Exercises 6, 13, 14, 21, 25, 26, pp. 230-233.

Problem 6. Are the following subrings of the ring of all functions from the closed interval $[0,1]$ to $\mathbb{R}$.

(a) the set of all functions $f(x)$ such that $f(q) = 0$ for all $q \in \mathbb{Q} \cap [0,1]$:

Yes. We check that these functions form an nonempty set closed under subtraction and multiplication. Nonemptiness is immediate.

If f, g are two functions in this set, then for any $q \in \mathbb{Q} \cap [0,1]$, $(f-g)(q) = f(q) - g(q) = 0 - 0 = 0$. Hence $f - g$ is in this set. Futhermore, $(fg)(q) = f(q)g(q) = 0 * 0 = 0$, so fg is in this set.

(b) the set of all polynomial functions:

Yes. Let p, q be polynomials. Clearly $p - q$ and pq are still polynomials, so polynomial functions are closed under subtraction and multiplication.

(c) the set of all functions which have only finite number of zeros, together with the zero function:

No. Let $f(x) = 1$ be the constant function and $g(x) = 1$ if $x \leq 1/2$ and $g(x) = -1$ if $x > 1/2$. Both f and g have a finite amount of zeros. However, $(f+g)(x) = 2$ if $x \leq 1/2$ else $(f-g)(x) = 0$, which has an infinite amount of zeros. Hence this set is not closed under $+$.

(d) the set of all functions which have an infinite number of zeros:

No. Let $f(x) = 0$ if $x \leq 1/2$ else 1 and let $g(x) = 1$ if $x \leq 1/2$ else 0. Then it is clear that $(f+g)(x) = 1$, which has no zeros. Hence this set is not closed under $+$.

(e) the set of all functions f such that $\lim_{x \to 1^-} f(x) = 0$:

Yes. We have from analysis that

$$\lim_{x \to 1^-} f(x) - \lim_{x \to 1^-} g(x) = \lim_{x \to 1^-} (f(x) - g(x))$$

and

$$\lim_{x \to 1^-} f(x) * \lim_{x \to 1^-} g(x) = \lim_{x \to 1^-} (f(x)g(x)).$$

Thus if $\lim_{x \to 1^-} f(x) = 0$ and $\lim_{x \to 1^-} g(x) = 0$, then

$$\lim_{x \to 1^-} f(x) - \lim_{x \to 1^-} g(x) = \lim_{x \to 1^-} f(x) * \lim_{x \to 1^-} g(x) = 0,$$

as desired.

(f) the set of all rational linear combinations of the fuctions $\sin nx$ and $\cos nx$, where $m, n \in \{0, 1, 2, \dots\}$:

???. TODO

And we're done.

Problem 13. An element x in R is called *nilpotent* if $x^m = 0$ for some $m \in \mathbb{Z}^+$.

(a) Show that if $n = a^k b$ for some integers a and b then $\overline{ab}$ is a nilpotent element of $\mathbb{Z}/n\mathbb{Z}$.

(b) If $a \in \mathbb{Z}$ is an integer, show that the element $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ is nilpotent if and only if every prime divisor of n is also a prime divisor of a. In particular, determine the nilpotent elements of $\mathbb{Z}/72\mathbb{Z}$ explicitly.

(c) Let R be the ring of functions from a nonempty set X to a field F. Prove that R contains no nonzero nilpotent elements.

Proof. We proceed with each separately:

(a) Let $n = a^k b$. If $k = 0$, then $n = b$ so $\overline{ab} = \overline{an} = \overline{0}$ is trivially nilpotent. Otherwise, if $k \geq 1$, we have $\overline{ab}^k = \overline{a^k b^k} = \overline{a^k b * b^{k-1}} = \overline{nb^{k-1}} = \overline{0}$, as desired. Thus $\overline{ab}$ is nilpotent.

(b) ($\Rightarrow$): Suppose every prime divisor of n is a divisor of a, i.e. for any prime p, $p \mid n \Rightarrow p \mid a$. By the fundemental theorem of arithmetic, write $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, where p_i are primes and $e_i > 0$. Then $p_1 \dots p_k \mid a$ by our hypothesis. Write $a = p_1 \dots p_k * b$ and $e = \max(e_1, \dots, e_k)$. Then

$$a^e = (p_1 \dots p_k * b)^e = p_1^e \dots p_k^e * b^e.$$

Since $e_i \leq e$, we can safely pull out each factor of $p_i^{e_i}$ to have $a^e = n * p_1^{e-e_1} \dots p_k^{e-e_k} * b^e$. Thus $\overline{a}$ is nilpotent:

$$\overline{a}^e = \overline{n * p_1^{e-e_1} \dots p_k^{e-e_k} * b^e} = \overline{0}.$$

($\Leftarrow$): If a is a nilpotent element of $\mathbb{Z}/n\mathbb{Z}$, then $a^m = 0$ for some $m \in \mathbb{Z}^+$. By the fundemental theorem of arithmetic, let $a = p_1^{d_i} \dots p_k^{d_k}$ for primes p_i and $d_i > 0$. Then $a^m = 0$ in $\mathbb{Z}/n\mathbb{Z}$ implies $n \mid a^m$ in $\mathbb{Z}$. Thus if p is any prime divisor of n, we have $p \mid n$ implies

$$p \mid n * b = a^m = p_1^{d_i m} \dots p_k^{d_k m} \Rightarrow \exists i, p \mid p_i^{d_i m} \Rightarrow \exists i, p = p_i.$$

Thus p is also a prime divisor of a, and our proof is complete.

TODO $\mathbb{Z}/72\mathbb{Z}$.

(c) We claim that anyu integral domain D has no nonzero nilpotent elements. Indeed, suppose $x \in D$ in nilpotent. Let $m \in \mathbb{Z}^+$ be the minimum number such that $x^m = 0$. If $m = 1$, then $x = x^1 = 0$, so we're done. Otherwise, if $m \geq 2$, then write $x^m = xx^{m-1} = 0$. By the minimality of m, we know that $x^{m-1} \neq 0$. Since D is an integral domain and therefore has no nonzero zero-divisors, we must have $x = 0$.

Now we return to the problem. Since F is a field it is also an integral domain. Then F has no nonzero nilpotent elements. Let $f \in R$ be nilpotent. Then $f^m = 0$ for some $m \in Z^+$. Thus for any $x \in X$, $f(x)^m = 0 \Rightarrow f(x) = 0$, i.e. $f = 0$, as desired.

□

Problem 14. Let x be a nilpotent element of the commutative ring R.

(a) Prove that x is either zero or a zero divisor.

(b) Prove that rx is nilpotent for all $r \in R$.

(c) Prove that $1 + x$ is a unit in R.

(d) Deduce that the sum of a nilpotent element and a unit is a unit.

Proof. Let x be nilpotent and $x^m = 0$ for some minimal number $m \in \mathbb{Z}^+$.

(a) Either $x = 0$ or $x^m = xx^{m-1} = 0$. In the second case, the minimality of m guarentees that $x^{m-1} \neq 0$; thus x is a zero-divisor.

(b) We may rewrite $(rx)^m = r^m x^m$ by the commutativity of R. Thus $(rx)^m = r^m x^m = r^m * 0 = 0$, as desired.

(c) We motivate ourselves with the well-known factorization of $1 - x^m$:

$$1 - x^m = (1 + x) \left(\sum_{k=0}^{m-1} (-1)^k x^k \right).$$

Since $x^m = 0$, the LHS is just 1, showing that $1 + x$ is a unit.

(d) Let $u \in R$ be a unit. Then $u + x = u(1 + u^{-1}x)$. Part (b) gives that $u^{-1}x$ is nilpotent; then part (c) gives that $1 + u^{-1}x$ is a unit. The product of units is a unit, thus $u(1 + u^{-1}x) = u + x$ is a unit.

□

Problem 21. Let X be any nonempty set.

(a) Prove that $\mathcal{P}(X)$ is a ring under the addition and multiplication given by the textbook.

(b) Prove that this ring is commutative, has an identity and is a Boolean ring.

Proof. We proceed with each separately:

(a) In the following let $A, B \subseteq X$.

1. $(X, +)$ *is a abelian group*:

   Closure: $(A - B \cap (B - A)$ is another subset of X, so addition is closed.

   Abelian: We have $A + B = (A - B) \cap (B - A) = (B - A) \cap (A - B) = B + A$.

   Identity: $\varnothing$, because $\varnothing + A = A + \varnothing = (A - \varnothing) \cup (\varnothing - A) = A \cup \varnothing = A$.

   Associativity: This is painful to check but it is true.

2. $(X, \times)$ *is a monoid*:

   Closure: $A \cap B$ is a subset of X, so multiplication is closed.

   Associativity: This is painful to check but it is true.

3. *Distribution laws*: Let $C \subseteq X$. Then

$$
\begin{aligned}
C \times (A + B) &= C \cap [(A - B) \cup (B - A)] \\
&= C \cap (A - B) \cup C \cap (B - A) \\
&= (C \cap A - C \cap B) \cup (C \cap B - C \cap A) \\
&= (C \times A - C \times B) \cup (C \times B - C \times A) \\
&= C \times A + C \times B.
\end{aligned}
$$

Thus $\mathcal{P}(X)$ is a ring.

(b) Clearly $A^2 = A \cap A = A$ for any $A \in \mathcal{P}(X)$. Hence $\mathcal{P}(X)$ is a boolean ring. By Exercise 15 in this section, every boolean ring is commutative. Thus $\mathcal{P}(X)$ is commutative. We have X is the identity, since $XA = X \cap A = A \cap X = AX = A$ for all $A \in \mathcal{P}(X)$.

□

Problem 25. Let I be the ring of integral Hamilton Quaterions and define

$$N : I \to \mathbb{Z} \text{ by } N(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2$$

(the map N is called the *norm*).

(a) Prove that $N(\alpha) = \alpha\overline{\alpha}$ for all $\alpha \in I$, where if $\alpha = a + bi + cj + dk$ then $\overline{\alpha} = a - bi - cj = dk$.

(b) Prove that $N(\alpha\beta) = N(\alpha)(\beta)$ for all $\alpha, \beta \in I$.

(c) Prove that an element of I is a unit if and only if it has norm $+1$. Show that $I^\times$ is isomprphic to the quaterion group of order 8.

Proof. **TODO** □

Problem 26. Let K be a field and $\nu : K^\times \to \mathbb{Z}$ a discrete valuation on K. Let R be the valuation ring of ν.

(a) Prove that R is a subring of K which contains the identity.

(b) Prove that for each nonzero element $x \in K$ either x or x^{-1} is in R.

(c) Prove that an element x is a unit of R if and only if $\nu(0) = 0$.

Proof. **TODO** □

Exercises 3, 4, 10, 11, pp. 238-239.

Problem 3. Let $R[[x]]$ be the *formal power series* of R in x. Define addition and multiplication as the textbook does.

(a) Prove that $R[[x]]$ is a commutative ring with 1.

(b) Show that $1 - x$ is a unit in $R[[x]]$ with inverse $1 + x + x^2 + \cdots$.

(c) Prove that $\sum_{n=0}^{\infty} a_n x^n$ is a unit in $R[[x]]$ if and only if a_0 is a unit in R.

Proof. We proceed with each separately:

(a) This proof is largely an extension of the proof that the power series $R[x]$ is a commutative ring. There is not much change in the fact that we may now have infinite nonzero indices.

(b) We have

$$\begin{aligned}(1-x)\left(\sum_{n=0}^{\infty} x^n\right) &= \sum_{n=0}^{\infty} x^n - \sum_{n=1}^{\infty} x^n \\ &= (1 + x + x^2 + \dots) - (x + x^2 + \dots) \\ &= 1.\end{aligned}$$

One may convince themselves that the sums telescope to "infinity," so the only term left is 1.

(c) Let $f(x) = \sum_{i=0}^{\infty} a_i x^i$. We want to find $g(x) = \sum_{j=0}^{\infty} b_j x^j$ such that $f(x)g(x) = 1$. Expanding the product, we have

$$f(x)g(x) = \left(\sum_{i=0}^{\infty} a_i x^i\right)\left(\sum_{j=0}^{\infty} b_j x^j\right) = \sum_{k=0}^{\infty}\left(\sum_{i=0}^{k} a_i b_{k-i}\right) x^k.$$

Comparing the coefficients, we see that $a_0 b_0 = 1$ and $\sum_{i=0}^{k} a_i b_{k-i} = 0$ for all $k \geq 1$. Hence if $f(x)$ is a unit, then a_0 is a unit in R.

Conversely, suppose a_0 is a unit in R. We proceed to constuct b_k for each $k \geq 1$ by recursion. We may rewrite each of the remaining equations as $a_0 b_k = -\sum_{i=1}^{k} a_i b_{k-i}$; multiplying by b_0 on both sides gives

$$b_k = -b_0 \sum_{i=1}^{k} a_i b_{k-i}.$$

Indeed, assume for the sake of strong induction that b_i is known for all $i < k$. Then clearly we can construct b_k. The base case $k = 0$ holds with $b_0 = a_0^{-1}$. Thus induction yields a solution for $f(x)g(x) = 1$. Therefore $f(x)$ is a unit.

□

Problem 4. Prove that if R is an integral domain then the ring of formal power series $R[[x]]$ is also an integral domain.

Proof. Let $f(x) = \sum_{i=0}^{\infty} a_i x^i$ and $g(x) = \sum_{j=0}^{\infty} b_j x^j$. We want to show that if $f(x)g(x) = 0$, then either $f(x) = 0$ or $g(x) = 0$.

Expanding the product, again we have

$$f(x)g(x) = \left(\sum_{i=0}^{\infty} a_i x^i\right)\left(\sum_{j=0}^{\infty} b_j x^j\right) = \sum_{k=0}^{\infty}\left(\sum_{i=0}^{k} a_i b_{k-i}\right) x^k.$$

We see that each coefficient $\sum_{i=0}^{k} a_i b_{k-i}$ must be zero. In particular, $a_0 b_0 = 0$; R is an integral domain, so $a_0 = 0$ or $b_0 = 0$. Without loss of generality assume that $b_0 = 0$. Note here that we may always assume $a_0 \neq 0$ by finding the smallest nonzero monomial $a_i x^i$ in $f(x)$ and factoring out x^i to write $f(x) = x^i f'(x)$. As proving $f(x)g(x) = 0$ is equivalent to $f'(x)g(x) = 0$, we may restart the proof with $f'(x)$ instead of $f(x)$ to guarentee $a_0' \neq 0$.

We proceed to show that $b_k = 0$ for all k via induction. Assume for the sake of induction that for all $i < k$, $b_i = 0$. Rewrite the coefficient equations as $a_0 b_k = -\sum_{i=1}^{k} a_i b_{k-i}$. The terms of the RHS each have a term b_i for $i < k$, so it collapses to zero. On the LHS, we know that $a_0 \neq 0$, therefore $b_k = 0$. Adding the base case $b_0 = 0$ completes the induction. Thus we have shown that $g(x) = 0$, and that $R[[x]]$ is an integral domain. $\square$

Problem 10. Consider the following elements of the integral group ring $\mathbb{Z}S_3$:

$$\alpha = 3(1,2) - 5(2,3) + 14(1,2,3) \text{ and } \beta = 6(1) + 2(2,3) - 7(1,3,2)$$

(where (1) is the identity of S_3). Compute the following elements:

(a) $\alpha + \beta$, **(b)** $2\alpha - 3\beta$, **(c)** $\alpha\beta$, **(d)** $\beta\alpha$, **(e)** a^2.

Proof. **TODO** Just apply the definitions given in the textbook.

(a) $\alpha + \beta = 6(1) + 3(1,2) - 3(2,3) + 14(1,2,3) - 7(1,3,2)$

(b)

$$\begin{aligned} 2\alpha - 3\beta &= 6(1,2) - 10(2,3) + 28(1,2,3) - 18(1) - 12(2,3) + 21(1,3,2) \\ &= -18(1) + 6(1,2) - 22(2,3) + 28(1,2,3) + 21(1,3,2) \end{aligned}$$

(c) $\alpha\beta =$ **TODO**

(d) **TODO**

(e) **TODO**

$\square$

Problem 11. Repeat the precedeing exercise under the assumption that the coefficients of α and β are in $\mathbb{Z}/3\mathbb{Z}$.

Proof. **TODO** $\square$

Exercises 15, 17, 18, 19, 24, 26, pp. 247-251.

Problem 15. Prove that the map $\mathcal{P}(X) \to R$ defined by $A \mapsto \chi_A$ is a ring homomorphism, where χ_A is the *characteristic function* of A.

Proof. **TODO** $\square$

Problem 17. Let R and S be nonzero rings with identity and denote their respective identities by 1_R and 1_S. Let $\varphi : R \to S$ be a nonzero homomorphism of rings.

(a) Prove that if $\varphi(1_R) \neq 1_S$, then $\varphi(1_R)$ is a zero divisor in S. Deduce that if S is an integral domain then every ring homomorphism from R to S sends the identity of R to the identity of S.

(b) Prove that if $\varphi(1_R) = 1_S$ then $\varphi(u)$ is a unit in S and that $\varphi(u^{-1}) = \varphi(u)^{-1}$ for each unit $u \in R$.

Proof. We proceed with each separately:

(a) We have $\varphi(1_R) = \varphi(1_R 1_R) = \varphi(1_R)\varphi(1_R)$. Factoring gives

$$0 = \varphi(1_R) - \varphi(1_R)\varphi(1_R) = \varphi(1_R)(1_S - \varphi(1_R)).$$

If $1_S \neq \varphi(1_R)$, then $1_S - \varphi(1_R)$ is nonzero; thus $\varphi(1_R)$ is a zero-divisor.

From this we may deduce that if S is an integral domain, then we must instead have $1_S - \varphi(1_R) = 0$. Thus $1_S = \varphi(1_R)$.

(b) Suppose $\varphi(1_R) = 1_S$ and let $u \in R$ be a unit. Then

$$\varphi(uu^{-1}) = \varphi(1_R) = 1_S = \varphi(u)\varphi(u^{-1}).$$

Similarily, $1_S = \varphi(u^{-1})\varphi(u)$. By definition then $\varphi(u^{-1}) = \varphi(u)^{-1}$ and $\varphi(u)$ is a unit.

□

Problem 18. Let R be a ring.

(a) If I and J are ideals of R prove that their intersection $I \cap J$ is also an ideal of R.

(b) Prove that the intersection of an arbitrary nonempty collection of ideals is again an ideal of R.

Proof. We proceed with each separately:

(a) Let $a \in I \cap J$ and $r \in R$. Then because I and J are ideals, $a \in I \Rightarrow ra \in I$ and $a \in J \Rightarrow ra \in J$. Thus $ra \in I \cap J$, as desired.

(b) Let $\{I_\alpha\}_{\alpha \in A}$ be an arbitrary nonempty collection of ideals. Let $a \in \bigcap_{\alpha \in A} I_\alpha$ and $r \in R$. Then

$$\forall \alpha \in A, a \in I_\alpha \Rightarrow ra \in I_\alpha.$$

Thus $ra \in \bigcap_{\alpha \in A} I_\alpha$ which proves that it is an ideal of R.

□

Problem 19. Prove that if $I_1 \subseteq I_2 \subseteq \ldots$ are ideals of R then $\bigcup_{n=1}^{\infty} I_n$ is an ideal of R.

Proof. Let $a \in \bigcup_{n=1}^{\infty} I_n$ and $r \in R$. We have $a \in I_m$ for some $m \in \mathbb{N}$. Thus $ra \in I_m \subseteq \bigcup_{n=1}^{\infty} I_n$; hence $\bigcup_{n=1}^{\infty} I_n$ is an ideal of R. □

Problem 24. Let $\varphi : R \to S$ be a ring homomorphism.

(a) Prove that if J is an ideal of S then $\varphi^{-1}(J)$ is an ideal of R. Apply this to the special case when R is a subring of S and φ is the inclusion homomorphism to deduce that if J is an ideal of S then $J \cap R$ is an ideal of R.

(b) Prove that if φ is surjective and I is an ideal of R then $\varphi(I)$ is an ideal of S. Give an example where this fails if φ is not surjective.

Proof. We proceed with each separately:

(a) Let $a \in \varphi^{-1}(J)$ and $r \in R$. We have $\varphi(a) \in J$ and $\varphi(r) \in S$, so since J is an ideal, $\varphi(r)\varphi(a) = \varphi(ra) \in J$. Hence $ra \in \varphi^{-1}(J)$, which proves that it is an ideal.

In the special case where $R \subseteq S$ and $\varphi = \iota$ is an inclusion, then $\varphi^{-1}(J) = J \cap R$ is an ideal of R.

(b) Let $b \in \varphi(I)$ and $s \in S$. Fix some $a \in R$ such that $\varphi(a) = b$. Since φ is surjective, there is some $r \in R$ such that $\varphi(r) = s$. Thus $sb = \varphi(r)\varphi(a) = \varphi(ra) \in \varphi(I)$, where the last equality is because $ra \in I$. Hence $\varphi(I)$ is an ideal.

If φ was not surjective, then consider the example $R = \mathbb{Z}$, $S = \mathbb{R}$, and $\varphi = \iota$ is the inclusion. Then $2\mathbb{Z}$ is an ideal of $\mathbb{Z}$, but not an ideal of $\mathbb{R}$, as $0.5 * 2 = 1 \notin 2\mathbb{Z}$.

□

Problem 26. Let R be a ring. For any $n \in \mathbb{Z}$ and $r \in R$, define $nr = r + \cdots + r$ (n times).

(a) Prove that the map $\mathbb{Z} \to R$ defined by $k \mapsto k1_R$ is a ring homomorphism whose kernel is $n\mathbb{Z}$, where n is the characteristic of R.

(b) Determine the characteristics of the rings $\mathbb{Q}$, $\mathbb{Z}[x]$, and $\mathbb{Z}/n\mathbb{Z}[x]$.

(c) Prove that if p is a prime and if R is a commutative ring of characteristic p, then $(a + b)^p = a^p + b^p$ for all $a, b \in R$.

Proof. We proceed with each separately:

(a) Denote the map by φ. We have $\ker \varphi \leq \mathbb{Z}$, and the subgroup structure of Z gives us $\ker \varphi = n\mathbb{Z}$ for some $n \in \mathbb{N}$. Since $n\mathbb{Z}$ is cyclic, we only need to look at where the generator, n, maps to. We must have $\varphi(n) = 0$ and furthermore n is the minimal number for which this occurs. Hence $\varphi(n) = n1_R = 0$ implies $\mathrm{char}(R) = n$.

(b) There is no $n \in \mathbb{N}$ such that $n1_{\mathbb{Q}} = n = 0$. Thus $\operatorname{char}(\mathbb{Q}) = 0$. Similarily, the variable x doesn't affect $n1_{\mathbb{Z}[x]}$, so $\operatorname{char}(\mathbb{Z}[x]) = 0$.

For $\mathbb{Z}/n\mathbb{Z}[x]$, we have $n1 = 0$ in $\mathbb{Z}/n\mathbb{Z}$, so the same holds in the polynomial ring. Thus $\operatorname{char}(\mathbb{Z}/n\mathbb{Z}[x]) = n$.

(c) As R is a communitative ring, we have enough structure to apply the binomal theorem:

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1} b + \binom{p}{2} a^{p-2} b^2 + \cdots + \binom{p}{p-1} a b^{p-1} + b^p.$$

If $k \neq 0, p$, consider $\binom{p}{k} = \frac{p!}{k!(p-k)!}$. The factors in the denominator $k!(p-k)!$ are strictly less than p, and thus do not divide p. Thus $p!/k!(p-k)!$ must have a factor of p. We have $\operatorname{char}(R) = p$, so all the terms but the first and last of $(a+b)^p$ are equal to zero. Thus $(a+b)^p = a^p + b^p$, as desired.

$\square$