

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

By the rational roots theorem if rational roots for  $x^3 + 3x + 1$  exist then they must be of the form  $\pm 1$ . However neither of those are roots. Thus  $x^3 + 3x + 1$  is irreducible over  $\mathbb{Q}$ .

Let  $\theta \in \mathbb{C}$  be a root of  $x^3 + 3x + 1$ . Then for the expression  $(1 + \theta)(1 + \theta + \theta^2)$  we have:

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

For the next expression,  $\frac{1+\theta}{1+\theta+\theta^2}$ , the multiplicative inverse of the bottom  $1+\theta+\theta^2$  is  $\frac{3}{7}\theta^2 - \frac{2}{7}\theta + \frac{8}{7}$ . This can be found by multiplying  $1 + \theta + \theta^2$  by  $(c + b\theta + c\theta^2)$  and extracting a system of linear equations. Then we have:

$$\begin{aligned}\frac{1 + \theta}{1 + \theta + \theta^2} &= (1 + \theta) \left( \frac{3}{7}\theta^2 - \frac{2}{7}\theta + \frac{8}{7} \right) \\ &= \frac{3}{7}\theta^3 + \frac{1}{7}\theta^2 + \frac{6}{7}\theta + \frac{8}{7} \\ &= \frac{1}{7}\theta^2 - \frac{3}{7}\theta + \frac{5}{7}\end{aligned}$$

**Problem 2.** Let  $w = e^{\pi i/6}$  so that  $w^{12} = 1$ , but  $w^k \neq 1$  for  $1 \leq k < 12$ . Find the minimal polynomial  $m_{w,\mathbb{Q}}(x)$  and compute  $[\mathbb{Q}[w] : \mathbb{Q}]$ .

Begin with the polynomial  $x^{12} - 1$  which we now that  $\omega$  is a root of. This factors as

$$x^{12} - 1 = (x^6 - 1)(x^6 + 1)$$

Since  $\omega$  of  $x^6 + 1$  and not the other we continue with it. This factors as

$$x^6 + 1 = (x^2 + 1)(x^4 - x^2 + 1)$$

As before  $x^4 - x^2 + 1$  has  $\omega$  as a root and the other does not. Now we will show that  $x^4 - x^2 + 1$  is irreducible.

By the rational root theorem the only possible rational roots are  $\pm 1$ . However neither of these are roots. The only way  $x^4 - x^2 + 1$  would not be irreducible is if it were the product of quadratics. Now consider  $x^4 - x^2 + 1$  as a polynomial with integer coefficients and suppose that

$$x^4 - x^2 + 1 = (ax^2 + bx + c)(dx^2 + ex + f) = adx^4 + (bd + ae)x^3 + (af + be + cd)x^2 + (bf + ce)x + fc$$

where  $a, b, c, d, e \in \mathbb{Z}$ . This gives us the following system of equations:

$$\begin{aligned}ad &= 1 \\ bd + ae &= 0 \\ af + dc + be &= -1 \\ bf + ce &= 0 \\ fc &= 1\end{aligned}$$

Consider these equations as polynomials in  $\mathbb{C}[a, b, c, d, e, f]$ . Then consider the ideal

$$\langle ad - 1, bd + ae, af + dc + be + 1, bf + ce, fc - 1 \rangle$$

The Gröbner basis for this ideal is  $\langle 1 \rangle$ . Since we are in an algebraically closed field there are no solutions to a set of polynomial equations when the ideal is the whole ring. Thus  $x^4 - x^2 + 1$  is not the product of quadratics and as such  $x^4 - x^2 + 1$  is irreducible.

Therefore  $x^4 - x^2 + 1$  is the minimal polynomial  $m_{\omega, \mathbb{Q}}(x)$  and as such  $[\mathbb{Q}[\omega] : \mathbb{Q}] = 4$ .

**Problem 3.** Compute the minimal polynomial  $m_{\alpha, F}(x)$  where  $\alpha = \sqrt{2} + \sqrt{5}$  and  $F$  is each of the following fields:

$$(a) \mathbb{Q}, \quad (b) \mathbb{Q}[\sqrt{5}], \quad (c) \mathbb{Q}[\sqrt{10}], \quad (d) \mathbb{Q}[\sqrt{15}].$$

(a)

(b)

(c)

(d)

**Problem 4.** Compute the minimal polynomial  $m_{\alpha, \mathbb{Q}}(x)$  where  $\alpha = \sqrt{2} + \sqrt[3]{5}$ .

Consider the polynomial  $f(x) = x^6 - 6x^4 - 10x^3 + 12x^2 - 60x + 17$ . Then  $f(\alpha) = 0$ . Now we wish to show that  $f(x)$  is irreducible. By the rational roots theorem if any rational roots exist then they will be of the form  $\pm 17$  neither of which are roots. Therefore if  $f(x)$  is reducible it will either be the product of two cubics or the product of a quartic and a quadratic.

Suppose that  $f(x)$  was the product of two cubics. Then we would have

$$x^6 - 6x^4 - 10x^3 + 12x^2 - 60x + 17 = (x^3 + ax^2 + bx + c)(x^3 + dx^2 + ex + f)$$

If we multiply out the latter terms we can extract the system of equations

$$\begin{aligned} a + d &= 0 \\ ad + b + e + 6 &= 0 \\ ad + be + c + f + 10 &= 0 \\ af + eb + cd - 12 &= 0 \\ bf + ec + 60 &= 0 \\ cf - 17 &= 0 \end{aligned}$$

If we consider the ideal

$$\langle a + d, ad + b + e + 6, ad + be + c + f + 10, af + eb + cd - 12, bf + ec + 60, cf - 17 \rangle \subset \mathbb{C}[a, b, c, d, e, f]$$

the Gröbner basis of this ideal is  $\langle 1 \rangle$  which implies that there are no solutions to the equation. Thus  $f(x)$  cannot be the product of two cubics.

Similarly suppose that  $f(x)$  was the product of a quartic and a quadratic. Then

$$\begin{aligned} x^6 - 6x^4 - 10x^3 + 12x^2 - 60x + 17 &= (x^4 + ax^3 + bx^2 + cx + d)(x^2 + ex + f) \\ &= x^6 + (a + e)x^5 + (ae + b + f)x^4 + (be + af + c)x^3 + (ce + bf + d)x^2 + (de + cf)x + df \end{aligned}$$

This gives us the system of equations

$$\begin{aligned}a + e &= 0 \\ae + b + f + 6 &= 0 \\be + af + c + 10 &= 0 \\ce + bf + d - 12 &= 0 \\de + cf + 60 &= 0 \\df - 17 &= 0\end{aligned}$$

As before consider the ideal

$$\langle df - 17, de + cf + 60, ce + bf + d - 12, be + af + c + 10, ae + b + f + 6 \rangle \subset \mathbb{C}[a, b, c, d, e, f]$$

The Gröbner basis for this ideal is  $\langle 1 \rangle$  which implies that there are no solutions. Therefore  $f(x)$  cannot be expressed as the product of a quartic and a quadratic.

Therefore  $f(x)$  is irreducible and as such is in fact the minimal polynomial for  $\alpha$ .

**Problem 5.** *If  $K$  is a field extension of the field of  $F$  and  $\alpha \in K$  has a minimal polynomial  $f(x) \in F[x]$  of odd degree, prove that  $F(\alpha) = F(\alpha^2)$ . Determine whether the condition on  $f(x)$  is necessary for  $F(\alpha) = F(\alpha^2)$ .*

*Proof.*

□

**Problem 6.** *6 Let  $K$  be an extension field of  $F$  that is algebraic over  $F$ . Show that any subring  $R$  of  $K$  which contains  $F$ , i.e.,  $F \subseteq R \subseteq K$ , is a field. Hence, prove that any subring of a finite dimensional extension field  $K/F$  containing  $F$  is a subfield.*

*Proof.*

□

**Problem 7.** *7 Suppose that  $K = F(\alpha)$  is a finite simple extension of the field  $F$ . Define an  $F$ -linear transformation  $T_\alpha : K \rightarrow K$  by  $T_\alpha(\beta) = \alpha\beta$  for all  $\beta \in K$ . Show that the minimal polynomial of  $\alpha$  over  $F$  is the characteristic polynomial of  $T_\alpha$ , that is*

$$m_{\alpha, F}(x) = \det(xI - T_\alpha).$$

*Proof.*

□