GALOIS THEORY
TOPIC XI
FIELD THEORY EXAMPLES

PAUL L. BAILEY

1. Irreducibility Examples

Example 1. Show that $f(x) = x^2 - 6x - 2$ is irreducible over $\mathbb{Q}$.

Solution. Any proper factorization over a field F of a quadratic polynomial would include a linear term $(x - \beta)$, where $\beta \in F$ and β is a root of f.

By the quadratic formula, the roots of f in $\mathbb{C}$ are

$$x = \frac{8 \pm \sqrt{64+8}}{2} = 4 \pm \sqrt{11}.$$

Thus f has no rational roots, and since f is quadratic, f is irreducible over $\mathbb{Q}$. □

Example 2. Show that $f(x) = x^3 - 4x + 2$ is irreducible over $\mathbb{Q}$.

Solution. Since f is cubic, any proper factorization over $\mathbb{Q}$ would include a linear term, so f would have a root in $\mathbb{Q}$. By the Rational Roots Theorem, the only conceivable rational roots of f are ± 1 or ± 2. But testing these shows that none of them are roots; thus f is irreducible. □

Example 3. Show that $f(x) = x^4 - x^2 + 6$ has no rational roots, but is reducible over $\mathbb{Q}$.

Solution. We can factor $f(x) = (x^2-3)(x^2+2)$, from which we see that the complex roots of f are ± 3 and $\pm i\sqrt{2}$. None of these roots are in $\mathbb{Q}$. □

Example 4. Show that $f(x) = x^3 - 42x^2 + 30x + 2772$ is irreducible over $\mathbb{Q}$.

Solution. The prime factorization of 2772 is $2^2 \cdot 3^2 \cdot 7 \cdot 11$. There are more factors of this number than we wish to try in applying the Rational Roots Theorem. On the other hand, if we reduce the polynomial modulo 5, we obtain

$$f(x) = x^3 - 2x^2 + 2.$$

Then in $\mathbb{Z}_5$, we have $f(0) = 2$, $f(1) = 1$, $f(2) = 2$, $f(3) = 2$, and $f(4) = 4$. Thus f has no roots in $\mathbb{Z}_5$, and since f is cubic, this implies that f has is irreducible over $\mathbb{Z}_5$. Thus f is irreducible over $\mathbb{Q}$ by the Modular Irreducibility Test. □

Date: December 6, 2006.

Example 5. Factor $f(x) = x^6 - 1$ into a product of polynomials which are irreducible over $\mathbb{Q}$.

Solution. Use the formula for the difference of cubes to see that

$$f(x) = (x^3 - 1)(x^3 + 1) = (x - 1)(x + 2)(x^2 + x + 1)(x^2 - x + 1).$$

The quadratic polynomials have negative discriminant, so their roots are nonreal, and therefore nonrational; thus they are irreducible over $\mathbb{Q}$. □

Example 6. Factor $f(x) = x^8 - 1$ into a product of polynomials which are irreducible over $\mathbb{Q}$.

Solution. We see that

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

Clearly $(x^2 + 1)$ is irreducible over $\mathbb{Q}$; is $x^4 + 1$ irreducible over $\mathbb{Q}$? Since it has no rational roots, if it factors, it must factor into the product of irreducible quadratics. We know that in any factorization over $\mathbb{R}$, complex conjugates produce pairs which are irreducible over $\mathbb{R}$. So, if $x^4 + 1$ factors over $\mathbb{Q}$, this must be the same factorization that it has over $\mathbb{R}$.

Now $(x - z)(x - \overline{z}) = x^2 - (z + \overline{z})x + z\overline{z} = x^2 - 2\Re(z) + |z|^2$. A root of $x^4 + 1$ is $e^{2\pi i/4} = \frac{\sqrt{2}+i\sqrt{2}}{2}$, and $2\Re(z) = \sqrt{2}$. This is not rational, so this quadratic is not over $\mathbb{Q}$. Thus the factorization of $x^4 + 1$ over $\mathbb{R}$ does not succeed over $\mathbb{Q}$, which shows that $x^4 + 1$ is irreducible over $\mathbb{Q}$. □

Example 7. Factor $f(x) = x^4 + x^2 + 1$ into a product of polynomials which are irreducible over $\mathbb{Q}$.

Solution. Since $f(x)$ clearly has no rational roots, we look for a factorization into irreducible quadratics. Again, it must factor of $\mathbb{R}$ into the product of two irreducible quadratics, and we only need to see if these quadratics have rational coefficients.

Since $f(x)$ looks like a cyclotomic polynomial in x^2, the natural thing to do is to multiply it by $x^2 - 1$, in order to better understand it. We obtain

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

Thus, the roots of $f(x)$ are the complex sixth roots of unity other than ±1. The primitive cube roots of unity are the roots of $x^2 + x + 1$, so this must be a factor of $f(x)$. Indeed,

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

Each of these factors is irreducible, since it is quadratic with no rational roots. □

Example 8. Determine if $f(x)$ is irreducible over $\mathbb{Q}$. Justify your answer.

(a) $f(x) = x - 16$
(b) $f(x) = x^5 - 32$
(c) $f(x) = x^3 + 15x^2 + 8x + 40$
(d) $f(x) = x^4 + 2x^2 + 1$
(e) $f(x) = x^5 + 6x^4 + 10x^3 + 8x + 18$
(f) $f(x) = 7x^2 - 9x + 3$

Solution. Since **(a)** is linear, it is irreducible.

Since 2 is a root of **(b)**, it is not irreducible.

Consider **(c)** modulo 3; it is $f(x) = x^3 - x + 1$. In $\mathbb{Z}_3$, $f(0) = 1$, $f(1) = 1$, and $f(2) = 1$. Thus f has no roots in $\mathbb{Z}_3$, and since f is cubic, it is irreducible in $\mathbb{Z}_3$. Thus f is irreducible in $\mathbb{Q}$ by the Modular Irreducibility Test, with $p = 3$.

Obviously $x^4 + 2x^2 + 1 = (x^2 + 1)^2$, so **(d)** is reducible.

(e) is irreducible by Eisenstein's Criterion, with $p = 2$.

The discriminant of the quadratic in **(f)** is $9^2 - 4(7)(2) = 81 - 84 < 0$, so **(f)** is irreducible. □

Example 9. Let $f(x) = x^4 - mx^2 + 1$, where $m \in \mathbb{Z}$.
Show that f is reducible over $\mathbb{Q}$ if and only if there exists $a \in \mathbb{Z}$ such that either

(i) $m = a^2 - 2$, in which case $f(x) = (x^2 - ax + 1)(x^2 + ax + 1)$, or
(ii) $m = a^2 + 2$, in which case $f(x) = (x^2 - ax - 1)(x^2 + ax - 1)$.

Proof. By the rational roots theorem, if f has a rational root, it is an integer dividing 1, so it is ±1, and $f(\pm 1) = 1 - m + 1 = 0$. Then $m = 2$ and

$$f(x) = (x - 1)(x + 1)(x - 1)(x + 1) = (x^2 + 2x + 1)(x^2 - 2x + 1).$$

This is case **(i)** with $a = 2$.

Otherwise, if f factors, it is a product of irreducible quadratics. Moreover, by Gauss' lemma, we may select these quadratics to have integer coefficients. In this case, the product of the leading coefficients will be the leading coefficient of f, which is one, so we may assume that the factors are monic.

Thus suppose that $f(x) = (x^2 + ax + b)(x^2 + cx + d)$, where $a, b, c, d \in \mathbb{Z}$. Multiplying this out gives

$$f(x) = x^4 + (a + c)x^3 + (b + d + ac)x^2 + (ad + bc)x + bd.$$

Matching coefficients gives the equations

(1) $a + c = 0$
(2) $b + d + ac = -m$
(3) $ad + bc = 0$
(4) $bd = 1$

The first equation says that $c = -a$, and the last say that $b = d = \pm 1$ (because $b, d \in \mathbb{Z}$). Then the second equation gives $2b - a^2 = -m$, so $m = a^2 - 2$ if $b = 1$ or $m = a^2 + 2$ if $b = -1$. Now multiply out the factorization given above to confirm that they do indeed give $f(x)$. □

2. Minimum Polynomial Examples

Example 10. Find the minimum polynomial over $\mathbb{Q}$ of $\beta = \sqrt[5]{2}$.

Solution. We see that $\beta^5 = 2$, so if $f(x) = x^5 - 2$, then $f(\beta) = 0$. This polynomial is irreducible by Eisenstein's criterion, and its coefficients are in $\mathbb{Q}$, so it is the minimum polynomial of β over $\mathbb{Q}$. □

Example 11. Find the minimum polynomial over $\mathbb{Q}$ of

$$\beta = 4\cos 18^\circ = \sqrt{10 + 2\sqrt{5}}.$$

.

Solution. Squaring gives $\beta^2 = 10+2\sqrt{5}$, so $\beta^2 - 10 = 2\sqrt{5}$. Thus $\beta^4 - 20\beta^2 + 100 = 20$, whence $\beta^4 - 20\beta^2 + 80 = 0$. Let $f(x) = x^4 - 20x^2 + 80$; then $f(\beta) = 0$. Moreover, f is irreducible over $\mathbb{Q}$ by Eisenstein's criterion, with $p = 5$. Thus f is the minimum polynomial of β over $\mathbb{Q}$. □

Example 12. Find the minimum polynomial over $\mathbb{Q}$ of

$$\beta = \sqrt{2} + \sqrt{3}.$$

Solution. It suffices to find a monic polynomial which annihilates β, and show that it is irreducible. Squaring both sides of the definition of β gives $\beta^2 = 2 + 2\sqrt{6} + 3$, so $\beta^2 - 5 = 2\sqrt{6}$, whence $(\beta^2 - 5)^2 = 24$. Therefore $\beta^4 - 10\beta^2 + 1 = 0$. Set $f(x) = x^4 - 10x^2 + 1$; then $f(\beta) = 0$. Showing that f is irreducible is possible by brute force, as demonstrated in Example 9. We give an alternate proof, using the field extensions and the product of degrees formula.

Claim 1: $\mathbb{Q}[\beta] = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$.
Clearly $\beta \in \mathbb{Q}[\sqrt{2}, \sqrt{3}]$, so $\mathbb{Q}[\beta] \subset \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. So to prove **(a)**, it suffices to show that $\sqrt{2}, \sqrt{3} \in \mathbb{Q}[\beta]$. Since $\mathbb{Q}[\beta]$ is a field,

$$\beta^{-1} = \frac{1}{\beta} = \frac{1}{\sqrt{3}+\sqrt{2}} = \frac{\sqrt{3}-\sqrt{2}}{3-2} = \sqrt{3} - \sqrt{2} \in \mathbb{Q}[\beta].$$

Thus $\beta - \beta^{-1} = 2\sqrt{3} \in \mathbb{Q}[\beta]$, so $\sqrt{3} \in \mathbb{Q}[\beta]$. Thus $\sqrt{2} = \beta - \sqrt{3} \in \mathbb{Q}[\beta]$.

Claim 2: $[\mathbb{Q}[\sqrt{2}, \sqrt{3}] : \mathbb{Q}] = 4$.
The minimum polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$, so $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$. It is impossible to solve the equation $\sqrt{3} = a + b\sqrt{2}$ for rational numbers a and b, so $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$. The minimum polynomial of $\sqrt{3}$ over $\mathbb{Q}$ is $x^2 - 3$; but since $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$ and $x^2 - 3$ is quadratic, it cannot possibly factor over $\mathbb{Q}[\sqrt{2}]$. Thus $x^2 - 3$ is irreducible over $\mathbb{Q}[\sqrt{3}]$, which shows that

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

Therefore, $[\mathbb{Q}[\beta] : \mathbb{Q}] = 4$, so the degree of the minimum polynomial of β over $\mathbb{Q}$ is 4. Since $f(x) = x^4 - 10x^2 + 1$ is a monic polynomial of degree four which annihilates β, it must be the minimum polynomial of β over $\mathbb{Q}$. Consequently, it is irreducible. □

Example 13. Let $\beta = \sqrt[3]{\sqrt{2}+\sqrt{3}}$.

(a) Find the minimum polynomial of β over $\mathbb{Q}$.

(b) Find the minimum polynomial of β over $\mathbb{Q}[\sqrt{6}]$.

Solution. Compute $\beta^3 = \sqrt{2}+\sqrt{3}$, so $\beta^6 = 5+2\sqrt{6}$, whence $(\beta^6-5)^2 = 24$. Writing this in standard form, we obtain

$$\beta^12 - 10\beta^6 + 1 = 0.$$

Let $f(x) = x^12 - 10x^6 + 1$; then $f(\beta) = 0$. Thus f is a monic polynomial which annihilates β; we wish to show that f is irreducible over $\mathbb{Q}$. Since we know that the minimum polynomial of β is divisible by f, it suffices to show that the degree of the minimum polynomial of β is 12. We also know that the degree of the minimum polynomial is equal to the degree of the corresponding primitive extension.

We show that $[\mathbb{Q}[\beta] : \mathbb{Q}] = 12$ by using the product of degrees formula.

The minimum polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is x^2-2, so $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$. It is impossible to solve the equation $\sqrt{3} = a + b\sqrt{2}$ for rational numbers a and b, so $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$.

The minimum polynomial of $\sqrt{3}$ over $\mathbb{Q}$ is x^2-3; but since $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$ and x^2-3 is quadratic, it cannot possibly factor over $\mathbb{Q}[\sqrt{2}]$. Thus x^2-3 is irreducible over $\mathbb{Q}[\sqrt{3}]$, which shows that

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

Let $\alpha = \sqrt{2}+\sqrt{3}$; we show that $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{2},\sqrt{3}]$. It is clear that $\alpha \in \mathbb{Q}[\sqrt{2},\sqrt{3}]$, so we show that $\sqrt{2},\sqrt{3} \in \mathbb{Q}[\alpha]$.

Set $h(x) = x^4 - 10x^2 + 1$. Then h is a polynomial which annihilates α, so α is algebraic over $\mathbb{Q}$, so $\mathbb{Q}[\alpha]$ is a field. The inverse of α is also in $\mathbb{Q}[\alpha]$, and may be computed as

$$\alpha^{-1} = \frac{1}{\sqrt{3}+\sqrt{2}} = \frac{\sqrt{3}-\sqrt{2}}{3-2} = \sqrt{3}-\sqrt{2}.$$

Thus $\dfrac{\alpha+\alpha^{-1}}{2} = \sqrt{3} \in \mathbb{Q}[\alpha]$, and consequently $\alpha - \sqrt{3} = \sqrt{2} \in \mathbb{Q}[\alpha]$. Conclude that $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{2},\sqrt{3}]$. Incidently, this also shows that h is irreducible over $\mathbb{Q}$, and that $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 4$.

Finally, it is clear that $\beta \notin \mathbb{Q}[\alpha]$. However, $x^3 - \alpha$ is a polynomial over $\mathbb{Q}[\alpha]$ which annihilates β. This cubic polynomial is irreducible unless it has a root in $\mathbb{Q}[\alpha]$. But the roots are β, $\beta\omega$, and $\beta\omega^2$, where $\omega = e^{2\pi i/3}$. The latter two are nonreal, and so are certainly not in the real field $\mathbb{Q}[\alpha]$. Thus $x^3-\alpha$ is the minimum polynomial of β over $\mathbb{Q}[\alpha]$. Thus

$$[\mathbb{Q}[\beta] : \mathbb{Q}] = [\mathbb{Q}[\beta] : \mathbb{Q}[\alpha]][\mathbb{Q}[\alpha] : \mathbb{Q}] = 3 \cdot 4 = 12.$$

This details why $f(x) = x^{12} - 10x^6 + 1$ must be irreducible over $\mathbb{Q}$.

Looking back at our initial computation, we see that $\beta^6 - 5 - 2\sqrt{6} = 0$. Thus let $g \in \mathbb{Q}[\sqrt{6}]$ be given as $g(x) = x^6 - (5+2\sqrt{6})$. Since $[\mathbb{Q}[\sqrt{6}] : \mathbb{Q}] = 2$, we must have $[\mathbb{Q}[\beta] : \mathbb{Q}[\sqrt{6}] = 12/2 = 6$. Thus g is irreducible. □

Example 14. Let $\beta = e^{2\pi/16}$.

(a) Find the minimum polynomial of β over $\mathbb{Q}$.
(b) Find the minimum polynomial of β over $\mathbb{Q}[i]$.
(c) Find the minimum polynomial of β over $\mathbb{Q}[\sqrt{2}]$.

Solution. Since $\beta^8 = e^{\pi i} = -1$, we see that β is a root of $f(x) = x^8 + 1$. We wish to show that f is irreducible, again by computing degrees.

Now $\beta = \text{cis}(2\pi i/16) = \cos(2\pi i/16) + i\sin(2\pi i/16)$; use the half angle formula to compute

$$\beta = \frac{\sqrt{2-\sqrt{2}}}{2} + i\frac{\sqrt{2+\sqrt{2}}}{2}.$$

Note that $\beta^2 = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$, and $\beta^4 = i$. Then $i, \sqrt{2}, \sqrt{2+\sqrt{2}} \in \mathbb{Q}[\beta]$.

Drawing on previous experience, we can see that $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$, but that $\sqrt{2+\sqrt{2}} \notin \mathbb{Q}[\sqrt{2}]$. Thus $[\mathbb{Q}[\sqrt{2+\sqrt{2}}] : \mathbb{Q}] = 4$. Since $\sqrt{2+\sqrt{2}} \in \mathbb{R}$, the field it generates over $\mathbb{Q}$ is also contained in $\mathbb{R}$, and in particular, does not contain i. Thus $[\mathbb{Q}[i, \sqrt{2+\sqrt{2}}] : \mathbb{Q}] = 8$, which proves that f is irreducible.

The minimum polynomial of β over $\mathbb{Q}[i]$ must be of degree 4, and $\beta^4 = i$. Thus, $x^4 - i$ is the minimum polynomial of β over $\mathbb{Q}[i]$.

The minimum polynomial of β over $\mathbb{Q}[\sqrt{2}]$ also is of degree 4; note that $\overline{\beta} = \beta^{-1}$ is the complex conjugate of β, so

$$\beta + \beta^{-1} = 2\Re(\beta) = \sqrt{2-\sqrt{2}}.$$

Squaring gives $\beta^2 + 2 + \beta^{-2} = 2 - \sqrt{2}$, so $\beta^4 + \sqrt{2}\beta^2 + 1 = 0$. Thus $x^4 + \sqrt{2}x^2 + 1$ is the minimum polynomial of β over $\sqrt{2}$. □

3. Splitting Extensions

Example 15. Let $f(x) = x^2 + 1$, and let E be the splitting field of f over $\mathbb{Q}$. Write $E/\mathbb{Q}$ as a multiple extension of $\mathbb{Q}$, and find $[E : \mathbb{Q}]$.

Solution. The roots of f are not $\pm i$. Clearly $E = \mathbb{Q}[i, -i] = \mathbb{Q}[i]$. Since f is irreducible, $[E : \mathbb{Q}] = 2$. □

Example 16. Let $f(x) = x^3 - 7x + 6$, and let E be the splitting field of f over $\mathbb{Q}$. Write $E/\mathbb{Q}$ as a multiple extension of $\mathbb{Q}$, and find $[E : \mathbb{Q}]$.

Solution. We see that $f(1) = 0$, and divide f by $(x - 1)$ to find

$$f(x) = (x - 1)(x - 2)(x + 3).$$

So, $E = \mathbb{Q}[1, 2, -3] = \mathbb{Q}$, and $[E : \mathbb{Q}] = 1$. □

Example 17. Let $f(x) = x^3 - 7x^2 + 6$, and let E be the splitting field of f over $\mathbb{Q}$. Write $E/\mathbb{Q}$ as a multiple extension of $\mathbb{Q}$, and find $[E : \mathbb{Q}]$.

Solution. We see that $f(1) = 0$, and divide f by $(x - 1)$ to find

$$f(x) = (x - 1)(x^2 - 6x - 6).$$

Let $g(x) = x^2 - 6x - 6$; this polynomial is irreducible over $\mathbb{Q}$, as the quadratic formula gives its roots to be

$$x = \frac{6 \pm \sqrt{36 + 24}}{2} = 3 \pm \sqrt{15}.$$

If we adjoin $\sqrt{15}$ to $\mathbb{Q}$, we will obtain all three roots of f; thus $E = \mathbb{Q}[\sqrt{15}]$. The minimum polynomial of $\sqrt{15}$ over $\mathbb{Q}$ is not g, but it is $x^2 - 15$, so $[E : \mathbb{Q}] = 2$. □

Example 18. Let $f(x) = x^5 - 2$, and let E be the splitting field of f over $\mathbb{Q}$. Write $E/\mathbb{Q}$ as a multiple extension, and find $[E : \mathbb{Q}]$.

Solution. Let $\alpha = \sqrt[5]{2}$, and let $\omega = e^{2\pi i/5}$. Then ω is a primitive fifth root of unity, and the five fifth roots of 2 generate E. Thus

$$E = \mathbb{Q}[\alpha, \alpha\omega, \alpha\omega^2, \alpha\omega^3, \alpha\omega^4].$$

Since E is a field, $\alpha^{-1} \in E$, so $\alpha^{-1}\alpha\omega \in E$. Then it is clear that $E = \mathbb{Q}[\alpha, \omega]$.

Now $[\mathbb{Q}[\alpha] : \mathbb{Q}] = \deg(f) = 5$; but ω is not in $\mathbb{Q}[\alpha]$. We know this because $\mathbb{Q}[\alpha]$ contains only real number, but ω is not real.

Recall that if p is prime and ζ is a primitive p^{th} root of unity, then ζ is a root of $x^p - 1 = (x - 1)(x^{p-1} + \cdots + x + 1)$, where $\Phi_p(x) = x^{p-1} + \cdots + 1$ is the p^{th} cyclotomic polynomial. We have seen that Φ_p is irreducible (we substituted $x + 1$ for x and applied Eisenstein's criterion to see this).

Thus $g(x) = x^4 + x^3 + x^2 + x + 1$ is the minimum polynomial of ω, and $[\mathbb{Q}[\omega] : \mathbb{Q}] = 4$. Thus the minimum polynomial of ω over $\mathbb{Q}[\alpha]$ is a factor of g, and $[E : \mathbb{Q}[\omega] \leq 4$.

Since $\mathbb{Q}[\alpha]$ and $\mathbb{Q}[\omega]$ are both subfields of E, we see that $[E : \mathbb{Q}]$ is divisible both by 5 and by 4, so $[E : F]$ is at least twenty, so $[E : \mathbb{Q}[\alpha]] \geq 4$.

We conclude that

$$[E : \mathbb{Q}] = [\mathbb{Q}[\alpha, \omega] : \mathbb{Q}[\alpha]] \cdot [\mathbb{Q}[\alpha] : \mathbb{Q}] = 4 \cdot 5 = 20.$$

□

Example 19. Let $f(x) = x^{12} - 1$, and let E be the splitting field of f over $\mathbb{Q}$. Write $E/\mathbb{Q}$ as a multiple extension, and find $[E : \mathbb{Q}]$.

Solution. Let $\beta = e^{2\pi i/12} = \frac{\sqrt{3}}{2} + i\frac{1}{2}$. Since β is a primitive twelfth root of unity, all the other roots of f are powers of β, so $E = \mathbb{Q}[\beta] = \mathbb{Q}[\sqrt{3}, i]$. Thus $[E : \mathbb{Q}] = 4$.

Let's find the minimum polynomial of β over $\mathbb{Q}$, by way of factoring f into irreducible polynomials:

$$\begin{aligned} x^{12} - 1 &= (x^6 - 1)(x^6 + 1) \\ &= (x^3 - 1)(x^3 + 1)(x^2 + 1)(x^4 - x^2 + 1) \quad \text{(sum of cubes formula)} \\ &= (x - 1)(x^2 + x + 1)(x + 1)(x^2 - x + 1)(x^2 + 1)(x^4 - x^2 + 1). \end{aligned}$$

The last factor is the only one whose degree is at least four; thus it must be the minimum polynomial of β over $\mathbb{Q}$, and is irreducible. We identify the powers of β which are roots of each of these polynomials:

- 1, the primitive first root of unity, is a root of $x - 1$;
- -1, the primitive second root of unity, is a root of $x + 1$;
- β^4, β^8, the primitive cube roots of unity, are roots of $x^2 + x + 1$;
- β^2, β^{10}, the primitive sixth roots of unity, are roots of $x^2 - x + 1$;
- $\pm\beta^3 = \pm i$, the primitive fourth roots of unity, are roots of $x^2 + 1$;
- $\beta, \beta^5, \beta^7, \beta^{11}$, the primitive twelfth roots of unity, are roots of $x^4 - x^2 + 1$.

□

Department of Mathematics and CSci, Southern Arkansas University
E-mail address: plbailey@saumag.edu