbb{Q}(\sqrt[3]{2})$.

2.

Determine the irreducible polynomial for $\alpha = \sqrt{3} + \sqrt{5}$ over the following fields. (You need to prove why they are the irreducible polynomials)

1. $\mathbb{Q}$
2. $\mathbb{Q}(\sqrt{15})$
3. $\mathbb{Q}(\sqrt[3]{2})$

(Hint: try to use $\pm\sqrt{3} \pm \sqrt{5}$ as the roots of the polynomial to find some polynomial over $\mathbb{Q}$. Use the tower of the field extension to find $[\mathbb{Q}(\sqrt{3}, \sqrt{5})\colon \mathbb{Q}(\sqrt{15})]$ and $[\mathbb{Q}(\sqrt{3}+\sqrt{5}, \sqrt[3]{2})\colon \mathbb{Q}(\sqrt[3]{2})]$.

Solution. Let $\beta = \sqrt{3} - \sqrt{5}$.

First, the polynomial $(x-\alpha)(x+\alpha)(x-\beta)(x+\beta) = x^4 - 16x^2 + 4$ is irreducible over $\mathbb{F}_5$, and so is irreducible over $\mathbb{Z}$ and hence over $\mathbb{Q}$. This is therefore the irreducible polynomial of α over $\mathbb{Q}$.

Next, $[\mathbb{Q}(\sqrt{15}) : \mathbb{Q}] = 2$ so $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{15})] = 2$. Since

$$(x-\alpha)(x+\alpha) = x^2 - (8 + 2\sqrt{15}) \in \mathbb{Q}(\sqrt{15})[x]$$

is of degree 2 and has root α, it is the irreducible polynomial of α over $\mathbb{Q}(\sqrt{15})$.

Finally, by the same reasoning as the solution to Problem 1, we see that $[\mathbb{Q}(\alpha, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})] = 4$, and so $x^4 - 16x^2 + 4$ is the irreducible polynomial of α over $\mathbb{Q}(\sqrt[3]{2})$.

▨

3.

Prove that any quadratic extension of $\mathbb{R}$ is isomorphic to $\mathbb{C}$.

Solution.

Let F be a quadratic extension of $\mathbb{R}$. Pick $\alpha \in F - \mathbb{R}$. Then $F \supseteq \mathbb{R}[\alpha] \supsetneq \mathbb{R}$ so since $[F : \mathbb{R}] = 2$, we have $F = \mathbb{R}[\alpha]$ and so the minimal polynomial of α over $\mathbb{R}$ has the form $f(x) = x^2 + bx + c \in \mathbb{R}[x]$. Then we have isomorphisms:

$$F = \mathbb{R}[\alpha] \cong \frac{\mathbb{R}[x]}{(f(x))} \cong \mathbb{C}.$$

The two isomorphisms above come from applying the first isomorphism theorem to the two evaluation maps

$$\begin{array}{ccccc} \mathbb{R}[x] & \to & \mathbb{R}[\alpha] & \subset F \\ x & \mapsto & \alpha & \end{array}, \qquad \begin{array}{ccc} \mathbb{R}[x] & \to & \mathbb{C} \\ x & \mapsto & \frac{-b+\sqrt{b^2-4c}}{2} \end{array}$$

▨

4.

Prove that the characteristic of a field F is either 0 or a prime number. If it is a prime number p, show that the map $\phi\colon x \mapsto x^p$ gives an injective ring homomorphism from F to itself.

Solution.

The n be the characteristic of a field F, i.e. the least nonnegative integer which generates the kernel of the map $\mathbb{Z} \to F : m \mapsto nm$. By the first isomorphism theorem, this induces an injective ring homomorphism

$$\mathbb{Z}/n\mathbb{Z} \hookrightarrow F.$$

Now F is an integral domain, so $\mathbb{Z}/n\mathbb{Z}$ is also an integral domain, so n is zero or a prime number.

The map ϕ is clearly multiplicative and sends 1 to 1. It is also additive, since $\binom{p}{i} \equiv 0 \pmod{p}$ for $i = 1, \ldots, p-1$ proves that

$$(x+y)^p = x^p + \binom{p}{1} x^{p-1} y + \binom{p}{1} x^{p-1} y + \cdots + \binom{p}{p-1} x y^{p-1} + y^p = x^p + y^p \text{ in } \mathbb{F}_p.$$

Finally $\ker \phi$ is an ideal of F not containing 1. Since F is a field, its only ideals are F and 0, and so $\ker \phi = 0$, so ϕ injects.

▨