(*March 21, 2005*)

# Solutions 13

*Paul Garrett* garrett@math.umn.edu http://www.math.umn.edu/˜garrett/

[13.1] Determine the degree of $\mathbf{Q}(\sqrt{65+56i})$ over $\mathbf{Q}$, where $i = \sqrt{-1}$.

We show that $65 + 56i$ is not a square in $\mathbf{Q}(i)$. We use the *norm*

$$N(\alpha) = \alpha \cdot \alpha^\sigma$$

from $\mathbf{Q}(i)$ to $\mathbf{Q}$, where as usual $(a + bi)^\sigma = a - bi$ for rational $a, b$. Since $-i$ is the other zero of the minimal polynomial $x^2 + 1$ of $i$ over $\mathbf{Q}$, the map $\sigma$ is a field automorphism of $\mathbf{Q}(i)$ over $\mathbf{Q}$. (Indeed, we showed earlier that there exists a $\mathbf{Q}$-linear field automorphism of $\mathbf{Q}(i)$ taking $i$ to $-i$.) Since $\sigma$ is a field automorphism, $N$ is *multiplicative*, in the sense that

$$N(\alpha\beta) = N(\alpha) \cdot N(\beta)$$

Thus, if $\alpha = \beta^2$, we would have

$$N(\alpha) = N(\beta^2) = N(\beta)^2$$

and the latter is a square in $\mathbf{Q}$. Thus, if $\alpha = 65 + 56i$ were a square, then

$$N(65 + 56i) = 65^2 + 56^2 = 7361$$

would be a square. One could factor this into primes in $\mathbf{Z}$ to see that it is not a square, or hope that it is not a square modulo some relatively small prime. Indeed, modulo 11 it is 2, which is not a square modulo 11 (by brute force, or by Euler's criterion (using the cyclicness of $(\mathbf{Z}/11)^\times$) $2^{(11-1)/2} = -1 \bmod 11$, or by recalling the part of Quadratic Reciprocity that asserts that 2 is a square mod $p$ only for $p = \pm 1 \bmod 8$).

[13.2] Fix an algebraically closed field $k$. Find a simple condition on $w \in k$ such that the equation $z^5 + 5zw + 4w^2 = 0$ has no repeated roots $z$ in $k$.

Use some form of the Euclidean algorithm to compute the greatest common divisor in $k(w)[z]$ of $f(z) = z^5 + 5zw + 4w^2$ and its (partial?) derivative (with respect to $z$, not $w$). If the characteristic of $k$ is 5, then we are in trouble, since the derivative (in $z$) vanishes identically, and therefore it is impossible to avoid repeated roots. So suppose the characteristic is not 5. Similarly, if the characteristic is 2, there will always be repeated roots, since the polynomial becomes $z(z^4 + w)$. So suppose the characteristic is not 2.

$$\begin{array}{rcl} (z^5 + 5zw + 4w^2) - \frac{z}{5} \cdot (5z^4 + 5w) & = & 4zw + 4w^2 \\ (z^4 + w) - \frac{1}{4w}(z^3 - z^2w + zw^2 - w^3) \cdot (4zw + 4w^2) & = & w - w^4 \end{array}$$

where we also assumed that $w \neq 0$ to be able to divide. The expression $w - w^4$ is in the ground field $k(w)$ for the polynomial ring $k(w)[z]$, so if it is non-zero the polynomial and its derivative (in $z$) have no common factor. We know that this implies that the polynomial has no repeated factors. Thus, in characteristic not 5 or 2, for $w(1 - w^3) \neq 0$ we are assured that there are no repeated factors.

**Remark:** The algebraic closedness of $k$ did not play a role, but may have helped avoid various needless worries.

[13.3] Fix a field $k$ and an indeterminate $t$. Fix a positive integer $n > 1$ and let $t^{1/n}$ be an $n^{\text{th}}$ root of $t$ in an algebraic closure of the field of rational functions $k(t)$. Show that $k[t^{1/n}]$ is isomorphic to a polynomial ring in one variable.

*(There are many legitimate approaches to this question...)*

We show that $k[t^{1/n}]$ is a free $k$-algebra on one generator $t^{1/n}$. That is, given a $k$-algebra $A$, a $k$-algebra homomorphism $f : k \to A$, and an element $a \in A$, we must show that there is a unique $k$-algebra homomorphism $F : k[t^{1/n}] \to A$ extending $f : k \to A$ and such that $F(t^{1/n}) = a$.

Let $k[x]$ be a polynomial ring in one variable, and let $f : k[x] \to k[t^{1/n}]$ be the (surjective) $k$-algebra homomorphism taking $x$ to $t^{1/n}$. If we can show that the kernel of $f$ is trivial, then $f$ is an isomorphism and we are done.

Since $k[t]$ is a free $k$-algebra on one generator, it is infinite-dimensional as a $k$-vectorspace. Thus, $k[t^{1/n}]$ is infinite-dimensional as a $k$-vectorspace. Since $f : k[x] \to k[t^{1/n}]$ is surjective, its image $k[x]/(\ker f) \approx f(k[x])$ is infinite-dimensional as a $k$-vectorspace.

Because $k[x]$ is a principal ideal domain, for an ideal $I$, either a quotient $k[x]/I$ is finite-dimensional as a $k$-vector space, or else $I = \{0\}$. There are no (possibly complicated) intermediate possibilities. Since $k[x]/(\ker f)$ is infinite-dimensional, $\ker f = \{0\}$. That is, $f : k[x] \to k[t^{1/n}]$ is an isomorphism. ///

**Remark:** The vague and mildly philosophical point here was to see why an $n^{\text{th}}$ root of an *indeterminate* is still such a thing. It is certainly possible to use different language to give structurally similar arguments, but it seems to me that the above argument captures the points that occur in any version. For example, use of the notion of field elements *transcendental* over some ground field does suggest a good intuition, but still requires attention to similar details.

[13.4] Fix a field $k$ and an indeterminate $t$. Let $s = P(t)$ for a monic polynomial $P$ in $k[x]$ of positive degree. Find the monic irreducible polynomial $f(x)$ in $k(s)[x]$ such that $f(t) = 0$.

Perhaps this yields to direct computation, but we will do something a bit more conceptual.

Certainly $s$ is a root of the equation $P(x) - s = 0$. It would suffice to prove that $P(x) - s$ is irreducible in $k(s)[x]$. Since $P$ is monic and has coefficients in $k$, the coefficients of $P(x) - s$ are in the subring $k[s]$ of $k(s)$, and their *gcd* is 1. In other words, as a polynomial in $x$, $P(x) - s$ has *content* 1. Thus, from Gauss' lemma, $P(x) - s$ is irreducible in $k(s)[x]$ if and only if it is irreducible in $k[s][x] \approx k[x][s]$. As a polynomial in $s$ (with coefficients in $k[x]$), $P(x) - s$ has content 1, since the coefficient of $s$ is $-1$. Thus, $P(x) - s$ is irreducible in $k[x][s]$ if and only if it is irreducible in $k(x)[s]$. In the latter ring it is simply a linear polynomial in $s$, so is irreducible.

**Remark:** The main trick here is to manage to interchange the roles of $x$ and $s$, and then use the fact that $P(x) - s$ is much simpler as a polynomial in $s$ than as a polynomial in $x$.

**Remark:** The notion of irreducibility in $k[s][x] \approx k[x][s]$ does not depend upon how we view these polynomials. Indeed, irreducibility of $r \in R$ is equivalent to the irreducibility of $f(r)$ in $S$ for any ring isomorphism $f : R \to S$.

**Remark:** This approach generalizes as follows. Let $s = P(t)/Q(t)$ with relatively prime polynomials $P, Q$ (and $Q \neq 0$). Certainly $t$ is a zero of the polynomial $Q(x)s - P(s)$, and we claim that this is a (not necessarily monic) polynomial over $k(x)$ of minimal degree of which $t$ is a 0. To do this we show that $Q(x)s - P(x)$ is irreducible in $k(s)[x]$. First, we claim that its content (as a polynomial in $x$ with coefficients in $k[s]$) is 1. Let $P(x) = \sum_i a_i x^i$ and $Q(x) = \sum_j b_j x^j$, where $a_i, b_j \in k$ and we allow some of them to be 0. Then

$$Q(x)s - P(x) = \sum_i (b_i t - a_i)\, x^i$$

The content of this polynomial is the *gcd* of the linear polynomials $b_i t - a_i$. If this *gcd* were 1, then all these linear polynomials would be scalar multiples of one another (or 0). But that would imply that $P, Q$ are scalar multiples of one another, which is impossible since they are relatively prime. So (via Gauss' lemma) the content is 1, and the irreducibility of $Q(x)s - P(x)$ in $k(s)[x]$ is equivalent to irreducibility in $k[s][x] \approx k[x][s]$. Now we verify that the content of the polynomial in $t$ (with coefficient in $k[x]$) $Q(x)s - P(x)$ is 1. The content is the *gcd* of the coefficients, which is the *gcd* of $P, Q$, which is 1 by assumption. Thus, $Q(x)s - P(x)$ is irreducible in $k[x][s]$ if and only if it is irreducible in $k(x)[s]$. In the latter, it is a polynomial of degree at most 1, with non-zero top coefficients, so in fact linear. Thus, it is irreducible in $k(x)[s]$. We conclude that $Q(x)s - P(x)$ was irreducible in $k(s)[x]$.

Further, this approach shows that $f(x) = Q(x) - sP(x)$ is indeed a polynomial of minimal degree, over $k(x)$, of which $t$ is a zero. Thus,

$$[k(t) : k(s)] = \max(\deg P,\ \deg Q)$$

Further, this proves a much sharper fact than that automorphisms of $k(t)$ only map $t \to (at+b)/(ct+d)$, since any rational expression with higher-degree numerator or denominator generates a strictly smaller field, with the degree down being the maximum of the degrees.

[13.5] Let $p_1, p_2, \ldots$ be any ordered list of the prime numbers. Prove that $\sqrt{p_1}$ is *not* in the field

$$\mathbf{Q}(\sqrt{p_2}, \sqrt{p_3}, \ldots)$$

generated by the square roots of all the *other* primes.

First, observe that any rational expression for $\sqrt{p_1}$ in terms of the other square roots can only involve finitely many of them, so what truly must be proven is that $\sqrt{p_1}$ is not in the field

$$\mathbf{Q}(\sqrt{p_2}, \sqrt{p_3}, \ldots, \sqrt{p_N})$$

generated by any finite collection of square roots of *other* primes.

Probably an induction based on direct computation can succeed, but this is not the most interesting or informative. Instead:

Let $\zeta_n$ be a primitive $n^{\text{th}}$ root of unity. Recall that for an odd prime $p$

$$\sqrt{p \cdot \left(\frac{-1}{p}\right)_2} \in \mathbf{Q}(\zeta_p)$$

Certainly $i = \sqrt{-1} \in \mathbf{Q}(\zeta_4)$. Thus, letting $n = 4p_1p_2 \ldots p_N$, all the $\sqrt{p_1}, \ldots \sqrt{p_N}$ are in $K = \mathbf{Q}(\zeta_n)$. From the Gauss sum expression for these square roots, the automorphism $\sigma_a(\zeta_n) = \zeta_n^a$ of $\mathbf{Q}(\zeta_n)$ has the effect

$$\sigma_a \sqrt{p_i \cdot \left(\frac{-1}{p_i}\right)_2} = \left(\frac{a}{p_i}\right)_2 \cdot \sqrt{p_i \cdot \left(\frac{-1}{p_i}\right)_2}$$

Thus, for $a = 1 \bmod 4$, we have $\sigma_a(i) = i$, and

$$\sigma_a(\sqrt{p_i}) = \left(\frac{a}{p_i}\right)_2 \cdot \sqrt{p_i}$$

Since $(\mathbf{Z}/p_i)^\times$ is cyclic, there *are* non-squares modulo $p_i$. In particular, let $b$ be a non-square mod $p_1$. if we have $a$ such that

$$\begin{cases} a &= 1 \bmod 4 \\ a &= b \bmod p_1 \\ a &= 1 \bmod p_2 \\ & \vdots \\ a &= 1 \bmod p_N \end{cases}$$

then $\sigma_a$ fixes $\sqrt{p_2}, \ldots, \sqrt{p_N}$, so when restricted to $K = \mathbf{Q}(\sqrt{p_2}, \ldots, \sqrt{p_N})$ is trivial. But by design $\sigma_a(\sqrt{p_1}) = -\sqrt{p_1}$, so this square root cannot lie in $K$. ///

[13.6] Let $p_1, \ldots, p_n$ be distinct prime numbers. Prove that

$$\mathbf{Q}(\sqrt{p_1}, \ldots, \sqrt{p_N}) = \mathbf{Q}(\sqrt{p_1} + \ldots + \sqrt{p_N})$$

Since the degree of a compositum $KL$ of two field extensions $K, L$ of a field $k$ has degree *at most* $[K:k]\cdot[L:k]$ over $k$,

$$[\mathbf{Q}(\sqrt{p_1}, \ldots, \sqrt{p_N}) : \mathbf{Q}] \le 2^N$$

since $[\mathbf{Q}(\sqrt{p_i}) : \mathbf{Q}] = 2$, which itself follows from the irreducibility of $x^2 - p_i$ from Eisenstein's criterion. The previous example shows that the bound $2^N$ is the actual degree, by multiplicativity of degrees in towers.

Again, a direct computation might succeed here, but might not be the most illuminating way to proceed. Instead, we continue as in the previous solution. Let

$$\alpha = \sqrt{p_1} + \ldots + \sqrt{p_n}$$

Without determining the minimal polynomial $f$ of $\alpha$ over $\mathbf{Q}$ directly, we note that any automorphism $\tau$ of $\mathbf{Q}(\zeta_n)$ over $\mathbf{Q}$ can *only* send $alf$ to other zeros of $f$, since

$$f(\tau\alpha) = \tau(f(\alpha)) = \tau(0) = 0$$

where the first equality follows exactly because the coefficients of $f$ are fixed by $\tau$. Thus, if we show that $\alpha$ has at least $2^N$ distinct images under automorphisms of $\mathbf{Q}(\zeta_n)$ over $\mathbf{Q}$, then the degree of $f$ is at least $2^N$. (It is at most $2^N$ since $\alpha$ does lie in that field extension, which has degree $2^N$, from above.)

As in the previous exercise, for each index $i$ among $1, \ldots, N$ we can find $a_i$ such that

$$\sigma_{a_i}(\sqrt{p_j}) = \begin{cases} +\sqrt{p_j} & \text{for } j \neq i \\ -\sqrt{p_j} & \text{for } j = i \end{cases}$$

Thus, among the images of $\alpha$ are

$$\pm\sqrt{p_1} \pm \sqrt{p_2} \pm \ldots \pm \sqrt{p_N}$$

with all $2^N$ sign choices. These elements are all distinct, since any equality would imply, for some non-empty subset $\{i_1, \ldots, i_\ell\}$ of $\{1, \ldots, N\}$, a relation

$$\sqrt{p_{i_1}} + \ldots + \sqrt{p_{i_\ell}} = 0$$

which is precluded by the previous problem (since no one of these square roots lies in the field generated by the others). Thus, there are at least $2^N$ images of $\alpha$, so $\alpha$ is of degree at least over $2^N$, so is of degree exactly that. By multiplicativity of degrees in towers, it must be that $\alpha$ generates all of $\mathbf{Q}(\sqrt{p_1}, \ldots, \sqrt{p_N})$. ///

[13.7] Let $\alpha = xy^2 + yz^2 + zx^2$, $\beta = x^2y + y^2z + z^2x$ and let $s_1, s_2, s_3$ be the elementary symmetric polynomials in $x, y, z$. Describe the relation between the quadratic equation satisfied by $\alpha$ and $\beta$ over the field $\mathbf{Q}(s_1, s_2, s_3)$ and the quantity

$$\Delta^2 = (x-y)^2(y-z)^2(z-x)^2$$

Letting the quadratic equation be $ax^2 + bx + c$ with $a = 1$, the usual $b^2 - 4ac$ will turn out to be this $\Delta^2$. (Thus, there is perhaps some inconsistency in whether these are *discriminants* or their squares.) The interesting question is how to best be sure that this is so. As usual, *in principle* a direct computation would work, but it is more interesting to give a less computational argument.

Let

$$\delta = b^2 - 4ac = (-\alpha - \beta)^2 - 4 \cdot 1 \cdot \alpha\beta = (\alpha - \beta)^2$$

The fact that this $\delta$ is the *square* of something is probably unexpected, unless one has anticipated what happens in the sequel. Perhaps the least obvious point is that, if any two of $x, y, z$ are identical, then $\alpha = \beta$. For example, if $x = y$, then

$$\alpha = xy^2 + yz^2 + zx^2 = x^3 + xz^2 + zx^2$$

and

$$\beta = x^2y + y^2z + z^2x = x^3 + x^2z + z^2x = \alpha$$

The symmetrical arguments show that $x - y$, $x - z$, and $y - z$ all divide $\alpha - \beta$, in the (UFD, by Gauss) polynomial ring $\mathbf{Q}[x, y, z]$. The UFD property implies that the product $(x - y)(x - z)(y - z)$ divides $\alpha - \beta$. Since $\delta = (\alpha - \beta)^2$, and since $\Delta$ is the *square* of that product of three linear factors, up to a constant they are equal.

To determine the constant, we need only look at a single monomial. For example, the $x^4y^2$ term in $(\alpha - \beta)^2$ can be determined with $z = 0$, in which case

$$(\alpha - \beta)^2 = (xy^2 - x^2y)^2 = 1 \cdot x^4y^2 + \text{other}$$

Similarly, in $\Delta^2$, the coefficient of $x^4y^2$ can be determined with $z = 0$, in which case

$$\Delta^2 = (x - y)^2(x)^2(y)^2 = x^4y^2 + \text{other}$$

That is, the coefficient is 1 in both cases, so, finally, we have $\delta = \Delta^2$, as claimed. ///

[13.8] Let $t$ be an integer. If the image of $t$ in $\mathbf{Z}/p$ is a square for every prime $p$, is $t$ necessarily a square?

*Yes*, but we need not only Quadratic Reciprocity but also Dirichlet's theorem on primes in arithmetic progressions to see this. Dirichlet's theorem, which has no intelligible *purely algebraic* proof, asserts that for a positive integer $N$ and integer $a$ with $\gcd(a, N) = 1$, there are infinitely many primes $p$ with $p = a \bmod N$.

Factor $t$ into prime powers $t = \varepsilon p_1^{m_1} \ldots p_n^{m_n}$ where $\varepsilon = \pm 1$, the $p_i$ are primes, and the $m_i$ are positive integers. Since $t$ is not a square either $\varepsilon = -1$ or some exponent $m_i$ is *odd*.

If $\varepsilon = -1$, take $q$ to be a prime different from all the $p_i$ and $q = 3 \bmod 4$. The latter condition assures (from the cyclicness of $(\mathbf{Z}/q)^\times$) that $-1$ is not a square mod $q$, and the first condition assures that $t$ is not 0 modulo $q$. We will arrange further congruence conditions on $q$ to guarantee that each $p_i$ is a (non-zero) *square* modulo $q$. For each $p_i$, if $p_i = 1 \bmod 4$ let $b_i = 1$, and if $p_i = 3 \bmod 4$ let $b_i$ be a non-square mod $p_i$. Require of $q$ that $q = 7 \bmod 8$ and $q = b_i \bmod p_i$ for odd $p_i$. (The case of $p_i = 2$ is handled by $q = 7 \bmod 8$, which assures that 2 is a square mod $q$, by Quadratic Reciprocity.) Sun-Ze's theorem assures us that these conditions can be met simultaneously, by *integer* $q$. Then by the main part of Quadratic Reciprocity, for $p_i > 2$,

$$\left(\frac{p_i}{q}\right)_2 = (-1)^{(p_i-1)(q-1)} \cdot \left(\frac{q}{p_i}\right)_2 = \begin{cases} (-1) \cdot \left(\frac{q}{p_i}\right)_2 & (\text{for } p_i = 3 \bmod 4) \\ (+1) \cdot \left(\frac{q}{p_i}\right)_2 & (\text{for } p_i = 1 \bmod 4) \end{cases} = 1 \ \ (\text{in either case})$$

That is, all the $p_i$ are squares modulo $q$, but $\varepsilon = -1$ is not, so $t$ is a non-square modulo $q$, since Dirichlet's theorem promises that there are infinitely many (hence, at least one) primes $q$ meeting these congruence conditions.

For $\varepsilon = +1$, there must be some odd $m_i$, say $m_1$. We want to devise congruence conditions on primes $q$ such that all $p_i$ with $i \geq 2$ are squares modulo $q$ but $p_1$ is *not* a square mod $q$. Since we do not need to make $q = 3 \bmod 4$ (as was needed in the previous case), we can take $q = 1 \bmod 4$, and thus have somewhat simpler conditions. If $p_1 = 2$, require that $q = 5 \bmod 8$, while if $p_1 > 2$ then fix a non-square $b \bmod p_1$ and let $q = b \bmod p_1$. For $i \geq 2$ take $q = 1 \bmod p_i$ for odd $p_i$, and $q = 5 \bmod 8$ for $p_i = 2$. Again, Sun-Ze assures us that these congruence conditions are equivalent to a single one, and Dirichlet's theorem assures that there are *primes* which meet the condition. Again, Quadratic Reciprocity gives, for $p_i > 2$,

$$\left(\frac{p_i}{q}\right)_2 = (-1)^{(p_i-1)(q-1)} \cdot \left(\frac{q}{p_i}\right)_2 = \left(\frac{q}{p_i}\right)_2 = \begin{cases} -1 & (\text{for } i = 1) \\ +1 & (\text{for } i \geq 2) \end{cases}$$

The case of $p_i = 2$ was dealt with separately. Thus, the product $t$ is the product of a *single* non-square mod $q$ and a bunch of squares modulo $q$, so is a non-square mod $q$.

**Remark:** And in addition to everything else, it is worth noting that for the 4 choices of odd $q$ modulo 8, we achieve all 4 of the different effects

$$\left(\frac{-1}{q}\right)_2 = \pm 1 \qquad \left(\frac{2}{q}\right)_2 = \pm 1$$

[13.9] Find the irreducible factors of $x^5 - 4$ in $\mathbf{Q}[x]$. In $\mathbf{Q}(\zeta)[x]$ with a primitive fifth root of unity $\zeta$.

First, by Eisenstein's criterion, $x^5 - 2$ is irreducible over $\mathbf{Q}$, so the fifth root of 2 generates a quintic extension of $\mathbf{Q}$. Certainly a fifth root of 4 lies in such an extension, so must be either rational or generate the quintic extension, by multiplicativity of field extension degrees in towers. Since $4 = 2^2$ is not a fifth power in $\mathbf{Q}$, the fifth root of 4 generates a quintic extension, and its minimal polynomial over $\mathbf{Q}$ is necessarily quintic. The given polynomial is at worst a multiple of the minimal one, and has the right degree, so is *it*. That is, $x^5 - 4$ is irreducible in $\mathbf{Q}[x]$. (*Comment:* I had overlooked this trick when I thought the problem up, thinking, instead, that one would be forced to think more in the style of the *Kummer* ideas indicated below.)

Yes, it is true that irreducibility over the larger field would imply irreducibility over the smaller, but it might be difficult to see directly that 4 is not a fifth power in $\mathbf{Q}(\zeta)$. For example, we do not know anything about the behavior of the ring $\mathbf{Z}[\zeta]$, such as whether it is a UFD or not, so we cannot readily attempt to invoke Eisenstein. Thus, our *first* method to prove irreducibility over $\mathbf{Q}(\zeta)$ uses the irreducibility over $\mathbf{Q}$.

Instead, observe that the field extension obtained by adjoining $\zeta$ is quartic over $\mathbf{Q}$, while that obtained by adjoining a fifth root $\beta$ of 4 is quintic. Any field $K$ containing both would have degree divisible by both degrees (by multiplicativity of field extension degrees in towers), and at most the product, so in this case exactly 20. As a consequence, $\beta$ has *quintic* minimal polynomial over $\mathbf{Q}(\zeta)$, since $[K : \mathbf{Q}(\zeta)] = 5$ (again by multiplicativity of degrees in towers). That is, the given quintic must be that minimal polynomial, so is irreducible. ///

*Another* approach to prove irreducibility of $x^5 - 4$ in $\mathbf{Q}[x]$ is to prove that it is irreducible modulo some prime $p$. To have some elements of $\mathbf{Z}/p$ not be $5^{\text{th}}$ powers we need $p = 1 \bmod 5$ (by the cyclic-ness of $(\mathbf{Z}/p)^\times$), and the smallest candidate is $p = 11$. First, 4 is not a fifth power in $\mathbf{Z}/11$, since the only fifth powers are $\pm 1$ (again using the cyclic-ness to make this observation easy). In fact, $2^5 = 32 = -1 \bmod 11$, so we can infer that 2 is a generator for the order 11 cyclic group $(\mathbf{Z}/11)^\times$. Then if $4 = \alpha^5$ for some $\alpha \in \mathbf{F}_{11^2}$, also $\alpha^{11^2-1} = 1$ and $4^5 = 1 \bmod 11$ yield

$$1 = \alpha^{11^2-1} = (\alpha^5)^{24} = 4^{24} = 4^4 = 5^2 = 2 \bmod 11$$

which is false. Thus, $x^5 - 4$ can have no linear or quadratic factor in $\mathbf{Q}[x]$, so is irreducible in $\mathbf{Q}[x]$. (*Comment:* And I had overlooked *this* trick, too, when I thought the problem up.)

*Yet another approach*, which illustrates more what happens in Kummer theory, is to grant ourselves just that $a$ is not a $5^{\text{th}}$ power in $\mathbf{Q}(\zeta)$, and prove irreducibility of $x^5 - a$. That $a$ is not a $5^{\text{th}}$ power in $\mathbf{Q}(\zeta)$ can be proven without understanding much about the ring $\mathbf{Z}[\zeta]$ (if we are slightly lucky) by taking *norms* from $\mathbf{Q}(\zeta)$ to $\mathbf{Q}$, in the sense of writing

$$N(\beta) = \prod_{\tau \in \mathrm{Aut}(\mathbf{Q}(\zeta)/\mathbf{Q})} \tau(\beta)$$

In fact, we know that $\mathrm{Aut}(\mathbf{Q}(\zeta)/\mathbf{Q}) \approx (\mathbf{Z}/5)^\times$, generated (for example) by $\sigma_2(\zeta) = \zeta^2$. We compute directly that $N$ takes values in $\mathbf{Q}$: for lightness of notation let $\tau = \sigma_2$, and then

$$\tau(N\beta) = \tau\left(\beta \cdot \tau\beta \cdot \tau^2\beta \cdot \tau^3\beta\right) = \tau\beta \cdot \tau^2\beta \cdot \tau^3\beta \cdot \tau^4\beta$$

$$= \beta \cdot \tau\beta \cdot \tau^2\beta \cdot \tau^3\beta = N(\beta)$$

since $\tau^4 = 1$, by rearranging. Since we are inside a cyclotomic field, we already know the (proto-Galois theory) fact that invariance under all automorphisms means the thing lies inside $\mathbf{Q}$, as claimed. And since $\tau$ is an automorphism, the norm $N$ is multiplicative (as usual). Thus, if $\beta = \gamma^5$ is a fifth power, then

$$N(\beta) = N(\gamma^5) = N(\gamma)^5$$

is a fifth power of a rational number. The norm of $\beta = 4$ is easy to compute, namely

$$N(4) = 4 \cdot 4 \cdot 4 \cdot 4 = 2^8$$

which is not a fifth power in $\mathbf{Q}$ (by unique factorization). So, without knowing much about the ring $\mathbf{Z}[\zeta]$, we do know that 4 does not become a fifth power there.

Let $\alpha$ be a fifth root of 4. Then, in fact, the complete list of fifth roots of 4 is $\alpha, \zeta\alpha, \zeta^2\alpha, \zeta^3\alpha, \zeta^4\alpha$. If $x^5 - 4$ factored properly in $\mathbf{Q}(\zeta)[x]$, then it would have a linear or quadratic factor. There can be no linear factor, because (as we just showed) there is no fifth root of 4 in $\mathbf{Q}(\zeta)$. If there were a proper *quadratic* factor it would have to be of the form (with $i \neq j \bmod 5$)

$$(x - \zeta^i\alpha)(x - \zeta^j\alpha) = x^2 - (\zeta^i + \zeta^j)\alpha x + \zeta^{i+j}\alpha^2$$

Since $\alpha \notin \mathbf{Q}(\zeta)$, this would require that $\zeta^i + \zeta^j = 0$, or $\zeta^{i-j} = -1$, which does not happen. Thus, we have irreducibility.

**Remark:** This last problem is a precursor to *Kummer theory.* As with cyclotomic extensions of fields, extensions by $n^{\text{th}}$ roots have the simplicity that we have an explicit and simple form for *all* the roots in terms of a given one. This is not typical.