Math 410, Spring 2026 Professor Rob Benedetto

Solutions to Homework 4

Problem 1. Cox, Section 4.1, Exercise 1:
Let $\alpha \in L \setminus \{0\}$ be algebraic over a subfield F. Prove that $1/\alpha$ is also algebraic over F.

Proof. By hypothesis, there is a nonconstant polynomial $f \in F[x]$ such that $f(\alpha) = 0$. Write $f(x) = a_n x^n + \cdots + a_0$. Let $j \geq 0$ be the smallest integer such that $a_j \neq 0$; after dividing f by x^j, we may assume that $a_0 \neq 0$. (Note that this dividing does not change the fact that $f(\alpha) = 0$, since x is nonzero at α, because we assumed $\alpha \neq 0$.)
Define $g(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n \in F[x]$, which is nonconstant. Then

$$g(1/\alpha) = a_0\alpha^{-n} + a_1\alpha^{-(n-1)} + \cdots + a_n = \alpha^{-n}\big(a_0 + a_1\alpha + \cdots + a_n\alpha^n\big) = \alpha^{-n} f(\alpha) = 0.$$

Thus, $1/\alpha$ is algebraic over F. QED

Problem 2. Cox, Section 4.1, Exercise 8:
If $f(x) \in F[x]$ is irreducible, it may or may not be irreducible over a particular extension field L/F, as you will show in this problem.

(a) Prove that $f(x) = x^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt{2})$.

(b) In Example 4.1.7, it was shown that $g(x) = x^4 - 10x^2 + 1$ is irreducible over $\mathbb{Q}$
(and it is the minimal polynomial of $\alpha = \sqrt{2} + \sqrt{3}$).
Prove that g is *reducible* over $\mathbb{Q}(\sqrt{3})$, by finding an explicit factorization.

Proof. (a): If $f(x) = x^2 - 3$ is reducible over $\mathbb{Q}(\sqrt{2})$, then since $\deg(f) = 2$, a Math 350 theorem says that f has a root in $\mathbb{Q}(\sqrt{2})$. In that case, let $\alpha \in \mathbb{Q}(\sqrt{2})$ be such a root, and write $\alpha = a + b\sqrt{2}$, with $a, b \in \mathbb{Q}$. Then

$$0 = f(\alpha) = (a + b\sqrt{2})^2 - 3 = a^2 + 2b^2 - 3 + 2ab\sqrt{2}.$$

Thus, $a^2 + 2b^2 - 3 = 0$ and $2ab = 0$. The second equation gives either $a = 0$ or $b = 0$. If $b = 0$, then the first equation gives $a^2 = 3$, which is impossible, since there is no $\sqrt{3}$ in $\mathbb{Q}$. If $a = 0$, then the first equation gives $2b^2 = 3$, i.e. $(2b)^2 = 6$, which is impossible, since there is no $\sqrt{6}$ in $\mathbb{Q}$. Hence, the existence of a root $\alpha \in \mathbb{Q}(\sqrt{2})$ leads to a contradiction, so there is no such root. Thus, f is irreducible over $\mathbb{Q}(\sqrt{2})$. QED

— — — — — — —

(b): Knowing (from Example 4.1.2) that the four roots of g are $\pm\sqrt{2} \pm \sqrt{3}$, define

$$h_1(x) = \big(x - \sqrt{2} - \sqrt{3}\big)\big(x + \sqrt{2} - \sqrt{3}\big) = x^2 - 2\sqrt{3}x + 1 \in \mathbb{Q}(\sqrt{3})$$

and

$$h_2(x) = \big(x - \sqrt{2} + \sqrt{3}\big)\big(x + \sqrt{2} + \sqrt{3}\big) = x^2 + 2\sqrt{3}x + 1 \in \mathbb{Q}(\sqrt{3})$$

We check that $h_1 h_2 = x^4 + (1 - 12 + 1)x^2 + 1 = g(x)$, so g factors nontrivially over $\mathbb{Q}(\sqrt{3})$. QED

Problem 3. Cox, Section 4.2, Exercise 5, variant:
Find the cyclotomic polynomial Φ_{24}, i.e., the minimal polynomial of ζ_{24} over $\mathbb{Q}$, as follows.

(a) Factor $x^{24} - 1$ over $\mathbb{Q}$.

(b) Remembering that the factors of $x^{24} - 1$ must be Φ_n for each $n \geq 1$ with $n|24$,
identify which factor is Φ_{24}.

[**Note**: You may assume without proof that each Φ_n is irreducible over $\mathbb{Q}$, and that $\deg(\Phi_n) = \phi(n)$, where $\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$. FYI: ϕ is known as the Euler totient function, or the Euler-ϕ function.]

Solution/Proof, of both parts together.

Using the identities $a^2 - b^2 = (a-b)(a+b)$ and $a^3 - b^3 = (a-b)(a^2+ab+b^2)$, and noting that the second one also yields $a^3 + b^3 = (a+b)(a^2 - ab + b^2)$, we have

$$\begin{aligned} x^{24} - 1 &= (x^{12}-1)(x^{12}+1) = (x^6-1)(x^6+1)(x^4+1)(x^8-x^4+1) \\ &= (x^3-1)(x^3+1)(x^2+1)(x^4-x^2+1)(x^4+1)(x^8-x^4+1) \\ &= (x-1)(x+1)(x^2+1)(x^2+x+1)(x^2-x+1)(x^4+1)(x^4-x^2+1)(x^8-x^4+1). \end{aligned}$$

Those factors are, in order, Φ_1, Φ_2, Φ_4, Φ_3, Φ_6, and three more.
The third-to-last, x^4+1, has as its roots the square roots of the roots of x^2+1, i.e., the square roots of the primitive fourth roots of unity. So its roots are the four primitive eighth roots of unity; i.e., $x^4 + 1 = \Phi_8$.
The second-to-last, $x^4 - x^2 + 1$, has as roots the square roots of the roots of $x^2 - x + 1$, i.e., the square roots of the primitive sixth roots of unity. So its roots are the four primitive twelfth roots of unity; i.e., $x^4 - x^2 + 1 = \Phi_{12}$.
Finally, the last, $x^8 - x^4 + 1$, has as roots the square roots of the roots of $x^4 - x^2 + 1 = \Phi_{12}$; i.e., the square roots of the primitive twelfth roots of unity. So its roots are the eight primitive 24-th roots of unity; i.e., $\boxed{\Phi_{24} = x^8 - x^4 + 1}$

Problem 4. Cox, Section 4.2, Exercise 7:
For each of the following polynomials, determine (and prove) whether or not it is irreducible over the given field, without using a computer.

(a) (4 points) $x^3 + x + 1$ over $\mathbb{F}_5$.

(b) (8 points) $x^4 + x + 1$ over $\mathbb{F}_2$.

Solution/Proof. (a): Writing $f(x) = x^3 + x + 1 \in \mathbb{R}_5[x]$, we use the fact that a cubic polynomial (over a field) is reducible if and only if it has a root in the field. Testing all elements of $\mathbb{F}_5 = \{0,1,2,3,4\} = \{0,1,2,-2,-1\}$ gives:

$$f(0) = 1, \quad f(1) = 3, \quad f(2) = 3+2+1 = 1, \quad f(-2) = -3-2+1 = 1, \quad f(-1) = -1-1+1 = -1,$$

none of which is 0 in $\mathbb{F}_5$. So f is $\boxed{\text{irreducible over } \mathbb{F}_5}$

(b): Writing $g(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$, we first observe that $g(0) = 1 \neq 0$ and $g(1) = 1+1+1 = 1 \neq 0$ in $\mathbb{F}_2$. That is, g has no roots in $\mathbb{F}_2 = \{0,1\}$, and hence it does not have a degree 1 factor. The only other way g could factor would be as a product of two degree 2 polynomials.
Suppose $g = hk$ for $h, k \in \mathbb{F}_2[x]$ both of degree 2. Since g has no roots in $\mathbb{F}_2$, neither can h or k. Any polynomial $p \in \mathbb{F}_2[x]$ of degree 2 must be of the form $p(x) = ax^2 + bx + c$ with $a, b, c \in \mathbb{F}_2$ and $a \neq 0$. That is, $a = 1$. In addition, since 0 is not a root, we have $c \neq 0$, and hence $c = 1$. But then $0 \neq p(1) = 1 + b + 1 = b$, so that $b = 1$ as well. That is, we must have $h = k = x^2 + x + 1$, since both h and k are quadratic with no roots in $\mathbb{F}_2$.
However, we compute $hk = (x^2+x+1)^2 = x^4 + x^2 + 1 \neq g$. So g is $\boxed{\text{irreducible over } \mathbb{F}_2}$

Problem 5. Cox, Section 4.2, Exercise 8:
Let $a \in \mathbb{Z}$ be a product of (a positive number of) distinct primes, and let $n \geq 1$.
Prove that $x^n - a$ is irreducible over $\mathbb{Q}$.

Proof. Let p be one of the primes dividing a. Then $p^2 \nmid a$ (since a is a product of *distinct* primes), and hence $f(x) = x^n - a$ satisfies Eisenstein's criterion at p. Therefore, by Eisenstein's criterion, f is irreducible over $\mathbb{Q}$. QED

Problem 6. Cox, Section 4.3, Exercise 2:
Compute the degrees of the following field extensions.

(a) $\mathbb{Q}(i, \sqrt[4]{2}) \,/\, \mathbb{Q}$

(b) $\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) \,/\, \mathbb{Q}$

(c) $\mathbb{Q}(\sqrt{2+\sqrt{2}}) \,/\, \mathbb{Q}$

(d) $\mathbb{Q}(i, \sqrt{2+\sqrt{2}}) \,/\, \mathbb{Q}$

SolutionsProofs. (a): We have $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ since $\sqrt[4]{2}$ is a root of $x^4 - 2 \in \mathbb{Q}[x]$, which is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion with $p = 2$.
Since $\mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$, the quadratic polynomial $x^2 + 1$ has no roots in $\mathbb{Q}(\sqrt[4]{2})$ and hence is irreducible over $\mathbb{Q}(\sqrt[4]{2})$. Therefore, $[\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}(\sqrt[4]{2})] = 2$. Thus, by the Tower Theorem,

$$[\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}] = [\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 2 \cdot 4 = 8.$$

(b): We have $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$ since $x^2 - 3$ is irreducible over $\mathbb{Q}$, and $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ since $x^3 - 2$ is irreducible over $\mathbb{Q}$, both by Eisenstein's Criterion (with $p = 3$ and $p = 2$, respectively; or for a whole bunch of other possible reasons).
Suppose, towards contradiction, that $\sqrt{3} \in \mathbb{Q}(\sqrt[3]{2})$. Then $\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2})$, whence

$$3 = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2[\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt{3})],$$

which would mean that 3 is divisible by 2. By this contradiction, we have $\sqrt{3} \notin \mathbb{Q}(\sqrt[3]{2})$, and hence $x^2 - 3$, being a quadratic polynomial, is irreducible over $\mathbb{Q}(\sqrt[3]{2})$. Thus, $[\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})] = 2$, and hence by the Tower Theorem,

$$[\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2 \cdot 3 = 6.$$

(c): Let $\alpha = \sqrt{2+\sqrt{2}}$. Then $\alpha^2 = 2 + \sqrt{2}$, so $\alpha^2 - 2 = \sqrt{2}$. Therefore, $(\alpha^2 - 2)^2 = 2$; expanding, this means α is a root of $f(x) = x^4 - 4x^2 + 2$. Note that f is irreducible over $\mathbb{Q}$ by Eisenstein's criterion with $p = 2$. Thus, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.

(d): Still writing $\alpha = \sqrt{2+\sqrt{2}}$, we have $\alpha \in \mathbb{R}$, so $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$. As in part (a), then, $x^2 + 1$ is irreducible over $\mathbb{Q}(\alpha)$, so that $[\mathbb{Q}(i, \alpha) : \mathbb{Q}(\alpha)] = 2$. Thus,

$$\left[\mathbb{Q}\left(i, \sqrt{2+\sqrt{2}}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(i, \sqrt{2+\sqrt{2}}\right) : \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)\right]\left[\mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right) : \mathbb{Q}\right] = 2 \cdot 4 = 8.$$

Problem 7. Cox, Section 4.3, Exercise 4:
Let L/F be a finite extension with $[L : F]$ prime.

(a) Prove that the only intermediate fields K (i.e., fields K with $L/K/F$) are F and L.

(b) For any $\alpha \in L \setminus F$, prove that $L = F(\alpha)$.

Proof. Let $p = [L : F]$, so p is prime.

(a): Let K be such an intermediate field. Then by the Tower Theorem,

$$[L : K][K : F] = [L : F] = p.$$

Since $[L : K]$ and $[K : F]$ are positive integers, we have either $[L : K] = 1$ or $[K : F] = 1$.
If $[L : K] = 1$, then $K = L$. Otherwise, $[K : F] = 1$, in which case $K = F$. QED

(b): Given $\alpha \in L \setminus F$, let $K = F(\alpha)$. Then $L/K/F$. In addition, since $\alpha \in K$ but $\alpha \notin F$, we have $K \neq F$. Therefore, by part (a), we have $K = L$, i.e., $L = F(\alpha)$. QED

Problem 8. Cox, Section 4.3, Exercise 5:
Let $L = \mathbb{Q}(\sqrt[4]{2}, \sqrt[3]{3})$. In this problem, you will compute $[L : \mathbb{Q}]$.

(a) Prove that both $x^4 - 2$ and $x^3 - 3$ are irreducible over $\mathbb{Q}$.

(b) Let $K_1 = \mathbb{Q}(\sqrt[4]{2})$, so that $L/K_1/\mathbb{Q}$. Use K_1 to prove that $4|[L:\mathbb{Q}]$ and that $[L:\mathbb{Q}] \leq 12$.

(c) Let $K_2 = \mathbb{Q}(\sqrt[3]{3})$, so that $L/K_2/\mathbb{Q}$. Use K_2 to prove that $3|[L:\mathbb{Q}]$.

(d) Use parts (b) and (c) to prove that $[L:\mathbb{Q}] = 12$.

Proof. (a): Let $f(x) = x^4 - 2$ and $g(x) = x^3 - 3$.
Then f satisfies Eisenstein's Criterion for $p = 2$, and g satisfies Eisenstein's Criterion for $p = 3$. Hence, both are irreducible over $\mathbb{Q}$. QED

(b): Let $m = [L : K_1]$. Since $L = K_1(\sqrt[3]{3})$, we have $m = \deg h$, where $h \in K_1[x]$ is the minimal polynomial of $\sqrt[3]{3}$ over K_1.
Since $g \in \mathbb{Q}[x] \subseteq K_1[x]$ and $g(\sqrt[3]{3}) = 0$, we have $h|g$, and hence $m = \deg(h) \leq \deg(g) = 3$.
We also have $[K_1 : \mathbb{Q}] = \deg(f) = 4$, since $f \in \mathbb{Q}[x]$ is a monic irreducible polynomial with $f(\sqrt[4]{2}) = 0$, and hence f is the minimal polynomial of $\sqrt[4]{2}$ over $\mathbb{Q}$.
Therefore, by the Tower Theorem, $[L:\mathbb{Q}] = [L:K_1][K_1:\mathbb{Q}] = 4m$. Since m is an integer, then, we have $4|[L:\mathbb{Q}]$; and since $m \leq 3$, we have $[L:\mathbb{Q}] = 4m \leq 12$. QED

(c): We have $[K_2 : \mathbb{Q}] = \deg(g) = 3$, since $g \in \mathbb{Q}[x]$ is a monic irreducible polynomial with $g(\sqrt[3]{3}) = 0$, and hence g is the minimal polynomial of $\sqrt[3]{3}$ over $\mathbb{Q}$.
Let $n = [L : K_2]$. Then by the Tower Theorem, $[L:\mathbb{Q}] = [L:K_2][K_2:\mathbb{Q}] = 3n$.
[In particular, $3n = [L:\mathbb{Q}] \leq 12$, so n is finite and hence an integer.]
Since n is an integer, then, we have $3|[L:\mathbb{Q}]$. QED

(d): By parts (b) and (c), we have that $[L:\mathbb{Q}]$ is a positive integer N with $1 \leq N \leq 12$, and which is divisible by both 3 and 4. But since $\gcd(3,4) = 1$, the latter condition implies that $12|N$. Since $1 \leq N \leq 12$, we have $N = 12$. QED