MATH 422 Assignment 2

Cindy Tan
57195142
2 Oct 2019

1. (a) If \( f(x) = 8x^3 - 6x - 1 \) is reducible in \( \mathbb{Q}[x] \), write \( f = gh \) where \( g, h \in \mathbb{Q}[x] \) and \( \deg g \leq \deg h \leq 2 \). \( \mathbb{Q} \) is a domain so \( \deg g + \deg h = \deg f = 3 \). Then \( \deg g = 1 \) so \( f \) has a rational root \( r = \frac{a}{b} \) where \( a, b \in \mathbb{Z} \) and \( \gcd(a, b) = 1 \). By the rational root test, \( a \mid 1 \) and \( b \mid 8 \), so \( r \in \{ \pm 1, \pm \frac{1}{2}, \pm \frac{1}{4}, \pm \frac{1}{8} \} \). None of these are roots:

\[
\begin{align*}
  f(1) &= 1, \quad f\left(\frac{1}{2}\right) = -3, \quad f\left(\frac{1}{4}\right) = \frac{1}{8} - \frac{5}{2} < 0, \quad f\left(\frac{1}{8}\right) = \frac{1}{64} - \frac{7}{4} < 0, \\
  f(-1) &= -3, \quad f\left(-\frac{1}{2}\right) = 1, \quad f\left(-\frac{1}{4}\right) = -\frac{9}{8} + \frac{3}{2} > 0, \quad f\left(-\frac{1}{8}\right) = -\frac{65}{64} + \frac{3}{4} < 0
\end{align*}
\]

Thus \( f \) is irreducible in \( \mathbb{Q}[x] \). \( \square \)

(b) It suffices to prove that \( f(x) = x^4 + x + 1 \) is irreducible in \( \mathbb{F}_2[x] \).

Suppose \( f = gh \) where \( g, h \in \mathbb{F}_2[x] \) and \( \deg g \leq \deg h \leq 3 \). Since \( f(0) = 1 \) and \( f(1) = 1 \), \( f \) has no root in \( \mathbb{F}_2 \), so \( \deg g > 1 \). Then \( \deg g = \deg h = 2 \).

Write \( g = x^2 + ax + 1 \) and \( h = x^2 + bx + 1 \) for \( a, b \in \mathbb{F}_2 \). The leading coefficients and constants are necessarily 1 because \( gh = f \). Then

\[
  f(x) = x^4 + x + 1 = (x^2 + ax + 1)(x^2 + bx + 1)
  = x^4 + (a + b)x^3 + (2 + ab)x^2 + (a + b)x + 1
\]

But this is a contradiction because the coefficients in \( f \) for \( x \) and \( x^3 \) are different.

Therefore \( f \) is irreducible in \( \mathbb{F}_2[x] \), and hence irreducible in \( \mathbb{Q}[x] \). \( \square \)

2. Applying the binomial theorem,

\[
(x + 2)^p = \sum_{k=0}^{p} \binom{p}{k} x^k 2^{p-k}
\]

\[
\frac{1}{x} ((x + 2)^p - 2^p) = \sum_{k=1}^{p} \binom{p}{k} x^{k-1} 2^{p-k} = x^{p-1} + 2 \binom{p}{p-1} x^{p-2} + \ldots + 2^{p-1} \binom{p}{1}
\]

Observe that \( p \) divides every coefficient except the leading coefficient, which is 1. Furthermore, \( p^2 \nmid p2^{p-1} \), the constant term. Thus Eisenstein’s criterion applies and the polynomial is irreducible in \( \mathbb{Q}[x] \).

Let \( f(x) = 1 + \prod_{i=1}^{n} (x - i) \in \mathbb{Z}[x] \) for \( n > 4 \). By Gauss’ lemma, it suffices to show that \( f \) is irreducible in \( \mathbb{Z}[x] \).

Suppose \( f = gh \) for \( g, h \in \mathbb{Z}[x] \) where \( \deg g, h \leq n - 1 \). For \( 1 \leq j \leq n \) we have that

\[ 1 = f(j) = g(j)h(j) \] so \( g(j) = h(j) \in \{1, -1\} \). Then the polynomial \( g - h \) has \( n \) roots. Since \( \deg(g - h) \leq \max(\deg g, \deg h) \leq n - 1 \), it must be that \( g - h = 0 \).

Then \( f = g^2 \) for \( g \in \mathbb{Z}[x] \) where \( g(j) = 1 \) for \( 1 \leq j \leq n \). Since \( \mathbb{Z} \) is a domain, \( n = \deg f = 2 \deg g \) is even.
Observe that for \( i, j \in \mathbb{Z} \), \( i - j \) divides \( g(i) - g(j) \) since \( g \) is a polynomial and
\( i^k - j^k = (i - j)(i^{k-1} + i^{k-2}j + \cdots + j^k) \). Suppose that \( g(1) = 1 \) (the case where \( g(1) = -1 \) is symmetric). If \( g(j) = -1 \) for some \( 2 \leq j \leq n \), then \( 1 - j \mid g(1) - g(j) = 2 \), so
\[ |1 - j| \leq 2 \implies j \leq 3. \]

Hence \( g(j) = 1 \) for \( j = 1 \) and for all \( 4 \leq j \leq n \). Then the polynomial \( g - 1 \) has \( n - 2 \) roots. Since \( n \geq 6 \), we have that \( n - 2 > \frac{n}{2} = \deg g \geq \deg(g - 1) \), so \( g - 1 = 0 \). This is clearly a contradiction because \( g = 1 \implies f = 1 \).

Therefore \( f \) is irreducible in \( \mathbb{Q}[x] \) because it is irreducible in \( \mathbb{Z}[x] \).

3. \( 1 \in F^\sigma \) because \( \sigma \) is a field automorphism so \( \sigma(1) = 1 \).

If \( x, y \in F^\sigma \), then \( \sigma(x \pm y) = \sigma(x) \pm \sigma(y) = x \pm y \) and \( \sigma(xy) = \sigma(x)\sigma(y) = xy \), so \( x \pm y, xy \in F^\sigma \).

For multiplicative inverses, note that \( 1 = \sigma(xx^{-1}) = \sigma(x)\sigma(x^{-1}) = x\sigma(x^{-1}) \). By uniqueness of inverses, \( \sigma(x^{-1}) = x^{-1} \), so \( x^{-1} \in F^\sigma \).

Therefore \( F^\sigma \) is a subfield of \( F \).

Let \( F_p \subseteq F \) denote the prime field of \( F \). Since \( F_p \) is contained in every subfield of \( F \), in particular \( F_p \subseteq F^\sigma \).

Let \( f(x) = x^p - x \in F[x] \). Then \( F^\sigma \) is precisely the set of all roots of \( f \). Since \( F[x] \) is a Euclidean domain, the number of roots of \( f \) is at most \( \deg f = p \) (evident by applying induction on the Euclidean division algorithm). Therefore \( F^\sigma = F_p \) since \( |F_p| = p \).

4. Let \( \phi : \mathbb{R}[x] \to \mathbb{C} \) be the ring map \( g \mapsto g(i) \). This map is surjective: Given \( a + bi \in \mathbb{C} \) for \( a, b \in \mathbb{R} \), we have \( a + bx \in \mathbb{R}[x] \) and \( \phi(a + bx) = a + bi \).

Let \( f = x^2 + 1 \in \mathbb{R}[x] \). \( f \) is irreducible since it has no roots in \( \mathbb{R} \) and \( \deg f = 2 \). Thus \( (f) \) is maximal since \( \mathbb{R}[x] \) is a PID. Evidently \( f = x^2 + 1 \in \ker \phi \) so by maximality, either \( \ker \phi = (f) \) or \( \ker \phi = \mathbb{R}[x] \). Since \( f \) does not map nonzero constant functions to 0, \( \ker \phi \neq \mathbb{R}[x] \). Thus \( \ker \phi = (f) \).

Then \( \phi \) descends to an isomorphism \( \mathbb{R}[x]/(f) \to \mathbb{C} \).