Math 121 Homework 7: Notes on Selected Problems

13.1.1. Show that $p(x) = x^3 + 9x + 6$ is irreducible in $\mathbf{Q}[x]$. Let θ be a root of $p(x)$. Find the inverse of $1 + \theta$ in $\mathbf{Q}(\theta)$.

Solution. The rational roots test implies that the possible rational roots of $p(x)$ are $\pm 1, \pm 2, \pm 3, \pm 6$. Evaluate $p(x)$ to see that none of these are roots.[1] A cubic is reducible if and only if it has linear factors so $p(x)$ is irreducible in $\mathbf{Q}[x]$.

We use the Euclidean algorithm to express 11 as a linear combination of the relatively prime polynomials $x^3 + 9x + 6$ and $x + 1$. Long division (in LaTeX you can `\usepackage{polynom}` and then type `\polylongdiv{x^3+9x+6}{x+1}` to typeset the following calculation) gives

$$\begin{array}{r|l} & x^2 - x + 10 \\ \hline x+1 & x^3 + 9x + 6 \\ & -x^3 - x^2 \\ \hline & \quad -x^2 + 9x \\ & \quad\ x^2 + x \\ \hline & \qquad 10x + 6 \\ & \qquad -10x - 10 \\ \hline & \qquad\quad -4 \end{array}$$

so

$$-\tfrac{1}{4}(x^3 + 9x + 6) + \tfrac{1}{4}(x^2 - x + 10)(x + 1) = 1.$$

Therefore $(1 + \theta)^{-1} = \frac{1}{4}(\theta^2 - \theta + 10)$. □

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

Solution. The polynomial $x^3 - 2x - 2$ is irreducible by Eisenstein's criterion with the prime 2. (Alternatively, by the rational roots test, the only possible rational roots of $x^3 - 2x - 2$ are $\pm 1, \pm 2$, but none of these are roots.)

Using the relation $\theta^3 = 2\theta + 2$ we compute

$$(1 + \theta)(1 + \theta + \theta^2) = 1 + 2\theta + 2\theta^2 + \theta^3 = 3 + 4\theta + 2\theta^2.$$

[1] In this case, a simple argument shows that no integer (or positive real number) can be a root of $p(x)$. The coefficients of $p(x)$ are positive so no positive real number is a root of $p(x)$. For any integer x, $x(x^2 + 9)$ has absolute value greater than 6, but $p(x) = x(x^2 + 9) + 6$ so no integer is a root of $p(x)$.

We compute

$$\begin{array}{r|l} & x-1 \\ \hline x^2+x+1) & x^3 \quad -2x-2 \\ & -x^3-x^2-x \\ \hline & -x^2-3x-2 \\ & x^2+x+1 \\ \hline & -2x-1 \end{array}$$

and

$$\begin{array}{r|l} & -\frac{1}{2}x-\frac{1}{4} \\ \hline -2x-1) & x^2+x+1 \\ & -x^2-\frac{1}{2}x \\ \hline & \frac{1}{2}x+1 \\ & -\frac{1}{2}x-\frac{1}{4} \\ \hline & \frac{3}{4} \end{array}$$

so

$$x^2+x+1-\big(x^3-2x-2-(x-1)(x^2+x+1)\big)(-\tfrac{1}{2}x-\tfrac{1}{4}) = 3/4$$

or

$$(\tfrac{1}{2}x+\tfrac{1}{4})(x^3-2x-2)+\big[-\tfrac{1}{2}x^2+\tfrac{1}{4}x+\tfrac{5}{4}\big](x^2+x+1) = 3/4.$$

Then

$$\big[\tfrac{2}{3}x^2+x+\tfrac{1}{3}\big](x^3-2x-2) + \big[-\tfrac{2}{3}x^3-\tfrac{1}{3}x^2+2x+\tfrac{5}{3}\big](x^2+x+1) = 1+x$$

so $\frac{1+\theta}{1+\theta+\theta^2} = -\frac{2}{3}\theta^3-\frac{1}{3}\theta^2+\frac{2}{3}\theta+\frac{5}{3}$, that is $\frac{1+\theta}{1+\theta+\theta^2} = -\frac{1}{3}\theta^2-\frac{2}{3}\theta+\frac{1}{3}$. □

13.1.3. Show that x^3+x+1 is irreducible over $\mathbf{F}_2$ and let θ be a root. Compute the powers of θ in $\mathbf{F}_2(\theta)$.

Solution. Neither 0 nor 1 is a root of x^3+x+1 in $\mathbf{F}_2$. A cubic is reducible if and only if it has a linear factor so x^3+x+1 is irreducible over $\mathbf{F}_2$. We compute

$$\begin{aligned} \theta^3 &= -\theta-1 = \theta+1 \\ \theta^4 &= \theta^2+\theta \\ \theta^5 &= \theta^3+\theta^2 = \theta^2+\theta+1 \\ \theta^6 &= \theta^3+\theta^2+\theta = \theta^2+1 \\ \theta^7 &= \theta^3+\theta = 1 \end{aligned}$$

so

$$\theta^i = \begin{cases} 1 & \text{if } i \equiv 0 \pmod 7 \\ \theta & \text{if } i \equiv 1 \pmod 7 \\ \theta^2 & \text{if } i \equiv 2 \pmod 7 \\ \theta + 1 & \text{if } i \equiv 3 \pmod 7 \\ \theta^2 + \theta & \text{if } i \equiv 4 \pmod 7 \\ \theta^2 + \theta + 1 & \text{if } i \equiv 5 \pmod 7 \\ \theta^2 + 1 & \text{if } i \equiv 6 \pmod 7 \end{cases}$$

are the powers of θ in $\mathbf{F}_2(\theta)$. □

13.2.2. Let $g(x) = x^2 + x - 1$ and let $h(x) = x^3 - x + 1$. Obtain fields of $4, 8, 9$ and 27 elements by adjoining a root of $f(x)$ to the field F where $f(x) = g(x)$ or $h(x)$ and $F = \mathbf{F}_2$ or $\mathbf{F}_3$. Write down the multiplication tables for the fields with 4 and 9 elements and show that the nonzero elements form a cyclic group.

Solution. The polynomials $g(x)$ and $h(x)$ do not have roots in $\mathbf{F}_2$ or $\mathbf{F}_3$ and are of degree at most 3 so are irreducible over $\mathbf{F}_2$ and $\mathbf{F}_3$. Then $\mathbf{F}_2[x]/g(x)$, $\mathbf{F}_2[x]/h(x)$, $\mathbf{F}_3[x]/g(x)$, $\mathbf{F}_3[x]/h(x)$ are fields with $4, 8, 9, 27$ elements, respectively, as can be seen by considering the degree over the base field.

Let α and β be the images of x in $\mathbf{F}_2[x]/g(x)$ and $\mathbf{F}_3[x]/g(x)$, respectively. Then $\alpha^2 = -\alpha + 1 = \alpha + 1$ and $\beta^2 = -\beta + 1$. Using these relations we may compute the multiplication table for $\mathbf{F}_2[x]/g(x)$:

	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

and the multiplication table for $\mathbf{F}_3[x]/g(x)$:

	0	1	-1	β	$1+\beta$	$-1+\beta$	$-\beta$	$1-\beta$	$-1-\beta$
0	0	0	0	0	0	0	0	0	0
1	0	1	-1	β	$1+\beta$	$-1+\beta$	$-\beta$	$1-\beta$	$-1-\beta$
-1	0	-1	1	$-\beta$	$-1-\beta$	$1-\beta$	β	$-1+\beta$	$1+\beta$
β	0	β	$-\beta$	$1-\beta$	1	$1+\beta$	$-1+\beta$	$-1-\beta$	-1
$1+\beta$	0	$1+\beta$	$-1-\beta$	1	$-1+\beta$	$-\beta$	-1	β	$1-\beta$
$-1+\beta$	0	$-1+\beta$	$1-\beta$	$1+\beta$	$-\beta$	-1	$-1-\beta$	1	β
$-\beta$	0	$-\beta$	β	$-1+\beta$	-1	$-1-\beta$	$1-\beta$	$1+\beta$	1
$1-\beta$	0	$1-\beta$	$-1+\beta$	$-1-\beta$	β	1	$1+\beta$	-1	$-\beta$
$-1-\beta$	0	$-1-\beta$	$1+\beta$	-1	$1-\beta$	β	1	$-\beta$	$-1+\beta$

.

To show that the respective multiplicative groups of we show there is an element with multiplicative order equal to the number of nonzero elements. In $\mathbf{F}_2[x]/g(x)$ we may take α (or $1+\alpha$) of multiplicative order 3. Similarly in $\mathbf{F}_3[x]/g(x)$, we seek an element of order 8. From the diagonal of the multiplication table, we see that -1 is the unique nontrivial square root of 1. Both of $-1+\beta$ and $1-\beta$ are square roots of -1. The square roots of $-1+\beta$ are $1+\beta$ and $-1-\beta$ and the square roots of $1-\beta$ are β and $-\beta$. Thus each of $1+\beta$, $-1-\beta$, β, and $-\beta$ have multiplicative order 8.[2] □

13.2.3. Determine the minimal polynomial over $\mathbf{Q}$ for the element $1+i$.

Solution. Conjugation shows that any polynomial with real coefficients and root $a+\mathrm{i}b$ must also have root $a-\mathrm{i}b$. So $1-\mathrm{i}$ is also a root of the minimal polynomial of $1+\mathrm{i}$, and $(x-(1+i))(x-(1-i)) = x^2-2x+2$ must divide the minimal polynomial of $1+\mathrm{i}$. Since $1+\mathrm{i}$ is not in $\mathbf{Q}$, this is the polynomial of smallest degree with rational coefficients and root $1+\mathrm{i}$. Finally, the minimal polynomial of $1+\mathrm{i}$ is x^2-2x+2. □

13.2.4. Determine the degree over $\mathbf{Q}$ of $2+\sqrt{3}$ and of $1+\sqrt[3]{2}+\sqrt[3]{4}$.

Solution. The degree over $\mathbf{Q}$ of $\mathbf{Q}(2+\sqrt{3}) = \mathbf{Q}(\sqrt{3})$ is 2 since $\sqrt{2}$ has minimal polynomial x^2-2. Similarly the degree over $\mathbf{Q}$ of $\mathbf{Q}(1+\sqrt[3]{2}+\sqrt[3]{4}) = \mathbf{Q}(\sqrt[3]{2})$ (note that $\sqrt[3]{4} = (\sqrt[3]{2})^2$) is 3 since $\sqrt[3]{2}$ has minimal polynomial x^3-2. □

Note. Irreducibility of the minimal polynomials can be seen either by the Eisenstein criterion or the rational roots test.

13.2.7. Prove that $\mathbf{Q}(\sqrt{2}+\sqrt{3}) = \mathbf{Q}(\sqrt{2},\sqrt{3})$. Conclude that $[\mathbf{Q}(\sqrt{2}+\sqrt{3}) : \mathbf{Q}] = 4$. Find an irreducible polynomial satisfied by $\sqrt{2}+\sqrt{3}$.

---

[2] In general, a finite subgroup of the multiplicative group of a field must be cyclic: Let d be the natural number generating the annihilator of the finite abelian subgroup considered as a $\mathbf{Z}$-module. There exists an element of the subgroup with order precisely d. (This follows by showing that the set of orders is closed under taking the least common multiple. Alternatively consider the structure theorem, invariant factor form, for finite abelian groups.) All of the elements of the subgroup are elements of the field satisfying $x^d-1=0$, of which there are at most d. Therefore the order of the subgroup is at most d, but it contains at least one element of order d so it must be cyclic of order d.

Solution. Since $\sqrt{2}+\sqrt{3}$ is a $\mathbf{Q}$-linear combination of the generators $\sqrt{2}$ and $\sqrt{3}$ of $\mathbf{Q}(\sqrt{2},\sqrt{3})$, $\mathbf{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbf{Q}(\sqrt{2},\sqrt{3})$. Since

$$(\sqrt{2}+\sqrt{3})^3 = 11\sqrt{2}+9\sqrt{3},$$

$\mathbf{Q}(\sqrt{2}+\sqrt{3})$ contains each of $\sqrt{2}$ and $\sqrt{3}$. Explicitly,

$$\sqrt{2} = [(\sqrt{2}+\sqrt{3})^3 - 9(\sqrt{2}+\sqrt{3})]/2$$

and

$$\sqrt{3} = [(\sqrt{2}+\sqrt{3})^3 - 11(\sqrt{2}+\sqrt{3})]/(-2).$$

Therefore $\mathbf{Q}(\sqrt{2}+\sqrt{3}) = \mathbf{Q}(\sqrt{2},\sqrt{3})$.

Note that $\sqrt{3}$ is not in $\mathbf{Q}(\sqrt{2})$, but is a root of the polynomial $x^2-3=0$ with coefficients in $\mathbf{Q}(\sqrt{2})$ so $[\mathbf{Q}(\sqrt{2},\sqrt{3}):\mathbf{Q}(\sqrt{2})] = 2$. Also $[\mathbf{Q}(\sqrt{2}):\mathbf{Q}] = 2$ so by multiplicativity of degrees $[\mathbf{Q}(\sqrt{2},\sqrt{3}):\mathbf{Q}] = 4$ and thus $[\mathbf{Q}(\sqrt{2}+\sqrt{3}):\mathbf{Q}] = 4$.

An ordered $\mathbf{Q}$-basis for $\mathbf{Q}(\sqrt{2},\sqrt{3})$ is given by $(1,\sqrt{2},\sqrt{3},\sqrt{6})$. With respect to this basis, multiplication by $\sqrt{2}+\sqrt{3}$ has matrix

$$\begin{bmatrix} 0 & 2 & 3 & 0 \\ 1 & 0 & 0 & 3 \\ 1 & 0 & 0 & 2 \\ 0 & 1 & 1 & 0 \end{bmatrix}.$$

This endomorphism satisfies its characteristic polynomial:

$$\lambda^4 - 10\lambda^2 + 1$$

so $\sqrt{2}+\sqrt{3}$ is a root of x^4-10x^2+1, and this polynomial is irreducible by the rational roots test. Alternatively, by Galois theoretic considerations, the minimal polynomial is

$$(x-(\sqrt{2}+\sqrt{3}))(x-(\sqrt{2}-\sqrt{3}))(x-(-\sqrt{2}+\sqrt{3}))(x-(-\sqrt{2}-\sqrt{3})). \quad \square$$

13.2.8. Let F be a field of characteristic $\neq 2$. Let D_1 and D_2 be elements of F, neither of which is a square in F. Prove that $F(\sqrt{D_1},\sqrt{D_2})$ is of degree 4 over F if and only if D_1D_2 is not a square in F and is of degree 2 over F otherwise. When $F(\sqrt{D_1},\sqrt{D_2})$ is of degree 4 over F the field is called a *biquadratic extension of* F.

Solution. Assume that $\sqrt{D_2}$ is in $F(\sqrt{D_1})$, say $\sqrt{D_2} = a + b\sqrt{D_1}$ for a and b in F. Necessarily b is nonzero since D_2 is not a square in F. Rearranging and squaring gives $a^2 = D_2 + b^2D_1 - 2b\sqrt{D_1D_2}$. Since the characteristic of F is not 2 and b is not zero, D_1D_2 must be a square

in F. Conversely, if D_1D_2 is a square in F, $\sqrt{D_2} = \frac{\sqrt{D_1D_2}}{D_1}\sqrt{D_1}$ (D_1 is nonzero since it is not a square in F) so $\sqrt{D_2}$ is in $F(\sqrt{D_1})$. Therefore

$$[F(\sqrt{D_1},\sqrt{D_2}) : F(\sqrt{D_1})] = \begin{cases} 1 & \text{if } D_1D_2 \text{ is a square in } F \\ 2 & \text{if } D_1D_2 \text{ is not a square in } F \end{cases}$$

and so by multiplicativity of degrees,

$$[F(\sqrt{D_1},\sqrt{D_2}) : F] = \begin{cases} 2 & \text{if } D_1D_2 \text{ is a square in } F \\ 4 & \text{if } D_1D_2 \text{ is not a square in } F. \end{cases}$$ □

13.2.10. Determine the degree of the extension $\mathbf{Q}(\sqrt{3+2\sqrt{2}})$ over $\mathbf{Q}$.

Solution. Attempting to write $\sqrt{3+2\sqrt{2}} = \sqrt{\alpha}+\sqrt{\beta}$ we see that we must have $\alpha+\beta = 3$ and $4\alpha\beta = 8$. Therefore we could take $\alpha = 1$ and $\beta = 2$ (or the reverse). Thus $\sqrt{3+\sqrt{2}} = 1+\sqrt{2}$ so the degree of the extension $\mathbf{Q}(\sqrt{3+2\sqrt{2}}) = \mathbf{Q}(\sqrt{2})$ over $\mathbf{Q}$ is 2.

You could also set $y = \sqrt{3+2\sqrt{2}}$ and eliminate radicals to obtain $y^2 = 3+2\sqrt{2}$ and $(y^2-3)^2 = 8$ or y^4-6y^2+1. This polynomial is reducible:

$$\begin{aligned} y^4-6y^2+1 &= y^4-2y^2+1-4y^2 \\ &= (y^2-1)^2-(2y)^2 \\ &= (y^2-2y-1)(y^2+2y-1), \end{aligned}$$

so the degree of the extension is 2. □

Problem 2. Let α be a root of $\alpha^3-\sqrt{2}\,\alpha+1$. Write down a polynomial P with rational coefficients so that $P(\alpha) = 0$. Express α^{-1} as a $\mathbf{Q}$-linear combination of $1, \alpha, \alpha^2, \ldots$.

Solution. Note that

$$(\alpha^3-\sqrt{2}\,\alpha+1)(\alpha^3+\sqrt{2}\,\alpha+1) = \alpha^6+2\alpha^3-2\alpha^2+1$$

has rational coefficients so we may let $P(t) = t^6+2t^3-2t^2+1$.[3]

[3]The group $\mathrm{Aut}(\mathbf{Q}(\sqrt{2})/\mathbf{Q})$ of automorphisms of $\mathbf{Q}(\sqrt{2})$ that restrict to the identity on $\mathbf{Q}$ (every field automorphism restricts to the identity on the prime subfield so this condition is vacuous) acts on $\mathbf{Q}(\sqrt{2})[x]$ by acting on the coefficients. For every element of $\mathbf{Q}(\sqrt{2})$ not in $\mathbf{Q}$, there exists an element of $\mathrm{Aut}(\mathbf{Q}(\sqrt{2})/\mathbf{Q})$ that does not fix this element. Therefore an element of $\mathbf{Q}(\sqrt{2})[x]$ is in $\mathbf{Q}[x]$ if and only if it is fixed by every element of $\mathrm{Aut}(\mathbf{Q}(\sqrt{2})/\mathbf{Q})$. Thus we have a map $\varphi\colon \mathbf{Q}(\sqrt{2})[x] \to \mathbf{Q}[x]$ taking $f(x)$ to $\prod \sigma(f(x))$ where the product is over all σ in $\mathrm{Aut}(\mathbf{Q}(\sqrt{2})/\mathbf{Q})$. Any $f(x)$ in $\mathbf{Q}(\sqrt{2})[x]$ divides $\varphi(f(x))$ in $\mathbf{Q}(\sqrt{2})[x]$ so if β is a root of $f(x)$, then it is also a root of $\varphi(f(x))$. Since $(\sqrt{2})^2-2 = 0$, for any σ in $\mathrm{Aut}(\mathbf{Q}(\sqrt{2})/\mathbf{Q})$, $(\sigma(\sqrt{2}))^2-2 = 0$ and so $\sigma(\sqrt{2}) = \pm\sqrt{2}$. Therefore $\mathrm{Aut}(\mathbf{Q}(\sqrt{2})/\mathbf{Q})$

From $1 = -\alpha^6 - 2\alpha^3 + 2\alpha^2$ we obtain $\alpha^{-1} = -\alpha^5 - 2\alpha^2 + 2\alpha$. □

Note. The above solution was motivated by Galois theory. In this case a direct solution is also available. Square the equation $\sqrt{2}\,\alpha = \alpha^3 + 1$ to get $2\alpha^2 = \alpha^6 + 2\alpha^3 + 1$ so $\alpha^6 + 2\alpha^3 - 2\alpha^2 + 1 = 0$.

Problem 3. Let α be a root of $x^3 + x + 1 = 0$. Compute the minimum polynomial m of $1 + \alpha + \alpha^2$ and prove that $\mathbf{Q}[t]/(m)$ is isomorphic to $\mathbf{Q}[x]/(x^3 + x + 1)$.

Solution. Note that $x^3 + x + 1$ is indeed irreducible over $\mathbf{Q}$ since it is cubic and has no rational roots. Thus the kernel of the $\mathbf{Q}$-linear map $\mathbf{Q}[t] \to \mathbf{Q}[x]/(x^3 + x + 1)$ sending t to $x^2 + x + 1$ is generated by $m(t)$, the minimal polynomial of $\alpha^2 + \alpha + 1$. The induced map is an imbedding $\mathbf{Q}[t]/(m(t)) \hookrightarrow \mathbf{Q}[x]/(x^3+x+1)$.[4] In particular, the degree of $m(t)$ is at most 3. Then $1+\alpha+\alpha^2$ satisfies a monic polynomial with rational coefficients of degree 3. Let $p(t) = t^3 + a_1t^2 + a_2t + a_3$ be a monic rational cubic polynomial. Using the relation $\alpha^3 = -\alpha-1$ we can reduce $p(1 + \alpha + \alpha^2)$ to a quadratic polynomial in α with coefficients in $\mathbf{Z}[a_1, a_2, a_3]$ as follows. We compute

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

---

consists of the identity and the transposition $\sqrt{2} \mapsto -\sqrt{2}$. For the given case, we took $P(x)$ to be the image under φ of $x^3 - \sqrt{2}\,x + 1$.

[4] We may immediately conclude, without computing the minimal polynomial, that the field extension $\mathbf{Q}[t]/(m(t)) \hookrightarrow \mathbf{Q}[x]/(x^3 + x + 1)$ is an isomorphism as follows. The degree of $\mathbf{Q}[t]/(m(t))$ over $\mathbf{Q}$ divides the degree of $\mathbf{Q}[x]/(x^3+x+1)$ over $\mathbf{Q}$ by multiplicativity of degrees. Therefore $m(t)$ either has degree 1 or 3. The degree of $m(t)$ must be greater than 1 since the ideal generated by $x^3 + x + 1$ in $\mathbf{Q}[x]$ does not contain any quadratic polynomials and in particular does not contain any linear polynomial of $x^2 + x + 1$. The degree of $m(t)$ is thus 3 and the result follows.

and so

$$\begin{aligned} & p(1+\alpha+\alpha^2) \\ &= a_3 + a_2(1+\alpha+\alpha^2) + a_1(-1-\alpha+2\alpha^2) + (-2-5\alpha-2\alpha^2) \\ &= (-2-a_1+a_2+a_3) + (-5-a_1+a_2)\alpha + (-2+2a_1+a_2)\alpha^2. \end{aligned}$$

Since x^3+x+1 is irreducible over $\mathbf{Q}$, $\{1,\alpha,\alpha^2\}$ is independent over $\mathbf{Q}$. Thus the equation $p(1+\alpha+\alpha^2)=0$ is equivalent to the system of linear equations

$$\begin{cases} 2 = -a_1 + a_2 + a_3 \\ 5 = -a_1 + a_2 \\ 2 = 2a_1 + a_2 \end{cases}$$

that has unique solution $(a_1,a_2,a_3) = (-1,4,-3)$. Hence the unique monic cubic polynomial with rational coefficients with root $1+\alpha+\alpha^2$ is t^3-t^2+4t-3, and so $m(t) = t^3-t^2+4t-3$. Finally, since $m(t)$ has degree 3, the imbedding $\mathbf{Q}[t]/(m(t)) \hookrightarrow \mathbf{Q}[x]/(x^3+x+1)$ is an isomorphism. □

Note. An alternative method to compute the minimal polynomial of $1+\alpha+\alpha^2$ is as follows. Using $\alpha^3 = -\alpha - 1$ we compute

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

so with respect to the ordered $\mathbf{Q}$-basis $(1,\alpha,\alpha^2)$ of $\mathbf{Q}(\alpha)$, multiplication by $1+\alpha+\alpha^2$ has matrix

$$\begin{bmatrix} 1 & -1 & -1 \\ 1 & 0 & -2 \\ 1 & 1 & 0 \end{bmatrix}.$$

The characteristic polynomial

$$\begin{aligned} -\det \begin{bmatrix} 1-\lambda & -1 & -1 \\ 1 & -\lambda & -2 \\ 1 & 1 & -\lambda \end{bmatrix} &= -[(1-\lambda)(\lambda^2+2) - (\lambda+1) + 2 - \lambda] \\ &= \lambda^3 - \lambda^2 + 4\lambda - 3 \end{aligned}$$

is at least divisible by the desired minimal polynomial and in this case is irreducible and so equals the desired minimal polynomial.

Problem 4. Write down all the irreducible polynomials of degree 5 over $\mathbf{Z}/2\mathbf{Z}$.

Solution. The linear polynomials x and $x+1$ are irreducible over $\mathbf{Z}/2\mathbf{Z}$. An irreducible polynomial over $\mathbf{Z}/2\mathbf{Z}$ of degree greater than 1 must have nonzero constant coefficient so that 0 is not a root and the sum of the coefficients must be nonzero so that 1 is not a root. Reducible polynomials of degree 2 and 3 must have a root so in these cases the above conditions are sufficient. The only irreducible quadratic polynomial is x^2+x+1 and the irreducible cubic polynomials are

$$x^3+x+1 \qquad \text{and} \qquad x^3+x^2+1.$$

The reducible quintic polynomials without roots are then

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

so the irreducible quintic polynomials over $\mathbf{Z}/2\mathbf{Z}$ are

$$\begin{gathered} x^5+x^2+1, x^5+x^3+1, \\ x^5+x^3+x^2+x+1, x^5+x^4+x^2+x+1, \\ x^5+x^4+x^3+x+1, x^5+x^4+x^3+x^2+1. \quad \square \end{gathered}$$

Problem 5. Assume that $f \in \mathbf{Q}[x]$. Explain how to test *in a finite time* whether or not f is irreducible. Your procedure need not be particularly efficient; it should just be clear that it always terminates in finite time.

Solution. First note that by Gauss's lemma, a polynomial with rational coefficients is reducible if and only if the associated primitive integer polynomial is a product of integer polynomials of smaller positive degree. To show that the latter can be tested in finite time, we find an exhaustive finite set of integer polynomial divisors of a polynomial in terms of its coefficients and degree.

We first show that the roots in the complex numbers of the polynomial $f(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0$ with $a_i \in \mathbf{C}$ and $a_n \neq 0$ are all in the interior of the circle of radius $1 + (\max_{1 \leq i \leq n-1} |a_i|)/|a_n|$

centered at the origin. For $|z| > 1$ we estimate

$$\begin{aligned}
|f(z)| &\geq |a_n|\,|z|^n - (\max_{1\leq i\leq n-1}|a_i|)(|z|^{n-1} + |z|^{n-2} + \cdots + |z| + 1) \\
&= |z|^n(|a_n| - (\max_{1\leq i\leq n-1}|a_i|)(|z|^{-1} + |z|^{-2} + \cdots + |z|^{-n})) \\
&> |z|^n(|a_n| - (\max_{1\leq i\leq n-1}|a_i|)(|z|^{-1} + |z|^{-2} + \cdots)) \\
&= |z|^n(|a_n| - (\max_{1\leq i\leq n-1}|a_i|)(|z| - 1)^{-1}) \\
&= |z|^n(|z| - 1)^{-1}(|a_n|(|z| - 1) - (\max_{1\leq i\leq n-1}|a_i|))
\end{aligned}$$

so $f(z) \neq 0$ when $|z| \geq 1 + (\max_{1\leq i\leq n-1}|a_i|)/|a_n|$, as desired. In particular, for any choice of k of the n roots of $f(z)$, the degree ℓ elementary symmetric polynomial in these roots has absolute value bounded by

$$M_{k,\ell} = \binom{k}{\ell}(1 + (\max_{1\leq i\leq n-1}|a_i|)/|a_n|)^{\ell}.$$

Now assume that $f(x)$ is a degree n element of $\mathbf{Z}[x]$. A degree d divisor in $\mathbf{Z}[x]$ of $f(x)$ has leading coefficient divisor b of a_n and z^m coefficient, for $m < d$, equal to the leading coefficient times a degree $d - m$ elementary symmetric polynomials in d of the roots of $f(x)$, which must therefore lie in the range $(-|b|M_{d,d-m}, +|b|M_{d,d-m})$. We have produced an exhaustive list of possible divisors of $f(x)$ in $\mathbf{Z}[x]$ that is finite, of cardinality

$$\sum_{d=0}^{n}\sum_{b|a_n}\prod_{m=0}^{d-1}(2\lceil |b|M_{d,d-m}\rceil - 1).$$

To test if a given polynomial of degree n with rational coefficients is reducible, we check if the associated primitive integer polynomial is divisible by any of the candidate divisors. (If the given polynomial is of degree n, it is sufficient to check just those candidate divisors of positive degree at most $\lfloor n/2 \rfloor$.) The given polynomial with rational coefficients is reducible if and only if the associated primitive integer polynomial is divisible by one of the candidate divisors, of which there are finitely many. □