MATH 4000/6000 – Homework #4

posted March 10, 2025; due March 17, 2025

You did a number on me. But, honestly, baby, who's counting?
— Taylor Swift

Assignments are expected to be neat and stapled. **Illegible work may not be marked**. Starred problems (*) are required for those in MATH 6000 and extra credit for those in MATH 4000.

0. (UNDERSTANDING CHECKS. NOT TO TURN IN!) Let R be a commutative ring, not the zero ring.

   (a) Show that x is never a unit in $R[x]$. Deduce that $R[x]$ is never a field.

   (b) Suppose R is a domain. Show that there cannot be nonzero polynomials $p(x), q(x) \in R[x]$ with $p(x)^2 = x \cdot q(x)^2$. (Hint: Consider degrees!)

1. (What are subrings?) Let R be a ring, and let R' be a subset of R. We call R' a subring of R if
   (A) R' is a ring for the same operations $+$ and $\cdot$ as in R, *and*
   (B) R' contains the multiplicative identity 1 of R.

   For example, making the identification discussed in class, $\mathbb{Z}$ is a subring of $\mathbb{Q}$. Also, $\mathbb{R}$ is a subring of $\mathbb{C}$, and $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$.

   (a) Let R be a ring. Suppose that R' is a subset of R closed under the $+$ and $\cdot$ operations of R, that R' contains the additive inverse (in R) of each of its elements, and that R' contains 1_R. Show that R' is a subring of R.

   Hint. (B) holds by assumption. Check that all the ring axioms hold for R' in order to verify (A). To get started, show that 0_R must belong to R'.

   (b) Find a two-element subset R' of $R = \mathbb{Z}_6$ that satisfies condition (A) in the definition of a subring but not (B). Presenting the subset is enough; you do **not** have to give a detailed proof that (A) holds.

2. Let F be a field in which $1 + 1 \neq 0$, and let a be a nonzero element of F. Show that the equation $z^2 = a$ has either no solutions in F or exactly two distinct solutions.

   Hint. If $z_1^2 = a$ and $z_2^2 = a$, how are z_1 and z_2 related?

3. (a) Let $f(x) = x^2 - 1 \in \mathbb{Z}_{12}[x]$. What are all of the roots of $f(x)$ in $\mathbb{Z}_{12}$?

   (b) Let F be a field, and let $f(x) \in F[x]$ be a polynomial of degree n. Show that $f(x)$ has at most n distinct roots in F. Why does this not contradict what you found in (a)?

   Hint: Use induction on n; the root factor theorem should be helpful. Make sure it is clear from your proof why it doesn't apply in $\mathbb{Z}_{12}$!

4. Let F be a field. Prove that the units in $F[x]$ are precisely the nonzero elements of F.

   Hint. If $u(x)v(x) = 1$, what can you say about the degrees of $u(x)$ and $v(x)$?

5. Let F be a field. Recall the definition of the gcd in $F[x]$: a gcd of $a(x), b(x)$ is a common divisor of $a(x)$ and $b(x)$ in $F[x]$ that is divisible by every common divisor in $F[x]$.

   Show that if $d(x) \in F[x]$ is a gcd of $a(x), b(x)$, then so is $c \cdot d(x)$ for every nonzero $c \in F$. Conversely, show that every gcd of $a(x), b(x)$ in $F[x]$ has the form $c \cdot d(x)$ for some nonzero $c \in F$.

6. Find a gcd of the given polynomials in $F[x]$, for the given field F. Show your work.

(a) $f(x) = x^3 - 1$, $g(x) = x^4 + x^3 - x^2 - 2x - 2$, $F = \mathbb{Q}$,

(b) $f(x) = x^2 + 2x + 2$, $g(x) = x^2 + 1$, $F = \mathbb{Z}_3$.

7. By applying the Euclidean algorithm and then backtracking, determine $X(x), Y(x) \in \mathbb{Q}[x]$ with $(x^3 + 1)X(x) + (x^2 + 1)Y(x) = 1$. Then repeat the exercise with $\mathbb{Q}[x]$ replaced by $\mathbb{Z}_5[x]$.

8. Let F be a field. Give a detailed proof that every nonconstant polynomial in $F[x]$ can be written as a product of irreducible polynomials. (You are not asked to prove uniqueness in this problem.)

9. Later in the course we will construct a field K with 4 elements containing $\mathbb{Z}_2$ as subring. In this exercise, *assume* K is such a field. Then in addition to $0, 1$ from $\mathbb{Z}_2$, the field K has two extra elements; call these α and β.

   (a) Show that $\alpha + 1 = \beta$.

   Hint. Try process of elimination.

   (b) Show that $\alpha^2 = \beta$.

   (c) Show that both α and β are roots of x^2+x+1 and deduce that $x^2+x+1 = (x-\alpha)(x-\beta)$ in $K[x]$.

MATH 6000 problems

10. (***; MATH 6000 problem**) Recall that the system of Gaussian integers was defined as $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$.

    (a) Check that $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$. (Use the criterion of Exercise 1(a).)

    (b) Define a function $N\colon \mathbb{C} \to \mathbb{R}$ by $N(z) = z \cdot \bar{z}$, where $\bar{z}$ is the complex conjugate of z. This is called the Gaussian **norm** of z. Explain why $N(z)$ is a nonnegative integer for every $z \in \mathbb{Z}[i]$. For which $z \in \mathbb{C}$ is $N(z) = 0$?

    (c) Prove that $N(zw) = N(z)N(w)$ for all $z, w \in \mathbb{C}$.

    (d) Using (b, c), show that $z \in \mathbb{Z}[i]$ is a unit $\iff N(z) = 1$. By solving the equation $N(z) = 1$ with $z \in \mathbb{Z}[i]$, find (with proof) all units in $\mathbb{Z}[i]$.

11. (***; MATH 6000 problem**) In this exercise, we outline a proof of the following Division Algorithm for $\mathbb{Z}[i]$.

    Division Algorithm for $\mathbb{Z}[i]$: Let $a, b \in \mathbb{Z}[i]$, with $b \neq 0$. There are $q, r \in \mathbb{Z}[i]$ with

    $$a = bq + r, \quad \text{and} \quad N(r) < N(b). \tag{†}$$

    Example: Let $a = 10 + i$ and $b = 2 - i$. We have

    $$10 + i = (2 - i)\overbrace{(4 + 2i)}^{q} + \overbrace{i}^{r},$$

    where $1 = N(i) < N(2 - i) = 5$.

    (a) Explain (perhaps with a picture) why every complex number is within a distance $\frac{\sqrt{2}}{2}$ of some element of $\mathbb{Z}[i]$.

    Hint. Think about the complex plane. Where are the elements of $\mathbb{Z}[i]$ located there? How is the distance between two elements related to the norm of their difference?

    (b) Given $a, b \in \mathbb{Z}[i]$ with $b \neq 0$, let $Q = a/b$. (Remember that $\mathbb{C}$ is a field, so a/b exists in $\mathbb{C}$.) From part (a), you can find a Gaussian integer q with $|a/b - q| \leq \frac{\sqrt{2}}{2}$.
    Prove that if we define $r := a - bq$, then (†) holds. In fact, prove the stronger statement that $N(r) \leq \frac{1}{2}N(b)$.

    (c) Find $q, r \in \mathbb{Z}[i]$ satisfying (†) if $a = 5 + 7i$ and $b = 3 - i$.