Math 410, Spring 2026 Professor Rob Benedetto

Solutions to the Midterm Exam

1. **(20 points)** Let $f(x) = x^4 + 9x^3 + 15x^2 - 6 \in \mathbb{Q}[x]$. Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{C}$ be the roots of f, so that $f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \alpha_4)$.

1(a) Prove that f is irreducible over $\mathbb{Q}$.

1(b) Compute $\alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2$.

Solution. (a) Apply Eisenstein's Criterion with $p = 3$. We have $3 \nmid 1$ but $3|9$, $3|15$, $3|0$, and $3|(-6)$, while $3^2 \nmid (-6)$. Thus, by Eisenstein with $p = 3$, f is irreducible over $\mathbb{Q}$. QED(a)

(b): $\sum \alpha_i^2 = \Big(\sum \alpha_i\Big)^2 - 2\Big(\sum \alpha_i\alpha_j\Big) = \sigma_1^2 - 2\sigma_2 = (-9)^2 - 2(15) = 81 - 30 = \boxed{51}$

---

2. **(25 points)** Let F be a field, let $f \in F[x]$ be a monic polynomial with $\deg(f) = 3$, and let L be a splitting field of f over F. Let $c = \Delta(f) \in F$ be the discriminant of f.

(a) Prove that $\sqrt{c} \in L$. That is, prove that $x^2 - c \in F[x]$ has a root in L.

(b) Prove that if f is irreducible over F, and if c is *not* the square of any element of F, then $[L : F] = 6$.

Solution. Let $\alpha_1, \alpha_2, \alpha_3 \in L$ be the roots of f.

(a) Let $b = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) \in L$. Then $b^2 = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2 = \Delta(f) = c$. Thus, $x^2 - c$ has a root in L, namely $b \in L$. QED (a)

Since f is irreducible, we have $[F(\alpha_1) : F] = \deg(f) = 3$.
Thus, by the Tower Theorem, $[L : F] = [L : F(\alpha_1)][F(\alpha_1) : F] = 3[L : F(\alpha_1)]$ is divisible by 3.

On the other hand, since $\sqrt{c} \notin F$, we have that $x^2 - c \in F[x]$ is irreducible over F,
since it has degree 2. Therefore, $[F(\sqrt{c}) : F] = 2$. Thus, by the Tower Theorem, since $\sqrt{c} \in L$,
we have $[L : F] = [L : F(\sqrt{c})][F(\sqrt{2}) : F] = 2[L : F(\sqrt{c})]$ is divisible by 2.

Hence, we have $6|[L : F]$. Since $\deg(f) = 3$, we know from a Theorem that its splitting field L has $[L : F] \leq 6$. Thus, $[L : F] = 6$. QED (b)

---

3. **(25 points)** Recall that the fifth root of unity $\zeta_5 \in \mathbb{C}$ is a root of the 5-th cyclotomic polynomial $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$, and that Φ_5 is irreducible over $\mathbb{Q}$. Define $\alpha = \zeta_5 + \zeta_5^{-1}$.

(a) Prove that α is a root of the polynomial $g(x) = x^2 + x - 1$.

(b) Prove that $\sqrt{5} \in \mathbb{Q}(\zeta_5)$.

Solution. (a) We have $g(\alpha) = (\zeta_5 + \zeta_5^{-1})^2 + (\zeta_5 + \zeta_5^{-1}) - 1 = \zeta_5^2 + 2 + \zeta_5^{-2} + \zeta_5 + \zeta_5^{-1} - 1$
$= \zeta_5^2 + \zeta_5 + 1 + \zeta_5^{-1} + \zeta_5^{-2} = \zeta_5^{-2}\Phi_5(\zeta_5) = 0$. QED (a)

(b) By the quadratic formula, the roots of g are $\dfrac{-1 \pm \sqrt{1 - (-4)}}{2} = \dfrac{-1 \pm \sqrt{5}}{2}$. Thus, by part (a), we have $2\alpha + 1 = \big(-1 \pm \sqrt{5}\big) + 1 = \pm\sqrt{5}$, so that $\sqrt{5} = \pm(2\alpha + 1) \in \mathbb{Q}(\zeta_5)$. QED (b)

---

4. **(30 points).** Recall that $\mathbb{F}_2$ denotes the field with 2 elements. Let $h(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$. Let $L = \mathbb{F}_2(\beta_1)$, where β_1 is a root of h.

(a) Prove that each of the following three elements of L is also a root of h:

$$\beta_2 = \beta_1^2, \qquad \beta_3 = \beta_1 + 1, \qquad \beta_4 = \beta_1^2 + 1.$$

(b) Prove that $\beta_1 \neq \beta_4$.

(c) In fact, it turns out that all four of $\beta_1, \beta_2, \beta_3, \beta_4$ are distinct. Assuming this fact, prove that L is normal and separable over $\mathbb{F}_2$.

Solution. (a) Using the facts that $(a+b)^2 = a^2 + b^2$ and hence also $(a+b)^4 = a^4 + b^4$, we compute:

$h(\beta_2) = \beta_1^8 + \beta_1^2 + 1 = (\beta_1^4 + \beta_1 + 1)^2 = 0^2 = 0$

$h(\beta_3) = (\beta_1 + 1)^4 + (\beta_1 + 1) + 1 = (\beta_1^4 + \beta_1 + 1) + 2 = 0 + 0 = 0$

$h(\beta_4) = (\beta_2 + 1)^4 + (\beta_2 + 1) + 1 = (\beta_2^4 + \beta_2 + 1) + 2 = 0 + 0 = 0$ QED (a)

(b) Suppose, towards contradiction, that $\beta_1 = \beta_4$. Then $\beta_1 = \beta_1^2 + 1$, so that $\beta_1^2 + \beta_1 + 1 = 0$
Adding the equation $\beta_1^4 + \beta_1 + 1 = 0$, we get $\beta_1^4 + \beta_1^2 = 0$, and hence $\beta_1^2(\beta_1 + 1)^2 = 0$, so either $\beta_1 = 0$ or $\beta_1 = 1$. But $h(0) = h(1) = 1$, so this is a contradiction. Thus, $\beta_1 \neq \beta_4$. QED (b)

(c) By the assumption, $\beta_1, \beta_2, \beta_3, \beta_4 \in L$ must be all four roots of h. By their definitions in part (a), each β_i can be expressed in terms of β_1, and hence h splits completely over $L = \mathbb{F}_2(\beta_1)$. So the splitting field is $K = \mathbb{F}_2(\beta_1, \beta_2, \beta_3, \beta_4) \subseteq L$.
On the other hand, $L \subseteq K$ since $\beta_1 \in K$. Thus, $L = K$ is the splitting field of h over F. Hence, by a Theorem, $L/\mathbb{F}_2$ is normal.
In addition, since all roots of h are distinct, the minimal polynomial of β_1 over $\mathbb{F}_2$ divides h and hence is separable. [In fact, h turns out to be irreducible and therefore is itself the minimal polynomial of β_1 over $\mathbb{F}_2$. But we didn't need that fact here, so I'm not going to prove it.]
Thus, by another Theorem, $L/\mathbb{F}_2$ is separable. QED (c)