Math 404 HW 4 Solutions

1 Problem 1

> Use Lagrange's method to solve the quartic
>
> $$f(x) = x^4 + x + 3/4$$

Let $\alpha_1, \ldots, \alpha_4$ be the roots of f. Let $s_1, \ldots, s_4$ denote the elementary symmetric functions in the α_i. Then we have

$$\begin{aligned} s_1 &= 0 \\ s_2 &= 0 \\ s_3 &= -1 \\ s_4 &= 3/4. \end{aligned}$$

Define

$$\begin{aligned} f_1 &= (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) \\ f_2 &= (\alpha_1 + \alpha_3)(\alpha_3 + \alpha_4) \\ f_3 &= (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3) \end{aligned}$$

Then as in homework 2, we have

$$\begin{aligned}
\alpha_1 &= \frac{\sqrt{-f_1} + \sqrt{-f_2} + \sqrt{-f_3}}{2} \\
\alpha_2 &= \frac{\sqrt{-f_1} - \sqrt{-f_2} - \sqrt{-f_3}}{2} \\
\alpha_3 &= \frac{-\sqrt{-f_1} + \sqrt{-f_2} - \sqrt{-f_3}}{2} \\
\alpha_4 &= \frac{-\sqrt{-f_1} - \sqrt{-f_2} + \sqrt{-f_3}}{2}
\end{aligned}$$

So now we just have to find the f_i.

From homework 2, we have the equalities

$$\begin{aligned}
f_1 + f_2 + f_3 &= 2s_2 = 0 \\
f_1f_2 + f_1f_3 + f_2f_3 &= s_2^2 + s_1s_3 - 4s_4 = -3 \\
f_1f_2f_3 &= s_1s_2s_3 - s_3^2 - s_1^2s_4 = -1.
\end{aligned}$$

Let $g(y)$ be the resolvent cubic of f, which using the equalities above is

$$\begin{aligned}
g(y) &= (y - f_1)(y - f_2)(y - f_3) \\
&= y^3 - (f_1 + f_2 + f_3)y^2 + (f_1f_2 + f_1f_3 + f_2f_3)y - f_1f_2f_3 \\
&= y^3 - 3y + 1.
\end{aligned}$$

To solve this cubic, we make the substitution

$$y = z - \frac{-3}{3z} = z + \frac{1}{z}.$$

After applying this substitution and simplifying, we get the equation

$$z^6 + z^3 + 1 = 0.$$

Applying the quadratic formula yields the solution

$$z^3 = \frac{-1}{2} \pm i\frac{\sqrt{3}}{2} \approx -0.5 \pm 0.8660i.$$

One solution is

$$z_0 = \sqrt[3]{\frac{-1}{2} + i\frac{\sqrt{3}}{2}} \approx 0.7660 + 0.6428i.$$

The other solutions are ωz and $\omega^2 z$, with $\omega = e^{2\pi i/3}$, the primitive cube root of unity. These yield the solutions

$$\begin{aligned}
z_0 &\approx 0.7660 + 0.6428i \\
\omega z_0 &\approx -0.9397 + 0.6428i \\
\omega^2 z_0 &\approx 0.1736 - 0.9848i.
\end{aligned}$$

Applying the substitution $y = z + 1/z$ yields the equations

$$\begin{aligned}
f_1 &\approx 1.5321 \\
f_2 &\approx -1.8794 \\
f_3 &\approx 0.3473
\end{aligned}$$

In turn, these yield the solutions for the α_i as

$$\begin{aligned}
\alpha_1 &\approx 0.6855 + 0.9135i \\
\alpha_2 &\approx -0.6855 + 0.3242i \\
\alpha_3 &\approx 0.6855 - 0.9135i \\
\alpha_4 &\approx -0.6855 - 0.3242i,
\end{aligned}$$

which can be checked by plugging back into the original polynomial f. Alternately, we could have expressed everything in radicals.

$\square$

2 Problem 2

First we make a general observation about roots over $\mathbb{F}_2$. A polynomial $f(x) \in \mathbb{F}_2[x]$ has $f(0) = 0$ if and only if it has zero constant term, and it has $f(1) = 0$ if and only if it has an even number of nonzero terms. The method we use below is called the Sieve of Eratosthenes, if you want to look into it further.

(a) There are 2. A polynomial of degree 3 is irreducible if and only if it has no roots. Using the root-finding criterion given above, we have just the two polynomials $x^3 + x + 1$ and $x^3 + x^2 + 1$.

(b) There are 3. A polynomial of degree 4 is irreducible if and only if it has no roots and no irreducible quadratic factor. The only irreducible quadratic in $\mathbb{F}_2[x]$ is $f = x^2 + x + 1$. So the only polynomial with f as a factor and no roots is $f^2 = x^4 + x^2 + 1$. So every polynomial of degree 4 with no roots besides this one is irreducible. Thus, we have the full list

$$x^4 + x + 1, x^4 + x^3 + 1, x^4 + x^3 + x^2 + x + 1$$

(c) Define

$$K = \frac{\mathbb{F}_2[x]}{(x^3 + x + 1)}$$
$$L = \frac{\mathbb{F}_2[y]}{(y^3 + y^2 + 1)}.$$

Since K and L are both fields, any ring homomorphism $L \to K$ will be injective. Furthermore, any ring homomorphism commutes with the action of $\mathbb{F}_2$ (multiplying by 1 does nothing, and 0 goes to 0), so any ring homomorphism will also be an inclusion of $\mathbb{F}_2$-vector spaces. Since both K and L have the same dimension as vector spaces over $\mathbb{F}_2$, this inclusion must be an isomorphism.

Thus, all we need to do is provide *some* ring homomorphism $\varphi : L \to K$. To do this, it suffices to find some element $\alpha \in K$ so that $\alpha^3 + \alpha^2 + 1 = 0$. We may uniquely write

$$\alpha = A + Bx + Cx^2,$$

with $A, B, C \in \mathbb{F}_2$. Recall that we have the following identities:

- $x^3 = x + 1$
- $A^2 = A$, $B^2 = B$, $C^2 = C$
- $2 = 0$.

Using these, we compute

$$\alpha^3 + \alpha^2 + 1 = (1 + BC + B + C) + x(AB + B + AC) + x^2(AB + B).$$

For this element to be zero, we must solve the equations

$$\begin{aligned} 1 + BC + B + C &= 0 \\ AB + B + AC &= 0 \\ AB + B &= 0 \end{aligned}$$

with $A, B, C \in \mathbb{F}_2$. One possible solution is $A = B = 1$ and $C = 0$. Since a solution exists, the desired α exists, and the result holds.

$\square$

3 Problem 4.3

Find all intermediate field extensions of $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$

I claim that the only intermediate field extensions are $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{6})$

Consider some intermediate field $\mathbb{Q} \subset K \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$. In the last homework I proved that $\mathbb{Q}(\sqrt{3}, \sqrt{2})$ was a degree 4 extension of $\mathbb{Q}$ with basis $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$. Thus, by the multiplicative property of the degree, we have that $[K : \mathbb{Q}]$ divides 4. Thus, it is either 1, 2, or 4. If $[K : \mathbb{Q}]$ is 1 or 4, then we have $K = \mathbb{Q}$ or $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, respectively. So for the rest of this problem we may assume that $[K : \mathbb{Q}] = 2$.

First, we show that K is a simple extension of $\mathbb{Q}$ with a particularly nice form.

Lemma 1. *Let $\mathbb{Q} \subset K$ be any degree 2 field extension. Then $K = \mathbb{Q}(\alpha)$, for some $\alpha \notin \mathbb{Q}$ with $\alpha^2 \in \mathbb{Q}$.*

Proof. Problem 6 on this homework yields that $K = \mathbb{Q}(\beta)$ for some β (just take any $\beta \in K \setminus \mathbb{Q}$). Then there is an irreducible monic polynomial $f(x) = x^2 + bx + c \in \mathbb{Q}[x]$ with $f(\beta) = 0$. The rest will follow from completing the square on f. Define

$$\alpha = \beta + b/2.$$

Then $\alpha \in \mathbb{Q}(\beta)$. Since $\mathbb{Q}(\beta)$ is a field containing α and $\mathbb{Q}$, we have by minimality of $\mathbb{Q}(\alpha)$ that $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\beta)$. We get the reverse containment $\mathbb{Q}(\beta) \subset \mathbb{Q}(\alpha)$ similarly, so we have that $K = \mathbb{Q}(\beta) = \mathbb{Q}(\alpha)$. Since K is a field strictly containing $\mathbb{Q}$, we must have that $\alpha \notin \mathbb{Q}$, so all that remains to be shown is that $\alpha^2 \in \mathbb{Q}$.

To see this, note that by construction, α is a root of

$$f(x - b/2) = x^2 + c - b^2/4 =: g(x).$$

Further, this shows that

$$\alpha^2 = b^2/4 - c \in \mathbb{Q},$$

as desired. $\square$

Resuming the original problem, we now know that we have some intermediate field extension $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$, with $\alpha^2 \in \mathbb{Q}$ but $\alpha \notin \mathbb{Q}$. We wish to show $\mathbb{Q}(\alpha) \in \{\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{6})\}$.

Since $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ forms a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, we may uniquely write

$$\alpha = A + B\sqrt{2} + C\sqrt{3} + D\sqrt{6},$$

with $A, B, C, D \in \mathbb{Q}$. Our goal is to show that at most one of B, C, or D are nonzero. To see why this suffices, note that if $C = D = 0$, then $\alpha = A + B\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, so we get $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\sqrt{2})$, and since these fields have the same degree over $\mathbb{Q}$, they must be equal. The other claimed intermediate fields show up for the other nonzero coefficients.

We compute

$$\alpha^2 = (A^2 + 2B^2 + 3C^2 + 6D^2) + \sqrt{2}(2AB + 6CD) + \sqrt{3}(2AC + 4BD) + \sqrt{6}(2AD + 2BC)$$

By assumption, we have that $\alpha^2 \in \mathbb{Q}$, so this sum also equals $\alpha^2 \cdot 1 + 0\sqrt{2} + 0\sqrt{3} + 0\sqrt{6}$. Linear independence of $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ over $\mathbb{Q}$ yields that we have three equations

$$2AB + 6CD = 0 \tag{1}$$

$$2AC + 4BD = 0 \tag{2}$$

$$2AD + 2BC = 0 \tag{3}$$

Suppose $D \neq 0$, we wish to show that $B = C = 0$. Dividing these equations by D yields the equations

$$C = \frac{-AB}{3D} \tag{4}$$

$$B = \frac{-AC}{2D} \tag{5}$$

$$A = \frac{-BC}{D}. \tag{6}$$

Plugging the first of these equations into the second yields

$$B = \frac{A^2 B}{6D^2}.$$

If $B \neq 0$, then this yields $6 = \left(\frac{A}{D}\right)^2$, so $\sqrt{6} \in \mathbb{Q}$, which we've shown is not true before. Thus, we must have that $B = 0$. Then equation (**??**) yields that $C = 0$ as well, as desired. Similar reasoning holds if we start by assuming $B \neq 0$ or $C \neq 0$, and so the result holds.

$\square$

4 Problem 4.4

(a) Note that $1 + \sqrt[3]{2} + \sqrt[3]{4} = 1 + \sqrt[3]{2} + (\sqrt[3]{2})^2$, so we have the geometric series formula

$$1 + \sqrt[3]{2} + (\sqrt[3]{2})^2 = \frac{(\sqrt[3]{2})^3 - 1}{\sqrt[3]{2} - 1} = \frac{1}{\sqrt[3]{2} - 1}.$$

Thus, if we let $\alpha = 1+\sqrt[3]{2}+\sqrt[3]{4}$, this shows $\alpha \in \mathbb{Q}(\sqrt[3]{2})$ and $\sqrt[3]{2} \in \mathbb{Q}(\alpha)$. Then by minimality we have $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\sqrt[3]{2})$ and $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\alpha)$, so we have $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[3]{2})$. This field is readily seen to be degree 3 over $\mathbb{Q}$, with basis $1, \sqrt[3]{2}, \sqrt[3]{4}$ (we showed this on the last homework).

$\square$

(b) Let $\zeta = e^{\frac{2\pi i}{p}}$. Then we have $\zeta^p = 1$, so ζ is a root of $x^p - 1$. Compute

$$x^p - 1 = (x - 1)(1 + x + x^2 + \cdots + x^{p-1}).$$

Plugging in ζ yields

$$0 = (\zeta - 1)(1 + \zeta + \zeta^2 + \cdots + \zeta^{p-1}).$$

Since $\zeta \neq 1$, we must have that ζ is a root of $1 + x + x^2 + \cdots + x^{p-1}$, which we showed was irreducible in last week's homework. Thus, this is the minimal polynomial for ζ, and its degree is the degree of $\mathbb{Q}(\zeta)/\mathbb{Q}$, which is $p-1$. Furthermore, we get that $1, \zeta, \zeta^2, \ldots, \zeta^{p-2}$ forms a basis for $\mathbb{Q}(\zeta)/\mathbb{Q}$. $\square$

(c) Let $\alpha = \sqrt{10 + 4\sqrt{6}}$ $\mathbb{Q}(\alpha, \sqrt{6}) = \mathbb{Q}(\sqrt{6})$. Note that

$$\frac{\alpha^2 - 10}{4} = \sqrt{6}$$

so $\sqrt{6} \in \mathbb{Q}(\alpha)$, so adjoining $\sqrt{6}$ to $\mathbb{Q}(\alpha)$ doesn't change anything. Thus, we get at least

$$\mathbb{Q}(\alpha, \sqrt{6}) = \mathbb{Q}(\alpha) \supseteq \mathbb{Q}(\sqrt{6}).$$

For the reverse containment, note that $2+\sqrt{6} \in \mathbb{Q}(\sqrt{6})$ and $(2+\sqrt{6})^2 = 10 + 4\sqrt{6}$, so $\alpha = 2 + \sqrt{6} \in \mathbb{Q}(\sqrt{6})$, so $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\sqrt{6})$.

Thus, the field we're considering is just $\mathbb{Q}(\sqrt{6})$, which we've previously shown is of degree 2 over $\mathbb{Q}$, with basis $1, \sqrt{6}$.

5 Problem 4.5

(a) Let $\alpha = 1 + \sqrt[3]{2} + \sqrt[3]{4}$. By problem 4 (a) we just need to find a monic degree 3 polynomial $f(x)$ with $f(\alpha) = 0$. That is, we seek rational numbers A, B, C so that

$$\alpha^3 = A + B\alpha + C\alpha^2.$$

We expand both sides and collect the coefficients of $\sqrt[3]{2}$ and $\sqrt[3]{4}$ and obtain

$$19 \cdot 1 + 15\sqrt[3]{2} + 12\sqrt[3]{4} = (A + B + 5C) \cdot 1 + (B + 4C)\sqrt[3]{2} + (B + 3C)\sqrt[3]{4}.$$

On the last homework, we showed that $1, \sqrt[3]{2}, \sqrt[3]{4}$ were linearly independent over $\mathbb{Q}$. Thus, we must have

$$\begin{aligned} 19 &= A + B + 5C \\ 15 &= B + 4C \\ 12 &= B + 3C. \end{aligned}$$

This system of equations has solution $A = 1$, $B = 3$, $C = 3$. Thus, we have the minimal polynomial

$$\boxed{f(x) = x^3 - 3x^2 - 3x - 1}$$

□

(b) In the previous problem, we figured out that

$$\sqrt{10 + 4\sqrt{6}} = 2 + \sqrt{6},$$

which is a root of the polynomial

$$(x - 2)^2 - 6 = x^2 - 4x - 2$$

For irreducibility, we can either use Eisenstein's criterion at the prime 2, or just note that

$$\mathbb{Q}(2 + \sqrt{6}) = \mathbb{Q}(\sqrt{6}),$$

which is a degree 2 extension of $\mathbb{Q}$. So any degree 2 polynomial that the generator of this extension is a root of must be a unit multiple of the irreducible minimal polynomial, and so irreducible.

□

(c) Again, since $\sqrt{10+4\sqrt{6}} = 2+\sqrt{6}$, it is a root of the polynomial $x-2-\sqrt{6} \in \mathbb{Q}(\sqrt{6})[x]$, which is irreducible as it is of degree 1.

(d) First we figure out what degree the minimal polynomial should have by figuring out the degree of the corresponding field extension is 4.

To do this, define

$$\begin{aligned} \alpha &= \sqrt{3}+\sqrt{\pi} \\ \beta &= \sqrt{3}-\sqrt{\pi}, \end{aligned}$$

so we are investigating $[\mathbb{Q}(\pi,\alpha) : \mathbb{Q}(\pi)]$. First we get a different set of generators. Note that

$$\alpha\beta = 3-\pi,$$

so

$$\beta = \frac{3-\pi}{\alpha} \in \mathbb{Q}(\alpha,\pi).$$

Then note that

$$\begin{aligned} \frac{\alpha+\beta}{2} &= \sqrt{3} \\ \frac{\alpha-\beta}{2} &= \sqrt{\pi}. \end{aligned}$$

Thus, we have that $\sqrt{3},\sqrt{\pi} \in \mathbb{Q}(\pi,\alpha)$. Since we also have $\pi,\alpha \in \mathbb{Q}(\sqrt{3},\sqrt{\pi})$, we have

$$\mathbb{Q}(\pi,\alpha) = \mathbb{Q}(\sqrt{3},\sqrt{\pi}).$$

We are motivated to consider the following diagram of field extensions

$$\begin{tikzcd} & \mathbb{Q}(\sqrt{\pi},\sqrt{3}) & \\ \mathbb{Q}(\sqrt{\pi}) \arrow[ur] & & \mathbb{Q}(\pi,\sqrt{3}) \arrow[ul] \\ & \mathbb{Q}(\pi) \arrow[ul] \arrow[ur] & \end{tikzcd} \tag{7}$$

Every move vertically in this diagram is obtained by adjoining a square root, which results in a degree 2 field extension so long as the square root doesn't already exist inside the smaller field. We move along the left half of this diagram to show that each intermediate extension is indeed degree 2.

For the extension $\mathbb{Q}(\pi) \subset \mathbb{Q}(\sqrt{\pi})$, recall that π is transcendental over $\mathbb{Q}$, so $\mathbb{Q}(\pi) \cong \mathbb{Q}(t)$, the ring of rational functions over $\mathbb{Q}$ (ratios of polynomials with nonzero denominator). So we suppose towards a contradiction that $\sqrt{\pi} \in \mathbb{Q}(\pi)$. Then there exist polynomials $f(\pi), g(\pi)$ with $g(\pi) \neq 0$ so that

$$\left(\frac{f(\pi)}{g(\pi)}\right)^2 = \pi.$$

Then we have that

$$f(\pi)^2 = \pi \cdot g(\pi)^2.$$

Recall that this means an equality of polynomials, that is all the coefficients of various powers π^i are the same on both sides. The degree on the right hand side is $1 + 2\deg(g)$, which is odd. The degree on the left hand side is $2\deg(f)$, which is even. Since no odd number can equal an even number, we have a contradiction.

For the extension $\mathbb{Q}(\sqrt{\pi}) \subset \mathbb{Q}(\sqrt{\pi}, \sqrt{3})$, we first show that $\sqrt{\pi}$ is transcendental over $\mathbb{Q}$. If not, then we would have that $[\mathbb{Q}(\sqrt{\pi} : \mathbb{Q}]$ is finite. Since $\mathbb{Q}(\pi)$ is a sub $\mathbb{Q}$-vector space of $\mathbb{Q}(\sqrt{\pi})$, this would yield $[\mathbb{Q}(\pi) : \mathbb{Q}]$ is finite as well. But then π would be algebraic over $\mathbb{Q}$, contradicting transcendentality of π.

So suppose towards a contradiction that we have $\sqrt{3} \in \mathbb{Q}(\sqrt{\pi})$. Then there exist polynomials $f(\sqrt{\pi}), g(\sqrt{\pi})$ with $g(\sqrt{\pi}) \neq 0$ so that

$$\left(\frac{f(\sqrt{\pi})}{g(\sqrt{\pi})}\right)^2 = 3$$
$$f(\sqrt{\pi})^2 = 3g(\sqrt{\pi})^2.$$

Let A be the leading coefficient of f, and let B be the leading coefficient of g (so $B \neq 0$). Then comparing leading coefficients on both sides yields

$$A^2 = 3B^2,$$

so $3 = (A/B)^2$, contradicting irrationality of $\sqrt{3}$. Thus, we can fill in some degrees in the field extension diagram

$$\begin{tikzcd}
& \mathbb{Q}(\sqrt{\pi}, \sqrt{3}) = \mathbb{Q}(\sqrt{\pi} + \sqrt{3}) & \\
\mathbb{Q}(\sqrt{\pi}) \arrow[ur, "2"] & & \mathbb{Q}(\pi, \sqrt{3}) \arrow[ul] \\
& \mathbb{Q}(\pi) \arrow[ul, "2"] \arrow[ur] &
\end{tikzcd} \tag{8}$$

Then the multiplicative property of the degree yields $[\mathbb{Q}(\sqrt{\pi} + \sqrt{3}) : \mathbb{Q}(\pi)] = 4$, with basis $1, \sqrt{\pi}, \sqrt{3}, \sqrt{3\pi}$.

So we are on the hunt for some degree 4 polynomial which has $\sqrt{\pi}+\sqrt{3}$ as a root.

I claim that the minimal polynomial for $\sqrt{\pi} + \sqrt{3}$ is

$$\boxed{f(x) = x^4 - 2(3 + \pi)x^2 + (\pi - 3)^2.}$$

Since f There are a couple of ways you could arrive at this minimal polynomial. One way is to let $f(x)$ be the minimal polynomial for $\sqrt{3} + \sqrt{\pi}$ over $\mathbb{Q}(\pi)$ and guess that the other roots of f are

$$-\sqrt{3} + \sqrt{\pi}, \sqrt{3} - \sqrt{\pi}, \text{ and } -\sqrt{3} - \sqrt{\pi},$$

so that

$$f(x) = \Big(x-(\sqrt{3}+\sqrt{\pi})\Big)\Big(x+(\sqrt{3}+\sqrt{\pi})\Big)\Big(x-(\sqrt{3}-\sqrt{\pi})\Big)\Big(x+(\sqrt{3}-\sqrt{\pi})\Big)$$

Later we will motivate this guess further by noting that the other roots of the minimal polynomial should be the orbit of $\sqrt{\sqrt{\pi} + \sqrt{3}}$ under the action of the Galois group, which must also send $\sqrt{\pi}$ and $\sqrt{3}$ to the other roots of their minimal polynomials, which are $-\sqrt{\pi}$ and $-\sqrt{3}$, respectively.

If you just found this minimal polynomial and didn't do the degree considerations to show it was irreducible, you could show that it's irreducible by showing that first none of the 4 roots are in $\mathbb{Q}(\pi)$, and then showing that no way of pairing up the linear factors given above into two quadratics yields a factorization of f in $\mathbb{Q}(\pi)[x]$.

For another approach, since the minimal polynomial is degree 4, we seek $A, B, C, D \in \mathbb{Q}(\pi)$ so that

$$(\sqrt{3}+\sqrt{\pi})^4 = A + B(\sqrt{3}+\sqrt{\pi}) + C(\sqrt{3}+\sqrt{\pi})^2 + D(\sqrt{3}+\sqrt{\pi})^3$$

Expanding out both sides and collecting coefficients of $1, \sqrt{3}, \sqrt{\pi}$, and $\sqrt{3\pi}$ yields

$$\begin{aligned}(9+18\pi+\pi^2)+(4\pi+12)\sqrt{3\pi} &= (A+3C+C\pi)\cdot 1+(B+3D+3D\pi)\sqrt{3}\\ &\quad +(B+9D+D\pi)\sqrt{\pi}+2C\sqrt{3\pi}\end{aligned}$$

Since $1, \sqrt{3}, \sqrt{\pi}$ and $\sqrt{3\pi}$ are linearly independent over $\mathbb{Q}(\pi)$, this yields the equations

$$\begin{aligned}9+18\pi+\pi^2 &= A+3C+C\pi\\ 0 &= B+3D+3D\pi\\ 0 &= B+9D+D\pi\\ 4\pi+12 &= 2C\end{aligned}$$

Solving this system of equations for A, B, C, D yields the given minimal polynomial.

6 Problem 6

Prove that a field extension $K \subset L$ of prime degree is simple.

Proof. Throughout this proof, we make use of the following basic fact. A field extension $E \subset F$ has degree 1 if and only if $E = F$. There is something to prove here, so please justify this for yourself.

Let $p = [L : K]$. Since $p > 1$, there is some $\alpha \in L$ with $\alpha \notin K$. I claim that $L = K(\alpha)$.

To see why this is the case, consider the chain of field extensions

$$K \subset K(\alpha) \subset L.$$

Then by the multiplicative property of the degree, we have that

$$p = [L : K(\alpha)] \cdot [K(\alpha) : K].$$

Since p is prime, exactly one of the following must hold

(1) $[L : K(\alpha)] = 1$ and $[K(\alpha) : K] = p$, or

(2) $[L : K(\alpha)] = p$ and $[K(\alpha) : K] = 1$.

These conditions imply the following two conditions, respectively

(1') $L = K(\alpha)$

(2') $K(\alpha) = K$.

We know that (2') does not hold, as $\alpha \notin K$ by assumption. Thus, (2) does not hold, so (1) must hold, so (1') holds, as desired. $\square$