Math 412. Adventure sheet on more rings

DEFINITION:

- A **domain** is a commutative ring R in which $0_R \neq 1_R$, and that has the property that whenever $ab = 0$ for $a, b \in R$, then either $a = 0$ or $b = 0$.
- A **field** is a commutative ring R in which $0_R \neq 1_R$ and every nonzero element has a multiplicative inverse.
- A **subring** S of a ring R as a subset which is a also a ring *with the same* $+, \times, 0$ *and* 1. **Caution!** This definition differs from the book's because they do not assume rings contain a multiplicative identity!

DEFINITION: Fix a commutative ring R.

- The **polynomial ring over** R is the set
$$R[x] = \{a_0 + a_1x + \cdots + a_nx^n \mid a_i \in R, n \in \mathbb{N}\},$$
with operations $+$ and $\times$ extended from those on the coefficients in R in the natural way.
- The **ring of** $n \times n$ **matrices over** R is the set $M_n(R)$ of $n \times n$ matrices with coefficients in R, with "matrix addition" and "matrix multiplication" as $+$ and $\times$.

A. WARM-UP: For each inclusion $S \subseteq R$, decide whether or not S is a subring of R.

(1) $\mathbb{N} \subseteq \mathbb{Z}$.
(2) The set of even integers $S = \{2n \mid n \in \mathbb{Z}\} \subseteq \mathbb{Z}$.
(3) $\mathbb{R}[x] \subseteq \mathbb{R}(x) := \left\{\frac{f(x)}{g(x)} \mid f(x), g(x) \in \mathbb{R}[x], g \neq 0\right\}$.[1]
(4) The set of diagonal matrices:
$$D := \left\{\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mid a, b \in \mathbb{R}\right\} \subseteq M_2(\mathbb{R}).$$
(5) The set of integer matrices $M_2(\mathbb{Z}) \subseteq M_2(\mathbb{R})$.
(6) The set of invertible real matrices
$$GL_2(\mathbb{R}) = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid ad - bc \neq 0, \text{ and } a, b, c, d \in \mathbb{R}\right\} \subseteq M_2(\mathbb{R}).$$
(7) Given a ring R, the set of constant polynomials $R \subseteq R[x]$.
(8) The set of polynomials with integer coefficients $\mathbb{Z}[x] \subseteq \mathbb{R}[x]$.
(9) $\mathbb{Z} \subseteq \mathbb{Z}[i]$
(10) The imaginary integers $\mathbb{Z}i = \{ni \mid n \in \mathbb{Z}\} \subseteq \mathbb{Z}[i]$.

B. FIND AN EXAMPLE OF:

(1) A noncommutative ring with a commutative subring.
(2) An infinite ring with a finite subring.
(3) A field that has a subring that is not a field.

C. Let $R = M_2(\mathbb{Z}_2)$ be the ring of 2×2 matrices over $\mathbb{Z}_2$.

(1) What are 0_R and 1_R?
(2) How many elements are in R?
(3) Is R commutative?
(4) Show that $r + r = 0_R$ for every element $r \in R$.

[1] $\mathbb{R}(x)$ is the ring of rational functions.

D. BASIC PROOFS.

(1) Let R be a ring, and suppose that $0_R = 1_R$. Show that $R = \{0_R\}$ is the ring with one element.
(2) Prove that every field is a domain.
(3) Prove that a subring of a field is a domain. Is the converse true?
(4) Let S be a subset of a ring R. Prove that S is a subring if and only if the inclusion map $S \hookrightarrow R$ sending $s \mapsto s$ is a ring homomorphism. Think carefully about the meaning of the symbols you are using in different contexts.
(5) Show that if R is a domain, and $x, y, z \in R$, then $xy = xz$ and $x \neq 0$ implies $y = z$.

THEOREM 4.3: The polynomial $R[x]$ is a domain if and only if R is a domain.

THEOREM 4.5: For any domain R, the **units** in $R[x]$ are the units in the subring R of constant polynomials. In particular, if $\mathbb{F}$ is a field, then the units in $\mathbb{F}[x]$ are the nonzero constant polynomials.

E. POLYNOMIAL RING PRACTICE. Use Theorem 4.3 and 4.5 above where appropriate.

(1) In $\mathbb{Z}_8[x]$, consider $f = (1 + 3x)$ and $g = (2x^2 + 4x^3)$. Compute and simplify $f + 4g$ and $(3x)^3 + g$. We abuse notation by representing congruence classes by any integer representative.
(2) How many polynomials of degree less than 3 are there in the ring $\mathbb{Z}_2[x]$?
(3) How many units are there in $\mathbb{Z}[x]$?
(4) Suppose that $f \in \mathbb{Q}[x]$ has degree 5. Find the degrees of the following polynomials: $f - x$, f^2, $f + 4x^{51}$, $f - 2x^5$, $(x^2 + 1)f^3$.
(5) Does $x^2 + 1$ have a multiplicative inverse in $\mathbb{Z}_2[x]$?
(6) In $\mathbb{Z}_8[x]$, compute $(1 + 4x)(1 - 4x)$. Is the hypothesis that R is a domain necessary in Theorem 4.5?

F. PROOF OF THEOREM 4.5. Let R be a domain. Consider R as the subring of $R[x]$ of constant polynomials.

(1) Show that any unit in R is a unit in $R[x]$.
(2) Explain why, for any $f, g \in R[x]$, $\deg(fg) = \deg f + \deg g$. What if R is not a domain?
(3) Prove that if $f \in R[x]$ is a unit, then f is a constant polynomial.
(4) Prove Theorem 4.5.
(5) Find a formula for the number of units in $\mathbb{Z}_p[x]$ where p is prime.