MATH 320 Unit 2 Exercises
Introduction to Rings

A *ring* is a set R with addition and multiplication, satisfying, for all $a, b, c \in R$:
(closure) $a + b \in R$ and $ab \in R$
(associativity) $(a + b) + c = a + (b + c)$ and $(ab)c = a(bc)$
(commutativity of $+$) $a + b = b + a$
(existence of 0) There is $0_R \in R$ such that $a + 0_R = 0_R + a = a$
(inverses of $+$) There is some $x \in R$ with $a + x = 0_R$. We write $x = (-a)$.
(distributivity) $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$
Optional: (existence of 1 "Ring with identity") There is some $1_R \in R$ such that $a1_R = 1_R a = a$
Optional: (commutativity of $\times$ "Commutative ring") $ab = ba$

Let R be a ring. Given $a, b \in R$, we say that a divides b, writing $a|b$, if there is some $c \in R$ with $ac = b$; we call a a *divisor* of b. If $r, s, t \in R$, we say that r is a *common divisor* of s, t if $r|s$ and $r|t$.

We call $a \in R$ a *unit* if there is some $x \in R$ with $ax = xa = 1_R$ (1_R must exist). We write $x = a^{-1}$. We call $a \in R$ a *zero divisor* if $a \neq 0_R$ and there is some nonzero $x \in R$ with $ax = 0_R$ or $xa = 0_R$.

Let R be a ring and $S \subseteq R$. We call S a *subring* of R if it is closed under addition and multiplication, contains 0_R, and for every $a \in S$ the solution of $a+x = 0_R$ is in S (not just in R).

A commutative ring R is an *integral domain* if it has identity 1_R and there are no zero divisors.

A nontrivial[a] commutative integral domain R is a *field* if every nonzero $a \in R$ is a unit.

For any ring R, we define $R[x] = \{a_0 + a_1x + \cdots + a_nx^n : a_i \in R, n \geq 0\}$, where x is a new element, that was not in R, which commutes with each element of R. We call n the *degree*[b] of the polynomial, writing $deg(f)$ or $deg(f(x))$, and a_n the *leading coefficient*, provided $a_n \neq 0_R$. $R[x]$ is called the *polynomial ring* with coefficients from R. Two polynomials are equal if their degrees are equal and all coefficients are equal. We call the polynomial *monic* if its leading coefficient $a_n = 1_R$.

Degree Sum Theorem: Let R be an integral domain, and $f(x), g(x)$ nonzero polynomials in $R[x]$. Then $deg(f(x)g(x)) = deg(f(x)) + deg(g(x))$.

[a] A ring R is trivial if $R = \{0_R\}$, i.e. $|R| = 1$.
[b] 0_R has no degree, while all other elements of R have degree 0.

For Sep. 23:

For problems 1 and 2: Fix $n \in \mathbb{Z}$ with $n \geq 2$. We work in $\mathbb{Z}_n$.

1. Let $a, b, c \in \mathbb{Z}$. Suppose that $[a] = [b]$. Prove that $[a + c] = [b + c]$ and $[ac] = [bc]$.

2. For $[a], [b] \in \mathbb{Z}_n$, we define addition and multiplication via $[a] \oplus [b] = [a + b]$ and $[a] \odot [b] = [ab]$. Prove that this is a commutative ring with identity, by verifying all the axioms.

3. Write out the addition and multiplication tables for $\mathbb{Z}_5$, using the names $[0], [1], [2], [3], [4]$ for the equivalence classes.

4. Solve $x^2 + x = [0]$ in $\mathbb{Z}_5$, then solve $x^2 + x = [0]$ in $\mathbb{Z}_6$.

For Sep. 25:

5. Let $R = \mathbb{Z}$ and define new operations via $a \oplus b = a + b - 1$ and $a \odot b = a + b - ab$. Prove that this is a commutative ring with identity.

6. Let R be a ring, and let $a \in R$ be a unit. Prove that we may cancel a from the left, i.e. if $ab = ac$ then $b = c$. [We may also cancel a from the right; no need to produce the very similar proof.] Also, prove that a (still a unit) is not a zero divisor.

7. Prove that $-a$ is unique, i.e. if $a + x = 0_R = a + x'$, then $x = x'$. Also, prove that if a is a unit, then a^{-1} is unique, i.e. if $ax = xa = 1_R = ax' = x'a$, then $x = x'$.

8. Set $S = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$. Prove that this is a subring of $\mathbb{R}$.

For Sep. 30:

9. Let R be a ring with identity. Suppose $a, b \in R$ are both units. Prove that ab is a unit.

10. Let $R = \left\{ \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix} \right) : a, b \in \mathbb{R} \right\}$, 2×2 matrices of a special type. Prove that this is a commutative ring with identity, using the usual matrix addition and multiplication as operations.

11. Let R, S be rings. We define addition and multiplication on the Cartesian product $R \times S$ via $(r, s) \oplus (r', s') = (r + r', s + s')$ and $(r, s) \odot (r', s') = (rr', ss')$, where $r + r'$ and rr' are using the operations in R and $s + s', ss'$ are using the operations in S. Prove that this forms a ring.

12. Determine which of $\mathbb{Z}_5$, $\mathbb{Z}_6$, the ring from exercise 5, the ring from exercise 8, and the ring from exercise 10, are integral domains or fields.

For Oct. 2:

13. Prove the Degree Sum Theorem. Then, demonstrate with an example that its conclusion does not hold for $R = \mathbb{Z}_6$.

14. Let R be an integral domain, and let $f(x) \in R[x]$. Prove that $f(x)$ is a unit in $R[x]$ if and only if $f(x) = a_0$ (i.e. $deg(f(x)) = 0$), where a_0 is some unit of R.

15. Let R be a ring, and let $f(x), g(x) \in R[x]$. Prove that $deg(f(x)g(x)) \leq deg(f(x)) + \deg(g(x))$ and $deg(f(x) + g(x)) \leq \max(deg(f(x)), deg(g(x)))$, whenever the degrees exist (i.e. we avoid the zero polynomial).

16. Let R be a ring with identity. Prove that $1_R x \in R[x]$ is neither a unit nor a zero divisor.

Extra:

17. Let p be prime. Prove that $x^2 + x = [0]$ in $\mathbb{Z}_p$ has exactly two solutions: $[0]$ and $[p-1]$.

18. Calculate (and simplify) $([a] \oplus [b])^3$ in $\mathbb{Z}_3$.

19. Let $R = M_2(\mathbb{R}) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) : a, b, c, d \in \mathbb{R}\}$, 2×2 matrices. Prove that this is a non-commutative ring with identity, using the usual matrix addition and multiplication as operations.

20. Find all the units in the ring from Exercise 19. Then find all the units the subring $S = M_2(\mathbb{Z}) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) : a, b, c, d \in \mathbb{Z}\}$.

21. Prove that if R is a ring and S is a subring of R, then S is itself a ring.

22. Let R be a commutative ring and let $b \in R$. Set $T = \{rb : r \in R\}$. Prove that T is a subring of R.

23. Let R, S be rings with identity. Prove that $R \times S$ has an identity, and determine the units in the ring $R \times S$.

24. Find a ring R and a polynomial $f(x) \in R[x]$ where $f(x)$ is a unit and $deg(f(x)) \geq 1$. Compare with Exercise 14.