Name: ____________________

Math 103B SP23 Midterm 2 May 17, 2023 **Student ID:** _______________

Unless otherwise specified, you have to provide justification to all of your answers.

1. (4 points) Compute the gcd of $f(x) = 2x^4 - x^3 + 3x^2 - x + 2$ and $g(x) = x^4 - x^2 + 2x - 1$ in $\mathbb{Q}[x]$.

Solution:

$$\begin{aligned} f(x) &= g(x) \cdot 2 + (-x^3 + 5x^2 - 5x + 4) \\ g(x) &= (-x^3 + 5x^2 - 5x + 4)(-x - 5) + (19x^2 - 19x + 19) \\ -x^3 + 5x^2 - 5x + 4 &= (19x^2 - 19x + 19)(-\frac{1}{19}x + \frac{4}{19}). \end{aligned}$$

Gcd needs to be monic. Thus $\gcd(f(x), g(x)) = x^2 - x + 1$.

2. (8 points) For each of the following, is the polynomial irreducible in the corresponding ring? Justify your answer.

   (a) (2 points) $x^5 - 7$ in $\mathbb{Q}[x]$.

   Solution: It is irreducible, since it satisfies the Eisenstein criterion for $p = 7$.

   (b) (3 points) $x^4 + 2x^2 + 1$ in $\mathbb{F}_3[x]$.

   Solution: It is not irreducible, since $x^4 + 2x^2 + 1 = (x^2 + 1)^2$.

   (c) (3 points) $2x^4 - x^3 - 4x + 2$ in $\mathbb{Q}[x]$.

   Solution: It is not irreducible, since $x = \frac{1}{2}$ is a solution. Note that since the polynomial has integer coefficients, a rational number $\frac{a}{b}$ in reduced form (i.e. $\gcd(a, b) = 1$) is a root of the polynomial would imply that a divides the constant term, and b divides the leading coefficient. Thus the only possible candidates for rational root are $\pm 1, \pm 2$ and $\pm \frac{1}{2}$.

3. (8 points) For each of the following statement, explain why it is incorrect. In all except Q3d, it is enough to give a counterexample.

(a) Let R be an integral domain. If $x \in R$ is irreducible, then x is prime.

> **Solution:** In $R = \mathbb{Z}[\sqrt{-5}]$, the element 2 is irreducible but not prime.

(b) Let R be an integral domain. If R is a UFD, then R is a PID.

> **Solution:** $\mathbb{Z}[x]$ is a UFD but not a PID.

(c) Let R be a commutative ring with 1. A polynomial $f(x)$ of degree n in $R[x]$ has at most n roots (counting multiplicity).

> **Solution:** The polynomial $2x$ in $(\mathbb{Z}/6)[x]$ is of degree 1, but has 2 roots, namely 0,3.

(d) Let F be a field and $\alpha \in F$. The evaluation map $\text{eva}_\alpha : \mathbb{F}(x) \to \mathbb{F}$ given by $\text{eva}_\alpha(f(x)) = f(\alpha)$ is a ring homomorphism. (This is never a ring homomorphism, and you need to explain why.)

> **Solution:** This is not well-defined. In particular, $\text{eva}_\alpha(\frac{1}{x-\alpha})$ is not well-defined.

4. (a) (2 points) Prove that $\mathbb{C}$ is an algebraic extension of $\mathbb{R}$.

> **Solution:** $\mathbb{C} = \mathbb{R}[i]$, and i is a root of the polynomial $x^2 + 1$.

(b) (2 points) Explain why $\mathbb{R}$ is not an algebraic extension of $\mathbb{Q}$.

> **Solution:** There exists elements in $\mathbb{R}$ that are transcendental over $\mathbb{Q}$, for instance e and π.

5. (a) (3 points) Show that the polynomial x^2+1 is irreducible in $\mathbb{F}_3[x]$.

Solution: x^2+1 has no root in $\mathbb{F}_3$. Since x^2+1 is of degree 2 and has no root, it is irreducible.

(b) (2 points) Prove that the ideal (x^2+1) is prime in $\mathbb{F}_3[x]$.

Solution:

Proof. Since $\mathbb{F}_3$ is a field, $\mathbb{F}_3[x]$ is a PID. Thus all irreducible elements are prime, and therefore the ideal (x^2+1) is prime. □

(c) (2 points) List all elements of $\mathbb{F}_3[x]/(x^2+1)$.

Solution: With division algorithm, all polynomials $f(x) \in \mathbb{F}_3[x]$ is congruent to their remainders modulo x^2+1. Thus we can represent all elements of $\mathbb{F}_3[x]/(x^2+1)$ by polynomials of degree at most 1, i.e. $0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2$.

(d) (2 points) Prove that the ring $\mathbb{F}_3[x]/(x^2+1)$ is a field.

Solution:

Proof. Since (x^2+1) is prime, the quotient $\mathbb{F}_3[x]/(x^2+1)$ is an integral domain. Since it is finite, it is a field (by Wedderburn's Theorem). □