

## Tutorial 8

1. A complex number  $\alpha$  is called an *algebraic integer* if it is a root of a monic polynomial  $f(x) \in \mathbb{Z}[x]$ . (A polynomial is called *monic* if its leading coefficient is 1). Show that if  $\alpha \in \mathbb{Q}$  is an algebraic integer then  $\alpha \in \mathbb{Z}$ . (Use the Rational Roots Theorem.)

*Solution.*

Suppose that  $\alpha \in \mathbb{Q}$  is an algebraic integer, and let  $\sum_{i=0}^d a_i x^i \in \mathbb{Z}[x]$  be a monic polynomial of which  $\alpha$  is a root. By the Rational Roots Theorem there exist integers  $p$  and  $q$  such that  $p|a_0$  and  $q|a_d$ , and  $\alpha = p/q$ . But  $a_d = 1$  since the polynomial is monic; so  $q = \pm 1$ , and  $\alpha = \pm p \in \mathbb{Z}$ .

2. Find a nonzero polynomial  $f(x) \in \mathbb{Q}[x]$  of which  $\sqrt{3} + \sqrt{2}$  is a root. (Hint: make a guess as to three other real numbers which will also be roots of any such polynomial in  $\mathbb{Q}[x]$ .)

*Solution.*

$$\begin{aligned} & (x - \sqrt{3} - \sqrt{2})(x - \sqrt{3} + \sqrt{2})(x + \sqrt{3} - \sqrt{2})(x + \sqrt{3} + \sqrt{2}) \\ &= ((x - \sqrt{3})^2 - 2)((x + \sqrt{3})^2 - 2) \\ &= (x^2 + 1 - 2\sqrt{3}x)(x^2 + 1 + 2\sqrt{3}x) \\ &= ((x^2 + 1)^2 - 12x^2) = x^4 - 10x^2 + 1. \end{aligned}$$

3. Let  $\alpha \in \mathbb{C}$  be a root of  $x^3 + 2x + 2 \in \mathbb{Q}[x]$ , and  $\beta \in \mathbb{C}$  a root of  $x^3 - 6x + 3 \in \mathbb{Q}[x]$ . Show that  $\alpha + \beta$  is a root of a polynomial  $f(x) \in \mathbb{Q}[x]$  of degree at most nine. (Hint: show that the elements  $\alpha^i \beta^j$  with  $i, j \in \{0, 1, 2\}$  span a finite dimensional  $\mathbb{Q}$ -subspace of  $\mathbb{C}$  which is closed under multiplication, and in particular contains all the powers of  $\alpha + \beta$ .)

*Solution.*

Since  $\mathbb{C}$  is a vector space over  $\mathbb{Q}$ , any finite subset of  $\mathbb{C}$  spans a finite-dimensional  $\mathbb{Q}$ -subspace of  $\mathbb{C}$ . So the set

$$E = \left\{ \sum_{i,j \in \{0,1,2\}} \lambda_{ij} \alpha^i \beta^j \mid \lambda_{ij} \in \mathbb{Q} \right\}$$

is certainly a  $\mathbb{Q}$ -subspace of dimension at most 9. Since  $\alpha^3 = -2\alpha - 2$  we see that  $\alpha^4 = -2\alpha^2 - 2\alpha$ , and similarly we have  $\beta^3 = 6\beta - 3$  and  $\beta^4 = 6\beta^2 - 3\beta$ . So if  $i, j \in \{0, 1, 2, 3, 4\}$  then  $\alpha^i \beta^j \in E$ ; for example,  $\alpha^4 \beta^4 = -12\alpha^2 \beta^2 + 6\alpha^2 \beta - 12\alpha \beta^2 + 6\alpha \beta$ , and  $\alpha \beta^3 = 6\alpha \beta - 3\alpha$ . But the product of any pair of elements of  $E$  will be a  $\mathbb{Q}$ -linear combination of products  $(\alpha^{i_1} \beta^{j_1})(\alpha^{i_2} \beta^{j_2})$  where  $i_1, j_1, i_2, j_2 \in \{0, 1, 2\}$ , and hence is a  $\mathbb{Q}$ -linear combination of elements  $\alpha^i \beta^j$  with  $i, j \in \{0, 1, 2, 3, 4\}$ , and hence is in  $E$ . Thus  $E$  is closed under multiplication.

If  $\gamma$  is any element of  $E$  then since  $E$  has dimension at most 9 the 10 elements  $\gamma^i$  for  $0 \leq i \leq 9$  must be linearly dependent (as they are all in  $E$  in view of closure of  $E$  under multiplication). So there exist scalars  $\lambda_i \in \mathbb{Q}$  which are not all 0 such that  $\sum_{i=0}^9 \lambda_i \gamma^i = 0$ . That is,  $\gamma$  is a root of the nonzero polynomial  $\sum_{i=0}^9 \lambda_i x^i \in \mathbb{Q}[x]$ .

Various different techniques from linear algebra can be used to explicitly construct a polynomial in  $\mathbb{Q}[x]$  with  $\alpha + \beta$  as a root. For example,

$$(\alpha + \beta) \begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \\ \beta \\ \alpha\beta \\ \alpha^2\beta \\ \beta^2 \\ \alpha\beta^2 \\ \alpha^2\beta^2 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ -2 & -2 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & -2 & -2 & 0 & 0 & 0 & 1 \\ -3 & 0 & 0 & 6 & 0 & 0 & 0 & 1 & 0 \\ 0 & -3 & 0 & 0 & 6 & 0 & 0 & 0 & 1 \\ 0 & 0 & -3 & 0 & 0 & 6 & -2 & -2 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \\ \beta \\ \alpha\beta \\ \alpha^2\beta \\ \beta^2 \\ \alpha\beta^2 \\ \alpha^2\beta^2 \end{pmatrix}$$

and so  $\alpha + \beta$  is an eigenvalue of the coefficient matrix, and hence a root of its characteristic polynomial. But this polynomial has rational coefficients since the matrix has rational entries.

4. Let  $\alpha = \sqrt[3]{2} \in \mathbb{R}$ , and let  $f(x) \in \mathbb{Q}[x]$  be the minimal polynomial of  $\alpha$ ; that is,  $f(x)$  is the least degree monic polynomial in  $\mathbb{Q}[x]$  such that  $f(\alpha) = 0$ . Prove that  $f(x)$  is a divisor of every  $g(x) \in \mathbb{Q}[x]$  such that  $g(\alpha) = 0$ .

*Solution.*

If we let  $K = \{g(x) \in \mathbb{Q}[x] \mid g(\alpha) = 0\}$  then  $K$  is an ideal in  $\mathbb{Q}[x]$  (as is easily proved, either directly or by observing that  $K$  is the kernel of the evaluation homomorphism  $g(x) \mapsto g(\alpha)$ ). Since  $f(x)$  is a nonzero element of  $K$  of minimal degree it generates  $K$  (by Theorem 9.4 of the course notes), and so  $f(x) \mid g(x)$  whenever  $g(x) \in K$ , as required.

The direct proof is almost as brief, or briefer. Suppose  $g(\alpha) = 0$ . By division for polynomials over a field,  $g(x) = q(x)f(x) + r(x)$  for some  $r(x) \in \mathbb{Q}[x]$  with  $\deg r(x) < \deg f(x)$ . As  $f(\alpha) = 0 = g(\alpha)$  it follows that  $r(\alpha) = 0$  too, whence  $r(x) \in K$ . If  $r(x)$  is nonzero it will have a monic associate (namely,  $c^{-1}r(x)$ , where  $c$  is the leading coefficient of  $r(x)$ ) which will also be in  $K$ , contradicting the fact that  $f(x)$  is the least degree monic polynomial in  $K$ . So  $r(x) = 0$ ; that is,  $f(x) \mid g(x)$ .

Note that we can now deduce easily that  $f(x) = x^7 - 2$ . The point is that  $x^7 - 2$  is irreducible over  $\mathbb{Q}$ , by Eisenstein's Criterion. But since  $\alpha$  is a root of  $x^7 - 2$  it follows from the result we have just proved that  $f(x)$  is a divisor of  $x^7 - 2$ . So  $f(x)$  is either a unit or an associate of  $x^7 - 2$ . But it cannot be a unit, since units are nonzero constant polynomials, whereas  $f(t) = 0$ . So  $f(x) = c(x^7 - 2)$  for some  $c \in \mathbb{Q}$ . But  $f(x)$  and  $x^7 - 2$  both have leading coefficient 1; so  $c = 1$ .

5. Let  $F$  be a field,  $E$  an extension field of  $F$ , and  $t \in E$ . Suppose that  $t$  is a root of some polynomial  $f(x) \in F[x]$ , and choose  $f(x)$  to be such a polynomial with degree as small as possible. Prove that  $f(x)$  is irreducible in  $F[x]$ . Is  $f(x)$  irreducible as an element of  $E[x]$ ?

*Solution.*

Suppose, for a contradiction, that  $f(x)$  has a divisor  $r(x) \in F[x]$  that is neither a unit nor an associate of  $f(x)$ . Then  $f(x) = r(x)s(x)$  for some  $s(x) \in F[x]$  with  $\deg s(x) > 0$  (since  $r(x)$  is not an associate of  $f(x)$ ) and  $\deg s(x) < \deg f(x)$  (since  $r(x)$  is not a unit). So  $\deg r(x)$  and  $\deg s(x)$  are both strictly less than  $\deg f(x)$ . But since

$$0 = f(t) = r(t)s(t),$$

and since we are working in a field, it follows that  $r(t) = 0$  or  $s(t) = 0$ . But this contradicts the fact that  $f(x)$  is the nonzero polynomial of minimal degree in  $F[x]$  that has  $t$  as a root. (The question should have said that  $f(x)$  is required to be nonzero. Of course then  $r(x)$  and  $s(x)$  above will be

nonzero since  $r(x)s(x) = f(x)$ .) So  $f(x)$  has no divisors other than units and associates of itself; hence  $f(x)$  is irreducible.

If we consider  $f(x)$  as an element of  $E[x]$  then it is certainly divisible by  $x - t$ , because applying the division algorithm in  $E[x]$  gives  $f(x) = (x - t)q(x) + r$  for some  $q(x) \in E[x]$  and some  $r \in E$ , and evaluating at  $x = t$  shows that  $r = 0$ . So  $f(x)$  is not irreducible in  $E[x]$  unless it is just an associate of  $x - t$ . This will hold if  $t \in F$ , but not otherwise. (If  $t \in F$  it is clear that  $x - t$  is a minimal degree nonzero element of  $F[x]$  with  $t$  as a root; if  $t \notin F$  then no associate of  $x - t$  lies in  $F[x]$ , since the associates of  $x - t$  all have the form  $sx - st$  with  $s \neq 0$ , and  $s, -st \in F$  would imply that  $t = -(-st)s^{-1} \in F$ .)

6. Let  $F$ ,  $E$  and  $t$  be as in Question 5. The *minimal polynomial* of  $t$  over  $F$  is the monic polynomial  $f(x) \in F[x]$  of minimal degree with the property that  $f(t) = 0$ . Show that if  $p(x) \in F[x]$  is irreducible and satisfies  $p(t) = 0$  then  $p(x)$  is an associate of the minimal polynomial of  $t$ . (That is,  $p(x) = cf(x)$ , where  $c \in F$  and  $f(x)$  is the minimal polynomial of  $t$ .)

*Solution.*

This is the same as Question 4 above, with an arbitrary  $t$  replacing  $\sqrt[3]{2}$ . The set  $\{g(x) \in F[x] \mid g(t) = 0\}$  is an ideal in  $F[x]$ , and the minimal polynomial of  $t$  is by definition a nonzero element of this ideal of least possible degree. So the minimal polynomial is a generator of the ideal. Writing  $f(x)$  for the minimal polynomial, we have shown that

$$\{g(x) \in F[x] \mid g(t) = 0\} = f(x)F[x],$$

and so if  $g(x) \in F[x]$  satisfies  $g(t) = 0$  then  $f(x) \mid g(x)$ . Again, we could prove this directly by using the division algorithm for polynomials to write  $g(x) = f(x)q(x) + r(x)$  (where  $\deg r(x) < \deg f(x)$ ) and then evaluate at  $x = t$  to deduce that  $r(t) = 0$ , whence  $r(x) = 0$  by minimality of  $f(x)$ .

Suppose that  $p(x)$  is irreducible and  $p(t) = 0$ . Then  $f(x) \mid p(x)$ , by what we have just proved, and so  $f(x)$  is a unit or an associate of  $p(x)$ , since  $p(x)$  is irreducible. Since  $f(t) = 0$  it is not possible for  $f(x)$  to be a nonzero constant polynomial; so it must be an associate of  $p(x)$ , as required.