MATH 3312, SPRING 2026: HOMEWORK 1

(1) Determine if the following statements are true or false. Give a line or two in justification.
  (a) For any commutative ring R and polynomials $f(x), g(x) \in R[x]$, we have
$$\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$$
  (b) $\mathbb{Z}/24\mathbb{Z}$ with its usual addition and multiplication is a field.
  (c) The quotient of $\mathbb{Z}[x]$ by the *subgroup* $\langle x \rangle$ generated by x has the structure of a commutative ring such that the quotient homomorphism
$$\mathbb{Z}[x] \to \mathbb{Z}[x]/\langle x \rangle$$
is a ring homomorphism.
  (d) There are only 3 finite abelian groups of order 8 up to isomorphism.
  (e) For a commutative ring R, the ideal generated by a polynomial $f(x) \in R[x]$ is all of $R[x]$ if and only if $f(x) = a$ is a constant polynomial with $a \in R^\times$.[1]

(2) Show that, for any commutative ring R, there is a *unique* ring homomorphism $\mathbb{Z} \to R$, and verify in addition that, if $R = k$ is a *field*, then we have the following dichotomy:
  (a) Either the homomorphism $\mathbb{Z} \to k$ is *injective*;
  (b) Or its kernel is $p\mathbb{Z}$ for a unique prime p.

Definition 1. If alternative (1) holds, we say that k has **characteristic** 0. If alternative (2) holds, we say that k has **characteristic** p.

(3) Construct a ring R with the following property: For any other commutative ring R', giving a ring homomorphism $f : R \to R'$ is equivalent to giving an element $x \in R'$ such that $x^2 + 1 = 0$.

(4) Fix a prime p, and construct a ring R with the following property: For any other commutative ring R', giving a ring homomorphism $f : R \to R'$ is equivalent to giving an element $x \in R'$ such that $x^2 + x + 1 = 0$ *and* requiring the condition that $p \cdot 1_R = 0 \in R$.

For any commutative ring R, write $R^\times \subset R$ for the set of invertible elements in R. For $a \in R$, write $m_a : R \xrightarrow{b \mapsto a \cdot b} R$ for the function given by multiplication-by-a.

An element $a \in R$ is a *zero divisor* if there exists a *non-zero* element $b \in R$ such that $a \cdot b = 0$. Otherwise, it is a *non*-zero divisor (the hyphenation here is still controversial).

(5) With the above notation:
  (a) Show that m_a is a homomorphism of additive groups (such a self-homomorphism is called an **endomorphism** of R as an additive group);
  (b) Show that m_a is invertible if and only if $a \in R^\times$ is invertible.
  (c) Show that m_a is injective if and only if a is a non-zero divisor.

A ring R is an **integral domain** if it contains no zero divisors apart from 0.

(6) Prove the following:
  (a) Every field is an integral domain;

[1] This is a tricky one!

(b) Every *finite* integral domain R is a field;
(c) The following assertions are equivalent for an integer $n \geq 1$:
   (i) $\mathbb{Z}/n\mathbb{Z}$ is a field.
   (ii) $\mathbb{Z}/n\mathbb{Z}$ is an integral domain.
   (iii) n is prime.

Hint: For (b), consider the multiplication by a endomorphism $m_a : R \to R$ for any non-zero $a \in R$.

(7) Fix a finite field k, and let $f(x) \in k[x]$ be a polynomial of degree ≥ 1. Show that the following are equivalent:
   (a) The quotient ring $k[x]/(f(x))$ is a field;
   (b) The quotient ring $k[x]/(f(x))$ is an integral domain;
   (c) $f(x)$ is irreducible.

(8) Let R be a commutative ring, and let $f(x) \in R[x]$ be a *monic* polynomial of degree n. Show:
   (a) $a \in R$ is such that $f(a) = 0$ *if and only if* $f(x) = (x-a)g(x)$ for some monic polynomial $g(x) \in R[x]$;
   (b) If $R = k$ is a field, then the set $\{a \in k : \ f(a) = 0\}$ has at most n elements.