Math 542 HW7

Hongtao Zhang

1 13.1

1.1 2

Show that $x^3 - 2x - 2$ is irreducible over $\mathbb{Q}$ and let θ be a root. Computer $(1+\theta)(1+\theta+\theta^2)$ and $\frac{1+\theta}{1+\theta+\theta^2}$ in $\mathbb{Q}(\theta)$.

Solution 1.1.1

$$\begin{aligned}(1+\theta)(1+\theta+\theta^2) &= 1+\theta+\theta^2+\theta+\theta^2+\theta^3\\ &= 1+2\theta+2\theta^2+\theta^3 = 1+2\theta+2\theta^2+2\theta+2\\ &= 3+4\theta+2\theta^2\end{aligned}$$

We want to find the inverse of $(1+\theta+\theta^2)$, thus by euclidean algorithm

$$\begin{aligned}x^3-2x-2 &= (x^2+x+1)(x-1)+(-2x-1)\\ x^2+x+1 &= (-2x-1)\left(-\frac{1}{2}x-\frac{1}{4}\right)+\left(\frac{3}{4}\right)\\ &= (x^3-2x-2-(x^2+x+1)(x-1))\left(-\frac{1}{2}x-\frac{1}{4}\right)+\left(\frac{3}{4}\right)\\ -\frac{3}{4} &= (x^3-2x-2)\left(-\frac{1}{2}x-\frac{1}{4}\right)-(x^2+x+1)\left(\left(-\frac{1}{2}x-\frac{1}{4}\right)(x-1)+1\right)\\ (x^2+x+1)^{-1} &= \frac{4}{3}\left(\left(-\frac{1}{2}x-\frac{1}{4}\right)(x-1)+1\right) = \frac{-2x^2+x+5}{3}\end{aligned}$$

Then

$$\frac{1+\theta}{1+\theta+\theta^2} = -\frac{2\theta^3}{3}-\frac{\theta^2}{3}+2\theta+\frac{5}{3} = -\frac{\theta^2}{3}+\frac{2}{3}\theta+\frac{1}{3}$$

1.2 5

Suppose α is a rational root of a monic polynomial in $\mathbb{Z}[x]$. Prove that α is an integer.

Solution 1.2.1

Suppose $\alpha = \frac{n}{d}$ where $|d| > 1$. The polynomial can be written as

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

Thus

$$\left(\frac{n}{d}\right)^n + a_{n-1}\left(\frac{n}{d}\right)^{n-1} + \ldots + a_1\left(\frac{n}{d}\right) + a_0 = 0$$

$$\begin{aligned} -\left(\frac{n}{d}\right)^n &= a_{n-1}\left(\frac{n}{d}\right)^{n-1} + \ldots + a_1\left(\frac{n}{d}\right) + a_0 \\ &= \frac{b}{d^{n-1}} \end{aligned}$$

for some $b \in \mathbb{Z}$. Since $|d| > 1$, we have reached a contradiction.

2 13.4

2.1 3

Splitting field over $\mathbb{Q}$ for $x^4 + x^2 + 1$.

Solution 2.1.1

$$x^4 + x^2 + 1 = (x^2 - x + 1)(x^2 + x + 1)$$

Thus we can find that it has 4 roots

$$\frac{-1 - i\sqrt{3}}{2}, \frac{1 + i\sqrt{3}}{2}, \frac{1 - i\sqrt{3}}{2}, \frac{-1 + i\sqrt{3}}{2}$$

Thus we have the splitting field

$$\mathbb{Q}(\sqrt{3})$$

2.2 4

Determine the splitting field and its degree over $\mathbb{Q}$ for $x^6 - 4$.

Solution 2.2.1

Note that $x^6 - 4 = 0 \Rightarrow x^6 = 4 \Rightarrow x^6 = \left(\sqrt[6]{4}\right) \cdot 1 = \sqrt[3]{2} \cdot 1$.

Thus the splitting field need to contain all the root of the polynomial, which is

$$\mathbb{Q}\left(\sqrt[3]{2}, \sqrt[3]{2}\zeta(6), \sqrt[3]{2}\zeta(6), \sqrt[3]{2}\zeta(6), \sqrt[3]{2}\zeta(6), \sqrt[3]{2}\zeta(6)\right)$$

The degree is 6.

2.3 5

Let K be a finite extension of F. Prove that K is a splitting field over F if and only if every irreducible polynomial in $F[x]$ that has a root in K splits completely in $K[x]$.

Solution 2.3.1

Denote the polynomial as $p \in F[x]$.

We know that k is a splitting field of p, and thus $k \cong F[x]/p$.

Assume there are two roots α, β in k such that $\alpha \in k$ and $\beta \notin k$.

We know that $F[\alpha] \cong F[x]/p \cong F[\beta]$. Thus we have an isomorphism $\varphi : F[\alpha] \cong F[\beta]$. Consider the splitting field of p denoted as k, thus we have an injective map from $F[\alpha] \hookrightarrow k$, and $F[\beta] \hookrightarrow k$.

Then we consider the algebratic closure of F noted as $\overline{F}$. Automatically we have an isomorphism that extends φ to $\overline{F}$. Restricting φ to k, we have a homomorphism $\overline{\varphi} : k \to k$ that sends $\alpha \mapsto \beta$, which means $\beta \in k$. This is a contradiction.

The other direction follows as definition of splitting field.