20. Cyclotomic III

The main goal is to prove that all cyclotomic polynomials $\Phi_n(x)$ are irreducible in $\mathbb{Q}[x]$, and to see what happens to $\Phi_n(x)$ over $\mathbb{F}_p$ when $p|n$.

The irreducibility over $\mathbb{Q}$ allows us to conclude that the automorphism group of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ (with ζ_n a primitive n^{th} root of unity) is

$$\mathrm{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \approx (\mathbb{Z}/n)^\times$$

by the map

$$(\zeta_n \longrightarrow \zeta_n^a) \longleftarrow a$$

The case of prime-power cyclotomic polynomials in $\mathbb{Q}[x]$ needs only Eisenstein's criterion, but the case of general n seems to admit no comparably simple argument. The proof given here uses ideas already in hand, but also an unexpected trick. We will give a different, less elementary, but possibly more natural argument later using p-adic numbers and Dirichlet's theorem on primes in an arithmetic progression.

---

1. *Prime-power cyclotomic polynomials over* $\mathbb{Q}$

The proof of the following is just a slight generalization of the prime-order case.

[1.0.1] **Proposition:** For p prime and for $1 \leq e \in \mathbb{Z}$ the prime-power p^e-th cyclotomic polynomial $\Phi_{p^e}(x)$ is irreducible in $\mathbb{Q}[x]$.

Proof: Not unexpectedly, we use Eisenstein's criterion to prove that $\Phi_{p^e}(x)$ is irreducible in $\mathbb{Z}[x]$, and the invoke Gauss' lemma to be sure that it is irreducible in $\mathbb{Q}[x]$. Specifically, let

$$f(x) = \Phi_{p^e}(x+1)$$

If $e = 1$, we are in the familiar prime-order case. Since p divides binomial coefficients $\binom{p}{i}$ for $0 < i < p$

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = x^{p-1} + \binom{p}{1}x^{p-2} + \ldots + \binom{p}{2}x + \binom{p}{1}$$

reaching the usual conclusion directly in this case.

Now consider $e > 1$. Let

$$f(x) = \Phi_{p^e}(x+1)$$

Recall that

$$\Phi_{p^e}(x) = \Phi_p(x^{p^{e-1}}) = \frac{x^{p^e} - 1}{x^{p^{e-1}} - 1}$$

First, we check that p divides all but the highest-degree coefficient of $f(x)$. To do so, map everything to $\mathbb{F}_p[x]$, by reducing coefficients modulo p. For $e \geq 1$

$$(x+1)^{p^{e-1}} = x^{p^{e-1}} + 1 \bmod p$$

Therefore, in $\mathbb{F}_p[x]$

$$f(x) = \Phi_p((x+1)^{p^{e-1}}) = \frac{(x+1)^{p^e} - 1}{(x+1)^{p^{e-1}} - 1}$$

$$= ((x+1)^{p^{e-1}})^{p-1} + ((x+1)^{p^{e-1}})^{p-2} + \ldots + ((x+1)^{p^{e-1}}) + 1$$

$$= (x^{p^{e-1}}+1)^{p-1} + (x^{p^{e-1}}+1)^{p-2} + \ldots + (x^{p^{e-1}}+1) + 1$$

$$= \frac{(x^{p^{e-1}}+1)^p - 1}{(x^{p^{e-1}}+1) - 1} = \frac{x^{p^{e-1}}+1-1}{x^{p^{e-1}}} = \frac{x^{p^e}}{x^{p^{e-1}}} = x^{p^{e-1}(p-1)}$$

in $\mathbb{F}_p[x]$. Thus, all the lower coefficients are divisible by p. [1] To determine the constant coefficient of $f(x)$, again use

$$\Phi_{p^e}(x) = \Phi_p(x^{p^{e-1}})$$

to compute

$$\text{constant coefficient of } f = f(0) = \Phi_{p^e}(1) = \Phi_p(1^{p^{e-1}}) = \Phi_p(1) = p$$

as in the prime-order case. Thus, p^2 does not divide the constant coefficient of f. Then apply Eisenstein's criterion and Gauss' lemma to obtain the irreducibility. ///

[1.0.2] Corollary: Let ζ be a primitive p^e-th root of unity. The automorphism group $\mathrm{Aut}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is isomorphic

$$(\mathbb{Z}/p^e)^\times \approx \mathrm{Aut}(\mathbb{Q}(\zeta)/\mathbb{Q})$$

by

$$a \longrightarrow \sigma_a$$

where

$$\sigma_a(\zeta) = \zeta^a$$

[1] Note that this argument in $\mathbb{F}_p[x]$ by itself cannot prove that p^2 does not divide the constant coefficient, since we are computing only in $\mathbb{F}_p[x]$.

Proof: This follows from the irreducibility of $\Phi_{p^e}(x)$ in $\mathbb{Q}[x]$ and the fact that all primitive p^e-th roots of unity are expressible as ζ^a with a in $(\mathbb{Z}/p^e)^\times$. More precisely, we saw earlier that for any other root β of $f(x) = 0$ in $\mathbb{Q}(\alpha)$ with f the minimal polynomial of α over $\mathbb{Q}$, there is an automorphism of $\mathbb{Q}(\alpha)$ sending α to β. Thus, for any a relatively prime to p there is an automorphism which sends $\zeta \longrightarrow \zeta^a$. On the other hand, any automorphism must send ζ to a root of $\Phi_{p^e}(x) = 0$, and these are all of the form ζ^a. Thus, we have an isomorphism. ///

---

2. *Irreducibility of cyclotomic polynomials over* $\mathbb{Q}$

Now consider general n, and ζ a primitive n^{th} root of unity. We prove irreducibility over $\mathbb{Q}$ of the n^{th} cyclotomic polynomial, and the very useful corollary that the automorphism group of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ (for a primitive n^{th} root of unity ζ_n) is isomorphic to $(\mathbb{Z}/n)^\times$.

[2.0.1] **Theorem:** The n^{th} cyclotomic polynomial $\Phi_n(x)$ is irreducible in $\mathbb{Q}[x]$.

Proof: Suppose that $\Phi_n(x) = f(x)g(x)$ in $\mathbb{Q}[x]$ with f of positive degree. Via Gauss' lemma we can suppose that both f and g are monic and are in $\mathbb{Z}[x]$. Let $x - \zeta$ be a linear factor of $f(x)$ in $k[x]$ for an extension field k of $\mathbb{Q}$. We wish to show that $x - \zeta^a$ is also a linear factor of f for every $a \in (\mathbb{Z}/n)^\times$, and thus that

$$\deg f = \varphi(n) = \deg \Phi_n$$

concluding that $f = \Phi_n$.

Since each $a \in (\mathbb{Z}/n)^\times$ is a product of primes p not dividing n, it suffices to show that $x - \zeta^p$ is a linear factor of $f(x)$ for all primes p not dividing n. If not, then $x - \zeta^p$ is necessarily a linear factor of $g(x)$, by unique factorization in $k[x]$. That is, ζ is a root of $g(x^p) = 0$ in k, so $x - \zeta$ divides $g(x^p)$ in $k[x]$.

Thus, in $\mathbb{Q}[x]$ the *gcd* of $f(x)$ and $g(x^p)$ is not 1: otherwise, there would be $r(x), s(x) \in Q[x]$ such that

$$1 = r(x) \cdot f(x) + s(x) \cdot g(x^p)$$

Mapping $\mathbb{Q}[x]$ to k by $x \longrightarrow \zeta$ would give the impossible

$$1 = r(\zeta) \cdot 0 + s(\zeta) \cdot 0 = 0$$

Thus, $d(x) = \gcd(f(x), g(x^p))$ in $\mathbb{Q}[x]$ is of positive degree. Let $a(x)$ and $b(x)$ be in $\mathbb{Q}[x]$ such that

$$f(x) = a(x) \cdot d(x) \qquad g(x^p) = b(x) \cdot d(x)$$

We can certainly take d to be in $\mathbb{Z}[x]$ and have content 1. By Gauss' lemma, $a(x)$ and $b(x)$ are in $\mathbb{Z}[x]$ and have content 1. In fact, adjusting by at most ± 1, we can take $a(x)$, $b(x)$, and $d(x)$ all to be monic.

Map everything to $\mathbb{F}_p[x]$. There $g(x^p) = g(x)^p$, so

$$\begin{cases} f(x) & = & a(x) \cdot d(x) \\ g(x)^p = g(x^p) & = & b \cdot d \end{cases}$$

Let $\delta(x) \in \mathbb{F}_p[x]$ be an irreducible dividing $d(x)$ in $\mathbb{F}_p[x]$. Then since $\delta(x)$ divides $g(x)^p$ in $\mathbb{F}_p[x]$ it divides $g(x)$. Also $\delta(x)$ divides $f(x)$ in $\mathbb{F}_p[x]$, so $\delta(x)^2$ apparently divides $\Phi_n(x) = f(x) \cdot g(x)$ in $\mathbb{F}_p[x]$. But p does not divide n, so $\Phi_n(x)$ has no repeated factor in $\mathbb{F}_p[x]$, contradiction. Thus, it could not have been that $\Phi_n(x)$ factored properly in $\mathbb{Q}[x]$. ///

[2.0.2] **Corollary:** Let ζ be a primitive n-th root of unity. The automorphism group $\mathrm{Aut}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is isomorphic

$$(\mathbb{Z}/n)^\times \approx \mathrm{Aut}(\mathbb{Q}(\zeta)/\mathbb{Q})$$

by

$$a \longrightarrow \sigma_a$$

where

$$\sigma_a(\zeta) = \zeta^a$$

Proof: This follows from the irreducibility of $\Phi_n(x)$ in $\mathbb{Q}[x]$ and the fact that all primitive n-th roots of unity are expressible as ζ^a with a in $(\mathbb{Z}/n)^\times$. More precisely, we saw earlier that for any other root β of $f(x) = 0$ in $\mathbb{Q}(\alpha)$ with f the minimal polynomial of α over $\mathbb{Q}$, there is an automorphism of $\mathbb{Q}(\alpha)$ sending α to β. Thus, for any a relatively prime to n there is an automorphism which sends $\zeta \longrightarrow \zeta^a$. On the other hand, any automorphism must send ζ to a root of $\Phi_n(x) = 0$, and these are all of the form ζ^a, because of the nature of cyclic groups. Thus, we have an isomorphism. ///

---

3. *Factoring $\Phi_n(x)$ in $\mathbb{F}_p[x]$ with $p|n$*

It turns out that a sensible proof of the following can be given using only the inductive definition of $\Phi_n(x)$ in $\mathbb{Z}[x]$.

[3.0.1] **Theorem:** For a prime p, integer m not divisible by p, and integer $e \geq 1$, in $\mathbb{F}_p[x]$ the $p^e m^{th}$ cyclotomic polynomial $\Phi_{p^e m}(x)$ is

$$\Phi_{p^e m}(x) = \Phi_m(x)^{\varphi(p^e)} = \Phi_m(x)^{(p-1)(p^{e-1})}$$

where φ is Euler's totient function.

Proof: From the recursive definition, for $1 \leq e \in \mathbb{Z}$,

$$\Phi_{p^e m}(x) = \frac{x^{p^e m} - 1}{\prod_{d|m,\ 0\leq\varepsilon<e} \Phi_{p^\varepsilon d}(x) \cdot \prod_{d|m,\ d<m} \Phi_{p^e d}(x)}$$

In characteristic p, the numerator is $(x^m - 1)^{p^e}$. The first product factor in the denominator is $x^{p^{e-1}m} - 1$, which in characteristic p is $(x^m - 1)^{p^{e-1}}$. Thus, the whole is

$$\Phi_{p^e m}(x) = \frac{(x^m - 1)^{p^e}}{(x^m - 1)^{p^{e-1}} \cdot \prod_{d|m,\ d<m} \Phi_{p^e d}(x)}$$

By induction on $d < m$, in the last product in the denominator has factors

$$\Phi_{p^e d}(x) = \Phi_d(x)^{\varphi(p^e)}$$

Cancelling,

$$\Phi_{p^e m}(x) = \frac{(x^m - 1)^{p^e}}{(x^m - 1)^{p^{e-1}} \cdot \prod_{d|m,\ d<m} \Phi_d(x)^{\varphi(p^e)}}$$

$$= \frac{(x^m - 1)^{(p-1)p^{e-1}}}{\prod_{d|m,\ d<m} \Phi_d(x)^{\varphi(p^e)}} = \left(\frac{x^m - 1}{\prod_{d|m,\ d<m} \Phi_d(x)}\right)^{\varphi(p^e)}$$

which gives $\Phi_m(x)^{\varphi(p^e)}$ as claimed, by the recursive definition. ///

---

4. *Worked examples*

[20.1] Prove that a prime p such that $p = 1 \bmod 3$ factors *properly* as $p = ab$ in $\mathbb{Z}[\omega]$, where ω is a primitive cube root of unity. (*Hint:* If p were prime in $\mathbb{Z}[\omega]$, then $\mathbb{Z}[\omega]/p$ would be a integral domain.)

The hypothesis on p implies that $(\mathbb{Z}/p)^\times$ has order divisible by 3, so there is a primitive third root of unity ζ in $\mathbb{Z}/p$. That is, the third cyclotomic polynomial $x^2 + x + 1$ factors mod p. Recall the isomorphisms

$$\mathbb{Z}[\omega]/p \approx (\mathbb{Z}[x]/(x^2 + x + 1))/p \approx (\mathbb{Z}/p)[x]/(x^2 + x + 1)$$

Since $x^2 + x + 1$ factors mod p, the right-most quotient is *not* an integral domain. Recall that a commutative ring modulo an ideal is an integral domain if and only if the ideal is prime. Thus, looking at the left-most quotient, the ideal generated by p in $\mathbb{Z}[\omega]$ is not prime. Since we have seen that $\mathbb{Z}[\omega]$ is Euclidean, hence a PID, the element p must factor properly. ///

[20.2] Prove that a prime p such that $p = 2 \bmod 5$ generates a prime ideal in the ring $\mathbb{Z}[\zeta]$, where ζ is a primitive fifth root of unity.

The hypothesis on p implies that $\mathbb{F}_{p^n}^\times$ has order divisible by 5 only for n divisible by 4. Thus, the fifth cyclotomic polynomial Φ_5 is irreducible modulo p: (If it had a linear factor then $\mathbb{F}_p^\times$ would contain a primitive fifth root of unity, so have order divisible by 5. If it had a quadratic factor then $\mathbb{F}_{p^2}^\times$ would contain a primitive fifth root of unity, so have order divisible by 5.) Recall the isomorphisms

$$\mathbb{Z}[\zeta]/p \approx (\mathbb{Z}[x]/\Phi_5)/p \approx (\mathbb{Z}/p)[x]/(\Phi_5)$$

Since Φ_5 is irreducible mod p, the right-most quotient is an integral domain. As recalled in the previous example, a commutative ring modulo an ideal is an integral domain if and only if the ideal is prime. Thus, looking at the left-most quotient, the ideal generated by p in $\mathbb{Z}[\zeta]$ is prime. ///

[20.3] Find the monic irreducible polynomial with rational coefficients which has as zero

$$\alpha = \sqrt{3} + \sqrt{5}$$

In this simple example, we can take a rather *ad hoc* approach to find a polynomial with α as 0. Namely,

$$\alpha^2 = 3 + 2\sqrt{3}\sqrt{5} + 5 = 8 + 2\sqrt{15}$$

Then

$$(\alpha^2 - 8)^2 = 4 \cdot 15 = 60$$

Thus,

$$\alpha^4 - 16\alpha^2 + 4 = 0$$

But this approach leaves the question of the irreducibility of this polynomial over $\mathbb{Q}$.

By Eisenstein, $x^2 - 3$ and $x^2 - 5$ are irreducible in $\mathbb{Q}[x]$, so the fields generated over $\mathbb{Q}$ by the indicated square roots are of degree 2 over $\mathbb{Q}$. Since (inside a fixed algebraic closure of $\mathbb{Q}$) $[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] \leq [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] \cdot [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]$,

$$[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] \leq 4$$

It is natural to claim that we have equality. To prove equality, one approach is to show that there is no $\sqrt{5}$ in $\mathbb{Q}(\sqrt{3})$: supposed that $(a + b\sqrt{3})^2 = 5$ with $a, b \in \mathbb{Q}$. Then

$$(a^2 - 3b^2) + 2ab\sqrt{3} = 5 = 5 + 0 \cdot \sqrt{3}$$

Since $\sqrt{3}$ and 1 are linearly independent over $\mathbb{Q}$ (this is what the field degree assertions are), this requires that either $a = 0$ or $b = 0$. In the latter case, we would have $a^2 = 5$. In the former, $3b^2 = 5$. In either case,

Eisenstein's criterion (or just unique factorization in $\mathbb{Z}$) shows that the corresponding polynomials $x^2 - 5$ and $3x^2 - 5$ are irreducible, so this is impossible.

To prove that the quartic of which $\alpha = \sqrt{3} + \sqrt{5}$ is a root is irreducible, it suffices to show that α generates $\mathbb{Q}(\sqrt{3}, \sqrt{5})$. Certainly

$$\frac{\alpha^2 - 8}{2} = \sqrt{15}$$

(If we were in characteristic 2 then we could not divide by 2. But, also, in that case $3 = 5$.) Then

$$(\frac{\alpha^2 - 8}{2}) \cdot \alpha = \sqrt{15} \cdot \alpha = 3\sqrt{5} + 5\sqrt{3}$$

The system of two linear equations

$$\begin{array}{rcl} \sqrt{3} + \sqrt{5} & = & \alpha \\ 5\sqrt{3} + 3\sqrt{5} & = & (\frac{\alpha^2 - 8}{2}) \cdot \alpha \end{array}$$

can be solved for $\sqrt{3}$ and $\sqrt{5}$. Thus, α generates the quartic field extension, so has a quartic minimal polynomial, which must be the monic polynomial we found. ///

A more extravagant proof (which generalizes in an attractive manner) that

$$[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 4$$

uses cyclotomic fields and (proto-Galois theoretic) facts we already have at hand about them. Let ζ_n be a primitive n^{th} root of unity. We use the fact that

$$\mathrm{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \approx (\mathbb{Z}/n)^\times$$

by

$$(\sigma_a : \zeta_n \longrightarrow \zeta_n^a) \longleftarrow a$$

Letting $n = 4pq$ with distinct odd primes p, q, by Sun-Ze's theorem

$$\mathbb{Z}/n \approx \mathbb{Z}/4 \oplus \mathbb{Z}/p \oplus \mathbb{Z}/q$$

Thus, given an automorphism τ_1 of $\mathbb{Q}(\zeta_p)$ over $\mathbb{Q}$, an automorphism τ_2 of $\mathbb{Q}(\zeta_q)$ over $\mathbb{Q}$, and an automorphism τ_3 of $\mathbb{Q}(i)$ over $\mathbb{Q}$, there is an automorphism σ of $\mathbb{Q}(\zeta_{4pq})$ over $\mathbb{Q}$ which restricts to τ_1 on $\mathbb{Q}(\zeta_p)$, to τ_2 on $\mathbb{Q}(\zeta_2)$, and to τ_3 on $\mathbb{Q}(i)$. Also,

$$\sqrt{p \cdot \left(\frac{-1}{p}\right)_2} \quad \in \quad \mathbb{Q}(\text{primitive } p^{th} \text{ root of unity})$$

In particular, letting ζ_p be a primitive p^{th} root of unity, the Gauss sum expression

$$\sqrt{p \cdot \left(\frac{-1}{p}\right)_2} = \sum_{b \bmod p} \left(\frac{b}{p}\right)_2 \cdot \zeta_p^b$$

shows (as observed earlier) that

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

The signs under the radicals can be removed by removing a factor of i, if necessary. Thus, we can choose $a \in (\mathbb{Z}/4pq)^\times$ with $a = 1 \bmod 4$ to assure that $\sigma_a(i) = i$, and

$$\begin{cases} \sigma_a(\sqrt{p}) & = & -\sqrt{p} \\ \sigma_a(\sqrt{q}) & = & \sqrt{q} \end{cases}$$

That is, a is any non-zero square modulo q and is a non-square modulo p. That is, σ_a is an automorphism of $\mathbb{Q}(\zeta_{4pq})$ which properly moves $\sqrt{p}$ but does not move $\sqrt{q}$. Thus, σ_a is trivial on $\mathbb{Q}(\sqrt{q}$, so this field cannot contain $\sqrt{p}$. Thus, the degree $[\mathbb{Q}(\sqrt{p},\sqrt{q}) : \mathbb{Q}] > 2$. But also this degree is at most 4, and is divisible by $[\mathbb{Q}(\sqrt{q}) : \mathbb{Q}] = 2$. Thus, the degree is 4, as desired. ///

[20.4] Find the monic irreducible polynomial with rational coefficients which has as zero

$$\alpha = \sqrt{3} + \sqrt[3]{5}$$

Eisenstein's criterion shows that $x^2 - 3$ and $x^3 - 5$ are irreducible in $\mathbb{Q}[x]$, so the separate field degrees are as expected: $[\mathbb{Q}\sqrt{3}) : \mathbb{Q}] = 2$, and $[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = 3$. This case is somewhat simpler than the case of two square roots, since the degree $[\mathbb{Q}(\sqrt{3}, \sqrt[3]{5}) : \mathbb{Q}]$ of any compositum is divisible by both $2 = [\mathbb{Q}(\sqrt{3})]$ and $3 = [\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = 3$, so is divisible by $6 = \text{lcm}(2, 3)$. On the other hand, it is at most the product $6 = 2 \cdot 3$ of the two degrees, so is exactly 6.

To find a sextic over $\mathbb{Q}$ satisfied by α, we should be slightly more clever. Note that immediately

$$(\alpha - \sqrt{3})^3 = 5$$

which is

$$\alpha^3 - 3\sqrt{3}\alpha^2 + 3 \cdot 3\alpha - 3\sqrt{3} = 5$$

Moving all the square roots to one side,

$$\alpha^3 + 9\alpha - 5 = \sqrt{3} \cdot 3 \cdot (\alpha^2 + 1)$$

and then square again to obtain

$$\alpha^6 + 81\alpha^2 + 25 + 18\alpha^4 - 10\alpha^3 - 90\alpha = 27(\alpha^4 + 2\alpha^2 + 1)$$

Rearranging gives

$$\alpha^6 - 9\alpha^4 - 10\alpha^3 + 27\alpha^2 - 90\alpha - 2 = 0$$

Thus, since α is of degree 6 over $\mathbb{Q}$, the polynomial

$$x^6 - 9x^4 - 10x^3 + 27x^2 - 90x - 2$$

of which α is a zero is irreducible. ///

[20.5] Find the monic irreducible polynomial with rational coefficients which has as zero

$$\alpha = \frac{1 + \sqrt[3]{10} + \sqrt[3]{10}^2}{3}$$

First, by Eisenstein's criterion $x^3 - 10$ is irreducible over $\mathbb{Q}$, so $\sqrt[3]{10}$ generates a cubic extension of $\mathbb{Q}$, and thus 1, $\sqrt[3]{10}$, and $\sqrt[3]{10}^2$ are linearly independent over $\mathbb{Q}$. Thus, α is not in $\mathbb{Q}$. Since it lies inside a cubic field extension of $\mathbb{Q}$, it satisfies a monic cubic equation with rational coefficients. The issue, then, is to find the cubic.

First we take advantage of the special nature of the situation. A little more generally, let $\beta^3 = A$ with $A \neq 1$. We note that

$$\beta^2 + \beta + 1 = \frac{\beta^3 - 1}{\beta - 1} = \frac{A - 1}{\beta - 1}$$

From $\beta^3 - A = 0$, using $\beta = (b\eta - 1) + 1$, we have

$$(\beta - 1)^3 + 3(\beta - 1)^2 + 3(\beta - 1)^2 - (A - 1) = 0$$

Dividing through by $(\beta - 1)^3$ gives

$$1 + 3(\frac{1}{\beta - 1}) + 3(\frac{1}{\beta - 1})^2 - \frac{A - 1}{(\beta - 1)^3} = 0$$

Multiplying through by $-(A - 1)^2$ and reversing the order of the terms gives

$$(\frac{A - 1}{\beta - 1})^3 - 3(\frac{A - 1}{\beta - 1})^2 - 3(A - 1)(\frac{A - 1}{\beta - 1}) - (A - 1)^2 = 0$$

That is, $1 + \sqrt[3]{A} + \sqrt[3]{A}^2$ is a root of

$$x^3 - 3x^2 - 3(A - 1)x - (A - 1)^2 = 0$$

Then $(1 + \sqrt[3]{A} + \sqrt[3]{A}^2)/3$ is a root of

$$x^3 - x^2 - (\frac{A - 1}{3})x - \frac{(A - 1)^2}{27} = 0$$

When $(A - 1)^2$ is divisible by 27 we have a nice simplification, as with $A = 10$, in which case the cubic is

$$x^3 - x^2 - 3x - 3 = 0$$

which has *integral* coefficients. ///

[4.0.1] **Remark:** The fact that the coefficients are integral despite the apparent denominator of α is entirely parallel to the fact that $\frac{-1 \pm \sqrt{D}}{2}$ satisfies the quadratic equation

$$x^2 - x + \frac{1 - D}{4} = 0$$

which has *integral coefficients* if $D = 1 \bmod 4$.

There is a more systematic approach to finding minimal polynomials that will work in more general circumstances, which we can also illustrate in this example. Again let $\beta = \sqrt[3]{A}$ where A is not a cube in the base field k. Then, again, we know that $1 + \beta + \beta^2$ is not in the ground field k, so, since it lies in a cubic field extension, has minimal polynomial over k which is an irreducible (monic) *cubic*, say $x^3 + ax^2 + bx + c$. We can determine a, b, c systematically, as follows. Substitute $1 + \beta + \beta^2$ for x and require

$$(1 + \beta + \beta^2)^3 + a(1 + \beta + \beta^2)^2 + b(1 + \beta + \beta^2) + c = 0$$

Multiply out, obtaining

$$(\beta^6 + \beta^3 + 1 + 3\beta^5 + 3\beta^4 + 3\beta^2 + 3\beta^4 + 3\beta^2 + 3\beta + 6\beta^3)$$

$$+ a(\beta^4 + \beta^2 + 1 + 2\beta^3 + 2\beta^2 + 2\beta) + b(\beta^2 + \beta + 1) + c$$

$$= 0$$

Use the fact that $\beta^3 = A$ (if β satified a more complicated cubic this would be messier, but still succeed) to obtain

$$(3A + 6 + 3a + b)\beta^2 + (6A + 3 + (A + 2)a + +b)\beta$$

$$+ (A^2 + 7A + 1 + (2A+1)a + b + c) = 0$$

Again, $1, \beta, \beta^2$ are linearly independent over the ground field k, so this condition is equivalent to the system

$$\begin{cases} 3a & + & b & & & = & -(3A+6) \\ (A+2)a & + & b & & & = & -(6A+3) \\ (2A+1)a & + & b & + & c & = & -(A^2+7A+1) \end{cases}$$

From the first two equations $a = -3$, and then $b = -3(A-1)$, and from the last $c = -(A-1)^2$, exactly as earlier. ///

[4.0.2] **Remark:** This last approach is only palatable if there's no other recourse.

[20.6] Let p be a prime number, and $a \in \mathbb{F}_p^\times$. Prove that $x^p - x + a$ is irreducible in $\mathbb{F}_p[x]$. (*Hint*: Verify that if α is a root of $x^p - x + a = 0$, then so is $\alpha + 1$.)

Comment: It might have been even more helpful to recommend to look at the effect of Frobenious $b \longrightarrow b^p$, but the hint as given reveals an interesting fact in its own right, and takes us part of the way to understanding the situation.

If α is a root in an algebraic closure, then

$$(\alpha+1)^p - (\alpha+1) + a = \alpha^p + 1 - \alpha - 1 + a = 0$$

so $\alpha + 1$ is another root. Thus, the roots of this equation are exactly

$$\alpha,\ \alpha+1,\ \alpha+2,\ \dots,\ \alpha+(p-1)$$

which are distinct. (The polynomial is of degree p, so there are no more than p zeros.)

Similarly, but even more to the point is that the Frobenius automorphism F has the effect

$$F(\alpha) = \alpha^p = (\alpha^p - \alpha + a) + \alpha - a = \alpha - a$$

Let A be a subset of this set of zeros. We have shown that a polynomial

$$\prod_{\beta \in A} (x - \beta)$$

has coefficients in $\mathbb{F}_p$ if and only if A is stable under the action of the Frobenius. Since $a \neq 0$, the smallest F-stable subset of A is necessarily the whole, since the values

$$F^\ell(\alpha) = \alpha - \ell \cdot a$$

are distinct for $\ell = 0, 1, \dots, p-1$. By unique factorization, any factor of $x^p - x + 1$ is a product of linear factors $x - F^\ell(\alpha)$, and we have shown that a product of such factors has coefficients in $\mathbb{F}_p$ only if *all* these factors are included. That is, $x^p - x + a$ is irreducible in $\mathbb{F}_p[x]$. ///

[20.7] Let $k = \mathbb{F}_p(t)$ be the field of rational expressions in an indeterminate t with coefficients in $\mathbb{F}_p$. Show that the polynomial $X^p - t \in k[X]$ is irreducible in $k[X]$, but has properly repeated factors over an algebraic closure of k.

That polynomial meets Eisenstein's criterion in $\mathbb{F}_p[t][X]$, since t is a prime element in the UFD $\mathbb{F}_p[t]$, so (via Gauss' lemma) $X^p - t$ is irreducible in $\mathbb{F}_p(t)[X]$. Let α be any root of $X^p - t = 0$. Then, because the inner binomial coefficients $\binom{p}{i}$ are divisible by p,

$$(X - \alpha)^p = X^p - \alpha^p = X^p - t$$

That is, over an algebraic closure of $\mathbb{F}_p(t)$, the polynomial $X^p - t$ is a linear polynomial raised to the p^{th} power.

[20.8] Let x be an indeterminate over $\mathbb{C}$. For a, b, c, d in $\mathbb{C}$ with $ad - bc \neq 0$, let

$$\sigma(x) = \sigma_{a,b,c,d}(x) = \frac{ax + b}{cx + d}$$

and define

$$\sigma\left(\frac{P(x)}{Q(x)}\right) = \frac{P(\sigma(x))}{Q(\sigma(x))}$$

for P and Q polynomials. Show that σ gives a field automorphism of the field of rational functions $\mathbb{C}(x)$ over $\mathbb{C}$.

The argument uses no properties of the complex numbers, so we discuss an arbitrary field k instead of $\mathbb{C}$.

Since the polynomial algebra $k[x]$ is the free k-algebra on one generator, by definition for any k-algebra A and chosen element $a \in A$, there is a unique k-algebra map $k[x] \longrightarrow A$ such that $x \longrightarrow a$. And, second, for any *injective* k-algebra map f of $k[x]$ to a *domain* R the field of fractions $k(x)$ of $k[x]$ has an associated map $\tilde{f}$ to the field of fractions of R, by

$$\tilde{f}(P/Q) = f(P)/f(Q)$$

where P and Q are polynomials.

In the case at hand, any choice $\sigma(x) = g(x)/h(x)$ in $k(x)$ (with polynomials g, h with h not the 0 polynomial) gives a unique k-algebra homomorphism $k[x] \longrightarrow k(x)$, by

$$\sigma(P(x)) = P(\sigma(x)) = P(\frac{g(x)}{h(x)})$$

To know that we have an extension to the field of fractions $k(x)$ of $k[x]$, we must check that the kernel of the map $k[x] \longrightarrow k(x)$ is non-zero. That is, we must verify for a positive-degree polynomial (assume without loss of generality that $a_n \neq 0$)

$$P(x) = a_n x^n + \ldots + a_o$$

that

$$0 \neq \sigma(P(x)) \in k(x)$$

Again,

$$\sigma(P(x)) = P(\sigma(x)) = P(\frac{g(x)}{h(x)}) = a_n(\frac{g}{h})^n + \ldots + a_o$$

$$= h^{-n} \cdot (a_n g^n + a_{n-1} g^{n-1} h + \ldots + a_1 g h^{n-1} + a_o h^n)$$

We could have assumed without loss of generality that g and h are relatively prime in $k[x]$. If the degree of g is positive, let $p(x)$ be an irreducible factor of $g(x)$. Then an equality

$$0 = a_n g^n + a_{n-1} g^{n-1} h + \ldots + a_1 g h^{n-1} + a_o h^n$$

would imply that $p|h$, contradiction. But if $\deg h > 0$ we reach a nearly identical contradiction. That is, a field map $k(x) \longrightarrow k(x)$ can send x to any element of $k(x)$ not lying in k. Thus, certainly, for $ad - bc \neq 0$, $(ax + b)/(cx + d)$ is not in k, and is a legitimate field map image of x.

To prove surjectivity of $\sigma(x) = (ax + b)/(cx + d)$, we find an inverse τ, specifically such that $\sigma \circ \tau = 1$. It may not be surprising that

$$\tau : x \longrightarrow \frac{dx - b}{-cx + a}$$

is such an inverse:

$$(\sigma\circ\tau)(x) = \frac{a(\frac{dx-b}{-cx+a})+b}{c(\frac{dx-b}{-cx+a})+d} = \frac{a(dx-b)+b(-cx+a)}{c(dx-b)+d(-cx+a)}$$

$$= \frac{(ad-bc)x-ab+ba}{cdx-cb-dcx+ad} = \frac{(ad-bc)x}{ad-bc} = x$$

That is, the given field maps are surjective. All field maps that do not map all elements to 0 are injective, so these maps are field automorphisms of $k(x)$.

[20.9] In the situation of the previous exercise, show that *every* automorphism of $\mathbb{C}(x)$ over $\mathbb{C}$ is of this form.

We did also show in the previous example that for g and h polynomials, not both constant, h not 0,

$$\sigma(x) = \frac{g(x)}{h(x)}$$

determines a field map $k(x) \longrightarrow k(x)$. If it were surjective, then there would be coefficients a_i and b_j in k such that x is expressible as

$$x = \frac{a_m\sigma(x)^m + \ldots + a_0}{b_n\sigma(x)^n + \ldots + b_0}$$

with $a_m \neq 0$ and $b_n \neq 0$. Let $\sigma(x) = p/q$ where p and q are relatively prime polynomials. Then

$$x\cdot q^{-n}(b_np^n + b_{n-1}p^{n-1}q + \ldots + b_0q^n) = q^{-m}(a_mp^m + a_{m-1}p^{m-1}q + \ldots + a_0q^m)$$

or

$$x\cdot q^{m}(b_np^n + b_{n-1}p^{n-1}q + \ldots + b_0q^n) = q^{n}(a_mp^m + a_{m-1}p^{m-1}q + \ldots + a_0q^m)$$

Collecting the only two terms lacking an explicit factor of p, we find that

$$(b_0x - a_0)\cdot q^{m+n}$$

is visibly a multiple of p. Since p and q are relatively prime and $k[x]$ is a UFD, necessarily p divides $b_0x - a_0$. Since degrees add in products, the degree of p is at most 1.

One argument to prove that $\deg q \leq 1$ is to observe that if p/q generates all of a field then so does its inverse q/p. Thus, by the previous paragraph's argument which showed that $\deg p \leq 1$, we have $\deg q \leq 1$.

For another argument concerning the denominator: a more direct computation approach does illustrate something useful about polynomial algebra: For $m > n$, we would have a polynomial equation

$$x\cdot q^{m-n}(b_np^n + b_{n-1}p^{n-1}q + \ldots + b_0q^n) = a_mp^m + a_{m-1}p^{m-1}q + \ldots + a_0q^m$$

The only term not visibly divisible by q is a_mp^m, so apparently q divides a_mp^m. Since p, q are relatively prime, this would imply that $\deg q = 0$. Similarly, for $m < n$, the polynomial equation

$$x\cdot (b_np^n + b_{n-1}p^{n-1}q + \ldots + b_0q^n) = q^{n-m}(a_mp^m + a_{m-1}p^{m-1}q + \ldots + a_0q^m)$$

implies that q divides $x\cdot b_np^n$, and the coprimality of p, q implies that $\deg q \leq 1$. If $m = n$, then the polynomial equation

$$x\cdot (b_np^n + b_{n-1}p^{n-1}q + \ldots + b_0q^n) = a_mp^m + a_{m-1}p^{m-1}q + \ldots + a_0q^m$$

implies that q divides (keeping in mind that $m = n$)

$$x\cdot b_np^n - a_mp^m = (xb_n - a_n)\cdot p^n$$

The coprimality of p, q implies that q divides $xb_n - a_n$, so $\deg q \le 1$ again in this case.

Thus, if $\sigma(x) = p/q$ gives a surjection of $k(x)$ to itself, the maximum of the degrees of p and q is 1. ///

[20.10] Let s and t be indeterminates over $\mathbb{F}_p$, and let $\mathbb{F}_p(s^{1/p}, t^{1/p})$ be the field extension of the rational function field $\mathbb{F}_p(s,t)$ obtained by adjoining roots of $X^p - s = 0$ and of $X^p - t = 0$. Show that there are infinitely-many (distinct) fields intermediate between $\mathbb{F}_p(s,t)$ and $\mathbb{F}_p(s^{1/p}, t^{1/p})$.

By Eisenstein's criterion in $k[s,t][X]$ we see that both $X^p - s$ and $X^p - t$ are irreducible in $k(s,t)[X]$, so $s^{1/p}$ and $t^{1/p}$ each generates a degree p extension of $k(s,t)$. We show that $[k(s^{1/p}, t^{1/p}) : k(s,t)] = p^2$. By Eisenstein's criterion in $\mathbb{F}_p(t)[s][X]$ the polynomial $X^p - s$ is irreducible, since the prime s in $\mathbb{F}_p(t)[s]$, but not its square, divides all but the highest term. And then $X^p - t$ is irreducible in $k(s^{1/p})[t][X]$ since the prime t in $k(s^{1/p}(s))[t]$ divides all the lower coefficients and its square does not divide the constant term.

Observe that for any polynomial $f(s,t)$, because the characteristic is p,

$$(s^{1/p} + f(s,t)t^{1/p})^p = s + f(s,t)^p\, t$$

For example, for any positive integer n

$$(s^{1/p} + s^n t^{1/p})^p = s + s^{np}\, t$$

Again, by Eisenstein's criterion in $\mathbb{F}_p(t)[s][X]$ the polynomial

$$X^p - (s + s^{np}t)$$

is irreducible, since the prime s in $\mathbb{F}_p(t)[s]$, but not its square, divides all but the highest term. Thus, the p^{th} root of any $s + s^{np}t$ generates a degree p extension of $\mathbb{F}_p(s,t)$.

We claim that for distinct positive integers m, n

$$\mathbb{F}_p(s,t,(s+s^{mp}t)^{1/p}) \neq \mathbb{F}_p(s,t,(s+s^{np}t)^{1/p})$$

To prove this, we will show that any subfield of $\mathbb{F}_p(s^{1/p}, t^{1/p})$ which contains both $(s + s^{mp}t)^{1/p}$ and $(s + s^{np}t)^{1/p}$ is the whole field $\mathbb{F}_p(s^{1/p}, t^{1/p})$, which is of degree p^2 (rather than p). Indeed,

$$(s+s^{mp}t)^{1/p} - (s+s^{np}t)^{1/p} = s^{1/p} + s^m t^{1/p} - (s^{1/p} + s^n t^{1/p}) = (s^m - s^n)t^{1/p}$$

Since $m \neq n$ we can divide by $s^m - s^n$ to obtain $t^{1/p}$. Then we can surely express $s^{1/t}$ as well. Thus, for $m \neq n$, the field obtained by adjoining the two different p^{th} roots is of degree p^2 over $\mathbb{F}_p(s,t)$, so the two degree p extensions cannot be identical (or the whole degree would be just p). ///

[4.0.3] **Remark:** From a foundational viewpoint, the above discussion is a bit glib about the interaction of s and t, and the interaction of $s^{1/n}$ and t. Though this is not the main point at the moment, detection of *implied relations* among *variables* can become serious. At present, the idea is that there are *no* relations between s and t, so relations between $s^{1/n}$ and t will not pop up. This *can* be made more precise in preparation for coping with more complicated situations later.

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

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

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

from $\mathbb{Q}(i)$ to $\mathbb{Q}$, 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 $\mathbb{Q}$, the map σ is a field automorphism of $\mathbb{Q}(i)$ over $\mathbb{Q}$. (Indeed, we showed earlier

that there exists a $\mathbb{Q}$-linear field automorphism of $\mathbb{Q}(i)$ taking i to $-i$.) Since σ 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 $\mathbb{Q}$. 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 $\mathbb{Z}$ 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 $(\mathbb{Z}/11)^\times$) $2^{(11-1)/2} = -1 \bmod 11$, or by recalling the part of Quadratic Reciprocity that asserts that 2 is a square mod p only for $p = \pm 1 \bmod 8$).

[20.12] 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.

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

[20.13] Fix a field k and an indeterminate t. Fix a positive integer $n > 1$ and let $t^{1/n}$ be an n^{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 $f : k \longrightarrow A$, and an element $a \in A$, we must show that there is a unique k-algebra homomorphism $F : k[t^{1/n}] \longrightarrow A$ extending $f : k \longrightarrow A$ and such that $F(t^{1/n}) = a$.

Let $k[x]$ be a polynomial ring in one variable, and let $f : k[x] \longrightarrow k[t^{1/n}]$ 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 $f : k[x] \longrightarrow k[t^{1/n}]$ 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, $f : k[x] \longrightarrow k[t^{1/n}]$ is an isomorphism. ///

[4.0.5] **Remark:** The vague and mildly philosophical point here was to see why an n^{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.

[20.14] 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.

[4.0.6] **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.

[4.0.7] **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 $f : R \longrightarrow S$.

[4.0.8] **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 $t \longrightarrow (at + b)/(ct + d)$, 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.

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

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

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

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

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 ζ_n be a primitive n^{th} root of unity. Recall that for an odd prime p

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

Certainly $i = \sqrt{-1} \in \mathbb{Q}(\zeta_4)$. Thus, letting $n = 4p_1p_2 \ldots p_N$, all the $\sqrt{p_1}, \ldots \sqrt{p_N}$ are in $K = \mathbb{Q}(\zeta_n)$. From the Gauss sum expression for these square roots, the automorphism $\sigma_a(\zeta_n) = \zeta_n^a$ of $\mathbb{Q}(\zeta_n)$ 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 $(\mathbb{Z}/p_i)^\times$ 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 σ_a fixes $\sqrt{p_2}, \ldots, \sqrt{p_N}$, so when restricted to $K = \mathbb{Q}(\sqrt{p_2}, \ldots, \sqrt{p_N})$ is trivial. But by design $\sigma_a(\sqrt{p_1}) = -\sqrt{p_1}$, so this square root cannot lie in K. ///

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

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

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,

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

since $[\mathbb{Q}(\sqrt{p_i}) : \mathbb{Q}] = 2$, 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 α over $\mathbb{Q}$ directly, we note that any automorphism τ of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ 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 τ. Thus, if we show that α has at least 2^N distinct images under automorphisms of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$, then the degree of f is at least 2^N. (It is at most 2^N since α 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 α 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 α, so α is of degree at least over 2^N, so is of degree exactly that. By multiplicativity of degrees in towers, it must be that α generates all of $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_N})$. ///

[20.17] 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 α and β over the field $\mathbb{Q}(s_1, s_2, s_3)$ 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 Δ^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 δ 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 $\mathbb{Q}[x, y, z]$. The UFD property implies that the product $(x-y)(x-z)(y-z)$ divides $\alpha - \beta$. Since $\delta = (\alpha - \beta)^2$, and since Δ 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 Δ^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. ///

[20.18] Let t be an integer. If the image of t in $\mathbb{Z}/p$ 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 $t = \varepsilon p_1^{m_1} \dots p_n^{m_n}$ 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 $(\mathbb{Z}/q)^\times$) 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 $p_i > 2$,

$$\left(\frac{p_i}{q}\right)_2 = (-1)^{(p_i-1)(q-1)} \cdot \left(\frac{q}{p_i}\right)_2$$

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

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 mod 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 $p_i > 2$,

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

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.

[4.0.9] **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

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

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

First, by Eisenstein's criterion, x^5-2 is irreducible over $\mathbb{Q}$, so the fifth root of 2 generates a quintic extension of $\mathbb{Q}$. 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 $\mathbb{Q}$, the fifth root of 4 generates a quintic extension, and its minimal polynomial over $\mathbb{Q}$ 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 $\mathbb{Q}[x]$. (*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 $\mathbb{Q}(\zeta)$. For example, we do not know anything about the behavior of the ring $\mathbb{Z}[\zeta]$, 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 $\mathbb{Q}(\zeta)$ uses the irreducibility over $\mathbb{Q}$.

Instead, observe that the field extension obtained by adjoining ζ is quartic over $\mathbb{Q}$, while that obtained by adjoining a fifth root β 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, β has *quintic* minimal polynomial over $\mathbb{Q}(\zeta)$, since $[K : \mathbb{Q}(\zeta)] = 5$ (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 $\mathbb{Q}[x]$ is to prove that it is irreducible modulo some prime p. To have some elements of $\mathbb{Z}/p$ not be 5^{th} powers we need $p = 1 \bmod 5$ (by the cyclicness of $(\mathbb{Z}/p)^\times$), and the smallest candidate is $p = 11$. First, 4 is not a fifth power in $\mathbb{Z}/11$, since the only fifth powers are ± 1 (again using the cyclicness 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 $(\mathbb{Z}/11)^\times$. Then if $4 = \alpha^5$ for some $\alpha \in \mathbb{F}_{11^2}$, 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 $\mathbb{Q}[x]$, so is irreducible in $\mathbb{Q}[x]$. (*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^{th} power in $\mathbb{Q}(\zeta)$, and prove irreducibility of $x^5 - a$. That a is not a 5^{th} power in $\mathbb{Q}(\zeta)$ can be proven without understanding much about the ring $\mathbb{Z}[\zeta]$ (if we are slightly lucky) by taking *norms* from $\mathbb{Q}(\zeta)$ to $\mathbb{Q}$, in the sense of writing

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

In fact, we know that $\mathrm{Aut}(\mathbb{Q}(\zeta)/\mathbb{Q}) \approx (\mathbb{Z}/5)^\times$, generated (for example) by $\sigma_2(\zeta) = \zeta^2$. We compute directly that N takes values in $\mathbb{Q}$: 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 $\mathbb{Q}$, as claimed. And since τ 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 $\mathbb{Q}$ (by unique factorization). So, without knowing much about the ring $\mathbb{Z}[\zeta]$, we do know that 4 does not become a fifth power there.

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

[4.0.10] **Remark:** This last problem is a precursor to *Kummer theory*. As with cyclotomic extensions of fields, extensions by n^{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.

Exercises

20.[4.0.1] Prove that a prime p such that $p = 3 \bmod 7$ generates a prime ideal in $\mathbb{Z}[\zeta]$ where ζ is a primitive 7^{th} root of unity.

20.[4.0.2] Let $P(y)$ be an irreducible polynomial in $k[x]$. Let n be an integer not divisible by the characteristic of the field k. Show that $x^n - P(y)$ is irreducible in $k[x, y]$.

20.[4.0.3] Let x be an indeterminate over a field k. Show that there is a field automorphism of $k(x)$ sending x to $c \cdot x$ for any non-zero element c of k.

20.[4.0.4] Let x be an indeterminate over a field k of characteristic p, a prime. Show that there are only finitely-many fields between $k(x)$ and $k(x^{1/p})$.

20.[4.0.5] Let k be an algebraically closed field of characteristic 0. Find a polynomial condition on $a \in k$ such that $z^5 - z + a = 0$ has distinct roots.