

(February 20, 2005)

Solutions 12

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

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

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

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

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 $\mathbf{Z}[\omega]$ is not prime. Since we have seen that $\mathbf{Z}[\omega]$ is Euclidean, hence a PID, the element p must factor properly. ///

[12.2] Prove that a prime p such that $p \equiv 2 \pmod{5}$ generates a prime ideal in the ring $\mathbf{Z}[\zeta]$, where ζ is a primitive fifth root of unity.

The hypothesis on p implies that $\mathbf{F}_{p^n}^\times$ 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 \mathbf{F}_p^\times would contain a primitive fifth root of unity, so have order divisible by 5. If it had a quadratic factor then $\mathbf{F}_{p^2}^\times$ would contain a primitive fifth root of unity, so have order divisible by 5. Recall the isomorphisms

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

Since Φ_5 is irreducible mod p , the right-most quotient is an integral domain. As recalled in the previous exercise, 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 $\mathbf{Z}[\zeta]$ is prime. ///

[12.3] 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 \mathbf{Q} .

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

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

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

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

Since $\sqrt{3}$ and 1 are linearly independent over \mathbf{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 \mathbf{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 $\mathbf{Q}(\sqrt{3}, \sqrt{5})$. 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

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

The system of two linear equations

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

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

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

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

$$\text{Aut}(\mathbf{Q}(\zeta_n)/\mathbf{Q}) \approx (\mathbf{Z}/n)^\times$$

by

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

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

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

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

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

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

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

The signs under the radicals can be removed by removing a factor of i , if necessary. Thus, we can choose $a \in (\mathbf{Z}/4pq)^\times$ with $a \equiv 1 \pmod{4}$ 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 $\mathbf{Q}(\zeta_{4pq})$ which properly moves \sqrt{p} but does not move \sqrt{q} . Thus, σ_a is trivial on $\mathbf{Q}(\sqrt{q})$, so this field cannot contain \sqrt{p} . Thus, the degree $[\mathbf{Q}(\sqrt{p}, \sqrt{q}) : \mathbf{Q}] > 2$. But also this degree is at most 4, and is divisible by $[\mathbf{Q}(\sqrt{q}) : \mathbf{Q}] = 2$. Thus, the degree is 4, as desired. ///

[12.4] 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 $\mathbf{Q}[x]$, so the separate field degrees are as expected: $[\mathbf{Q}(\sqrt{3}) : \mathbf{Q}] = 2$, and $[\mathbf{Q}(\sqrt[3]{5}) : \mathbf{Q}] = 3$. This case is somewhat simpler than the case of two square roots, since the degree $[\mathbf{Q}(\sqrt{3}, \sqrt[3]{5}) : \mathbf{Q}]$ of any compositum is divisible by both $2 = [\mathbf{Q}(\sqrt{3}) : \mathbf{Q}]$ and $3 = [\mathbf{Q}(\sqrt[3]{5}) : \mathbf{Q}] = 3$, 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 \mathbf{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 \mathbf{Q} , the polynomial

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

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

[12.5] 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 \mathbf{Q} , so $\sqrt[3]{10}$ generates a cubic extension of \mathbf{Q} , and thus $1, \sqrt[3]{10},$ and $\sqrt[3]{10}^2$ are linearly independent over \mathbf{Q} . Thus, α is not in \mathbf{Q} . Since it lies inside a cubic field extension of \mathbf{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

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

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

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

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

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

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

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

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*. ///

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 $D \equiv 1 \pmod{4}$.

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 satisfied 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. ///

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

[12.6] Let p be a prime number, and $a \in \mathbf{F}_p^\times$. Prove that $x^p - x + a$ is irreducible in $\mathbf{F}_p[x]$. (*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 Frobenius $b \rightarrow b^p$, but the hint as given reveals an interesting fact in its own right, and which takes one 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 \mathbf{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 \mathbf{F}_p only if *all* these factors are included. That is, $x^p - x + a$ is irreducible in $\mathbf{F}_p[x]$. ///

[12.7] Let $k = \mathbf{F}_p(t)$ be the field of rational expressions in an indeterminate t with coefficients in \mathbf{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 $\mathbf{F}_p[t][X]$, since t is a prime element in the UFD $\mathbf{F}_p[t]$, so (via Gauss' lemma) $X^p - t$ is irreducible in $\mathbf{F}_p(t)[X]$. 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 $\mathbf{F}_p(t)$, the polynomial $X^p - t$ is a linear polynomial raised to the p^{th} power.

[12.8] Let x be an indeterminate over \mathbf{C} . For a, b, c, d in \mathbf{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 $\mathbf{C}(x)$ over \mathbf{C} .

The argument uses no properties of the complex numbers, so we discuss an arbitrary field k instead of \mathbf{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 $k[x] \rightarrow A$ such that $x \rightarrow a$. 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 $k[x] \rightarrow k(x)$, by

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

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 $k[x] \rightarrow k(x)$ is non-zero. That is, we must verify for a positive-degree polynomial (assume without loss of generality that $a_n \neq 0$)

$$P(x) = a_n x^n + \dots + a_0$$

that

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

Again,

$$\begin{aligned} \sigma(P(x)) &= P(\sigma(x)) = P\left(\frac{g(x)}{h(x)}\right) = a_n \left(\frac{g}{h}\right)^n + \dots + a_0 \\ &= h^{-n} \cdot (a_n g^n + a_{n-1} g^{n-1} h + \dots + a_1 g h^{n-1} + a_0 h^n) \end{aligned}$$

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

$$0 = a_n g^n + a_{n-1} g^{n-1} h + \dots + a_1 g h^{n-1} + a_0 h^n$$

would imply that $p|h$, contradiction. But if $\deg h > 0$ we reach a nearly identical contradiction. That is, a field map $k(x) \rightarrow k(x)$ 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

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

is such an inverse:

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

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

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 $k(x)$.

[12.9] In the situation of the previous exercise, show that *every* automorphism of $\mathbf{C}(x)$ over \mathbf{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 $k(x) \rightarrow k(x)$. If it were surjective, then there would be coefficients a_i and b_j in k such that x is expressible as

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

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

$$x \cdot q^{-n}(b_n p^n + b_{n-1} p^{n-1} q + \dots + b_0 q^n) = q^{-m}(a_m p^m + a_{m-1} p^{m-1} q + \dots + a_0 q^m)$$

or

$$x \cdot q^m(b_n p^n + b_{n-1} p^{n-1} q + \dots + b_0 q^n) = q^n(a_m p^m + a_{m-1} p^{m-1} q + \dots + a_0 q^m)$$

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

$$(b_0 x - a_0) \cdot q^{m+n}$$

is visibly a multiple of p . Since p and q are relatively prime and $k[x]$ is a UFD, necessarily p divides $b_0 x - a_0$. 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

$$x \cdot q^{m-n}(b_n p^n + b_{n-1} p^{n-1} q + \dots + b_0 q^n) = a_m p^m + a_{m-1} p^{m-1} q + \dots + a_0 q^m$$

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

$$x \cdot (b_n p^n + b_{n-1} p^{n-1} q + \dots + b_0 q^n) = q^{n-m}(a_m p^m + a_{m-1} p^{m-1} q + \dots + a_0 q^m)$$

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

$$x \cdot (b_n p^n + b_{n-1} p^{n-1} q + \dots + b_0 q^n) = a_m p^m + a_{m-1} p^{m-1} q + \dots + a_0 q^m$$

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

$$x \cdot b_n p^n - a_m p^m = (x b_n - a_n) \cdot p^n$$

The coprimality of p, q implies that q divides $x b_n - a_n$, so $\deg q \leq 1$ 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.

///

[12.10] Let s and t be indeterminates over \mathbf{F}_p , and let $\mathbf{F}_p(s^{1/p}, t^{1/p})$ be the field extension of the rational function field $\mathbf{F}_p(s, t)$ 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 $\mathbf{F}_p(s, t)$ and $\mathbf{F}_p(s^{1/p}, t^{1/p})$.

First, 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 $k(s, t)$. First, we show that $[k(s^{1/p}, t^{1/p}) : k(s, t)] = p^2$. First, by Eisenstein's criterion in $\mathbf{F}_p(t)[s][X]$ the polynomial $X^p - s$ is irreducible, since the prime s in $\mathbf{F}_p(t)[s]$, 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 $\mathbf{F}_p(t)[s][X]$ the polynomial

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

is irreducible, since the prime s in $\mathbf{F}_p(t)[s]$, 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 $\mathbf{F}_p(s, t)$.

We claim that for distinct positive integers m, n

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

To prove this, we will show that any subfield of $\mathbf{F}_p(s^{1/p}, t^{1/p})$ which contains both $(s + s^{mp}t)^{1/p}$ and $(s + s^{np}t)^{1/p}$ is the whole field $\mathbf{F}_p(s^{1/p}, t^{1/p})$, 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 $\mathbf{F}_p(s, t)$, so the two degree p extensions cannot be identical (or the whole degree would be just p). ///

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.