Math 412. Adventure sheet 8: 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
$$R[x] = \{a_0 + a_1 x + \cdots + a_n x^n \mid a_i \in R, n \in \mathbb{N}\},$$
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 $\times$.

Part 1: Continuing practice.

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 $\mathbb{Z}i = \{ni \mid n \in \mathbb{Z}\} \subseteq \mathbb{Z}[i]$.

Solution.

(1) No, no additive inverses.
(2) No. missing multiplicative identity.
(3) Yes.
(4) yes.
(5) yes.
(6) No, no zero.
(7) Yes.

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

(8) Yes.
(9) Yes.
(10) No, no 1.

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.

Solution.

(1) A6 above
(2) Example 1: $\mathbb{Z}_n \subseteq \mathbb{Z}_n[x]$
Example 2: $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots$
(3) $\mathbb{Z} \subseteq \mathbb{Q}$

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 $r \in R$.

Solution.

(1) $0_R = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, $1_R = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.
(2) $2^4 = 16$
(3) No:
$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}.$$
(4) This follows from the fact that this is true in every entry of a matrix in $\mathbb{Z}_2$.

D. SHORT 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 domain is a domain. In particular, a subring of a field is a domain.
(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 $y = z$.

Solution.

(1) It suffices to show that for any $r \in R$, $r = 0_R$. Since $r = r1_R = r0_R = 0_R$, this is so.
(2) Let $\mathbb{F}$ be a field. Assume $a, b \in \mathbb{F}$ satisfy $ab = 0$ but $a \neq 0$. Multiplication on the left by a^{-1} gives $a^{-1}(ab) = (a^{-1}a)b = 1 \cdot b = b = 0$. QED.
(3) It is clear that a subring of a domain is a domain: assume $a, b \in S \subset R$, where R is a domain, and $ab = 0$ in S. This also holds in the bigger ring R, so $a = 0_R$ or $b = 0_R$, since R is a a domain. Since $0_R = 0_S$, it follows that S is a domain too.

(4) Call the inclusion map ϕ. First, assume $S \subset R$ is a subring. We need to prove ϕ is a ring homomorphism. Since the 1 in R is the 1 of S, we know $\phi(1_S) = 1_R$. Also since ϕ is the inclusion map, $\phi(s_1 + s_2) = s_1 + s_2 = \phi(s_1) + \phi(s_2)$. Ditto for multiplication. So ϕ is a ring homomorphism.
Conversely, assume that $\phi : S \hookrightarrow R$ is a ring homomorphism. In particular S is a ring. Then $1_S = \phi(1_S) = 1_R$, so S and R have the same identity. Also $\phi(s_1 +_S s_2) = \phi(s_1) +_R \phi(s_2) = s_1 +_R s_2$. This is in S, since it is in the image of $s_1 +_S s_2$ under ϕ. So S is closed under the multiplication of R. Similarly, S is closed under the multiplication of R. Finally, for all $s \in$, we have $s +_R -s = 0_S$ using the addition in S. Applying ϕ, we have $\phi(s +_R -s) = \phi(0_S)$, which means that $\phi(s) +_R S\phi(-s) = 0_R$.

(5) Let R be a domain. $xy = xz$ implies $xy - xz = 0$, so $x(y - z) = 0$ by the distributive property. It follows from the definition of domain that $y - z = 0$, so $y = z$.

Part 2: Looking forward.

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?

Solution.

(1) $f + 4g = 1 + 3x$. $3x^3 + g = 7x^3 + 2x^2$.
(2) $2^3 = 8$
(3) By the theorem, the only units are the units in $\mathbb{Z}$, which are ± 1.
(4) 5, 51, not enough information, 17
(5) No, it is not a unit by the theorem.
(6) It is 1! Yes, the hypothesis of domain is necessary.

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.

Solution.

(1) There is some $s \in R$ such that $rs = 1$. This s also lives in $R[x]$, and is an inverse for r there.

(2) Whether R is a domain or not, $\deg(fg) \leq \deg f + \deg g$ always holds, since when we expand the product fg, we can only get terms of degree at most $\deg f + \deg g$. If R is a domain, and $f, g \neq 0$, let $f = ax^{\deg f} + f'$ and $g = bx^{\deg g} + g'$, where $\deg f' < \deg f$, $\deg g' < \deg g$, and $a, b \neq 0$. Then $fg = abx^{\deg f + \deg g} +$ lower degree terms, so $\deg fg = \deg f + \deg g$. If R was not a domain, we could have had $ab = 0$. E6 is an explicit example.

(3) If f is a unit, there is some g such that $fg = 1$. Since $\deg 1 = 0$, and $\deg f + \deg g = \deg fg = 0$, we must have $\deg f = 0$.

(4) We have already shown one implication in part 1. For the other, if f is a unit in $R[x]$, then $f \in R$ by part 3. If $fg = 1$, then g is also a unit, hence also a constant. Thus, f is a constant with a constant inverse, so is a unit in R.

(5) The units are exactly the units of $\mathbb{Z}_p$, which are the nonzero elements of $\mathbb{Z}_p$, of which there are exactly $p - 1$.