Westlake University
Fundamental Algebra and Analysis I

Exercise sheet 6 - 1 : rings and modules

1. Let $r \in \mathbb{Z}^\times$. We equip the Abelian group $\mathbb{Z}^2$ with the multiplication $*$ defined by, $\forall\ (x_1, x_2) \in \mathbb{Z}^2$ and $(y_1, y_2) \in \mathbb{Z}^2$ by

$$(x_1, x_2) * (y_1, y_2) = (x_1y_1 + rx_2y_2, x_1y_2 + x_2y_1).$$

Verify that $(\mathbb{Z}^2, +, *)$ is a commutative unitary ring.

2. Let A be a unitary ring. For all $x, y \in A$, we put $[x, y] = xy - yx$.

(1) The Abelian group of A, equipped with the "product" $(x, y) \mapsto [x, y]$, is it a ring ?

(2) For all $x, y, z \in A$, verify

$$[x, [y, z]] + [y, [z, x]] + [z, [z, y]] = 0.$$

3. For an $n \in \mathbb{N}_{\geqslant 1}$, find all the homomorphisms of rings from $\mathbb{Z}^n$ to $\mathbb{Z}$.

4. In a unitary ring A, we suppose that, $\forall\ x \in A$, we have $x^2 = x$. We call this kind of ring a **Boolean ring**.

(1) Prove that A is commutative.

(2) If A contains at least 3 distinct elements, prove that A has a zero divisor.

(3) Prove that A cannot have exactly 3 elements.

(4) Construct an example of Boolean ring which has exactly 4 elements.

5. Prove that the only automorphism of $\mathbb{Q}$ is $\mathrm{Id}_{\mathbb{Q}}$, and this is an isomorphism from $\mathbb{Q}$ to $\mathbb{Q}$.

6. Prove that the only sub-field $\mathbb{Q}$ is $\mathbb{Q}$.

7. Let M be a subgroup of the additive group $(\mathbb{Z}, +)$. We assume that $M \neq \{0\}$.

(1) Show that $M \cap \mathbb{N}_{>0}$ is not empty.

(2) Let d be the least element of $M \cap \mathbb{N}_{>0}$. Show that any element of M is divisible by d.

(3) Deduce that $M = d\mathbb{Z}$, where $d\mathbb{Z}$ is defined as $\{dn \,|\, n \in \mathbb{Z}\}$.

8. Let $\mathbb{N}_{\geqslant 1}$ be the set of positive integers and R the set of functions defined on $\mathbb{N}_{\geqslant 1}$ with values in a commutative ring K. Define the sum in R to be the ordinary addition of functions, and define the **convolution product** by the formula

$$(f * g)(m) = \sum_{xy=m} f(x)g(y),$$

where the sum is taken over all pairs (x, y) of positive integers such that $xy = m$.

(1) Show that R is a commutative ring, whose unit element is the function δ such that

$$\delta(x) = \begin{cases} 1, & x = 1 \\ 0, & x \neq 1. \end{cases}$$

(2) A function f is said to be **multiplicative** if $f(mn) = f(tn)f(n)$ whenever m, n are relatively prime. If f, g are multiplicative, show that $f * g$ is multiplicative.

(3) Let μ be the **Möbius function** such that

$$\mu(n) = \begin{cases} 1, & n = 1, \\ (-1)^r, n = p_1 \cdots p_r, & p_1, \ldots, p_r \text{ are distinct primes}, \\ 0, & \text{others}. \end{cases}$$

Show that $\mu * \phi_1 = \delta$, where ϕ_1 denotes the constant function having value 1. [**Hint :** Show first that μ is multiplicative, and then prove the assertion for prime powers.] The Möbius inversion formula of elementary number theory is then nothing else but the relation $\mu * \phi_1 * f = f$.

9. Let A be a commutative unitary ring.

(1) Show that the multiplicative law

$$A \times A \longrightarrow A, \quad (a, b) \longmapsto ab$$

defines a structure of A-module on the additive group $(A, +)$.

(2) We call *ideal* of A any sub-A-module of A. Let I be a sub-A-module of A. Show that the mapping

$$(A/I) \times (A/I) \longrightarrow A/I, \quad ([a], [b]) \longmapsto [ab]$$

is well defined and determines a structure of monoid on A/I.

(3) Let I be an ideal of A. Show that the set A/I equipped with the additive law (from the quotient module structure on A/I) and the above multiplicative law forms a commutative unitary ring. Show that the projection mapping $A \to A/I$ is a morphism of unitary rings.

(4) Let $f : A \to B$ be a morphism of unitary rings.

  (a) Show that the kernel of f is an ideal of A.

  (b) Show that the image of f is a unitary subring of B.

  (c) Show that the mapping

$$\widetilde{f} : A/\operatorname{Ker}(f) \longrightarrow B, \quad [a] \longmapsto f(a)$$

  is an isomorphism of unitary rings.

(5) Show that there exists a unique morphism of unitary rings from $\mathbb{Z}$ to A.

10. Let k be a commutative unitary ring. In this exercice, we write the set of sequences in k parametrized by $\mathbb{N}$ (usually denoted as $k^{\mathbb{N}}$) in the form of $k[\![T]\!]$. If $(a_n)_{n\in\mathbb{N}}$ is a sequence in k, viewed as an element of $k[\![T]\!]$, we express it as

$$a_0T^0 + a_1T + a_2T^2 + \cdots + a_nT^n + \cdots$$

or in the form of

$$\sum_{n\in\mathbb{N}} a_nT^n.$$

We call it a *formal power series* with coefficients in k. In the above formal sum, we often omit the summand with coefficient 0. Moreover, the summand a_0T^0 is often written as a_0 for simplicity. For example, if $a_0 = a_2 = 1$ and $a_n = 0$ for $n \in \mathbb{N} \setminus \{0, 2\}$, then the formal series

$$\sum_{n\in\mathbb{N}} a_nT^n$$

is written in the abbreviated form as

$$1 + T^2.$$

(1) Show that the set $k[\![T]\!]$ equipped with the following composition law (written additively)

$$k[\![T]\!] \times k[\![T]\!] \longrightarrow k[\![T]\!],$$
$$\Big(\sum_{n\in\mathbb{N}} a_nT^n, \sum_{n\in\mathbb{N}} b_nT^n\Big) \longmapsto \sum_{n\in\mathbb{N}} (a_n + b_n)T^n$$

forms a commutative group.

(2) Show that the set $k[\![T]\!]$ equipped with the following composition law (written multiplicatively)

$$k[\![T]\!] \times k[\![T]\!] \longrightarrow k[\![T]\!],$$
$$\Big(\sum_{n\in\mathbb{N}} a_n T^n, \sum_{n\in\mathbb{N}} b_n T^n\Big) \longmapsto \sum_{n\in\mathbb{N}} \Big(\sum_{i=0}^{n} a_i b_{n-i}\Big) T^n$$

forms a commutative monoid.

(3) Show that, for any $(a,b) \in k \times k$ and any $(n,m) \in \mathbb{N} \times \mathbb{N}$, one has

$$(aT^n)(bT^m) = (ab)T^{n+m}.$$

(4) Show that $k[\![T]\!]$ equipped with the above (additive and multiplicative) compositions laws forms a commutative unitary ring .

(5) Show that an element

$$f = \sum_{n\in\mathbb{N}} a_n T^n$$

of $k[\![T]\!]$ is invertible if and only if a_0 is an invertible element of k. Write an algorithm to determine the inverse of f when it is invertible.

(6) Determine $(1 - aT)^{-1}$, where a is an element of k.

In the rest of the exercice, we suppose that the image of any $n \in \mathbb{N}_{\geqslant 1}$ by the unique morphism of unitary rings $\mathbb{Z} \to k$ is invertible.

(7) Show that there exists an element $f \in k[\![T]\!]$ such that $f^2 = 1 + T$. Determine this element.

(8) Let $D : k[\![T]\!] \to k[\![T]\!]$ be the mapping sending

$$f = \sum_{n\in\mathbb{N}} a_n T^n \in k[\![T]\!]$$

to

$$f' := \sum_{n\in\mathbb{N}} (n+1) a_{n+1} T^n.$$

Show that D is a surjective k-linear mapping.

(9) Determine the kernel of D.

(10) Determine the set of all formal series $f \in k[\![T]\!]$ which satisfy the equation

$$f' = f.$$

11. Let k be a commutative unitary ring. We denote by $k[T]$ the subring of $k[\![T]\!]$ that is composed of formal power series

$$P = \sum_{n\in\mathbb{N}} a_n T^n$$

such that

$$\deg(P) := \sup\{n \in \mathbb{N} \mid a_n \neq 0\}$$

is not $+\infty$. The element $\deg(P) \in \mathbb{N}\cup\{-\infty\}$ is called the *degree* of P. We say that P is *monic* if its degree is $\geqslant 0$ and if

$$a_{\deg(P)} = 1.$$

The formal power series that belong to $k[T]$ are called *polynomials.*

(1) Let F and G be polynomials. We assume that F is monic. Show that $\deg(FG) = \deg(F) + \deg(G)$.
(2) Let P be a monic polynomial. Show that, for any $F \in k[T]$, there exists a unique pair $(Q, R) \in k[T] \times k[T]$ such that $\deg(R) < \deg(P)$ and $F = PQ + R$. We could reason by induction on the degree of F.
(3) Let I be an ideal of $k[T]$. Suppose that there exists a monic polynomial $P \in I$ such that

$$\forall\, F \in I \setminus \{0\}, \quad \deg(P) \leqslant \deg(F).$$

Show that

$$I = Pk[T] = \{PQ \mid Q \in k[T]\}.$$

Prove that such monic polynomial of minimal degree P is unique.
(4) Suppose that k is a field. Show that any ideal I of $k[T]$ which is different from $\{0\}$ contains a monic polynomial P such that

$$\forall\, F \in I \setminus \{0\}, \quad \deg(P) \leqslant \deg(F).$$

(5) For any $F = a_0 + a_1T + \cdots + a_dT^d \in k[T]$ and any $x \in k$, let

$$F(x) = a_0 + a_1x + \cdots + a_dx^d \in k.$$

Show that, for any $x \in k$, the mapping

$$\mathrm{ev}_x : k[T] \longrightarrow k, \quad F \longmapsto F(x)$$

is a morphism of unitary rings.

12. Let k be a field, P be a non-zero element of $k[T]$ and d be the degree of P. Suppose that P is of the form

$$a_0 + a_1 T + \cdots + a_d T^d.$$

If x is an element of k such that $P(x) = 0$, then we say that x is a *root* of P.

(1) Let $x \in k$. Show that, if $P(x) = 0$, then there exists a unique element $Q \in k[T]$ such that $P = (T - x)Q$.

(2) Show that P can be written in the form

$$P = (T - x_1)^{d_1} \cdots (T - x_n)^{d_n} \widetilde{P},$$

where $x_1, \ldots, x_n$ are distinct roots of P in k and $\widetilde{P}$ does not have any root in k. Show that $d_1 + \cdots + d_n \leqslant d$.

(3) Deduce that the number of roots of P does not exceed d.

13. In this exercice, we let P be the element $T^2 + 1 \in \mathbb{R}[T]$ and we denote by I the ideal

$$P\mathbb{R}[T] = \{PQ \mid Q \in \mathbb{R}[T]\}.$$

We denote by $\mathbb{C}$ the quotient ring $\mathbb{R}[T]/I$ and denote by i the class of $T \in \mathbb{R}[T]$ in the quotient ring $\mathbb{C} = \mathbb{R}[T]/I$.

(1) Show that $i^2 = -1$ in $\mathbb{C}$.

(2) Show that any element of $\mathbb{C}$ can be written as $a + bi$, where a and b are real numbers. We could use the fact that any polynomial $F \in \mathbb{R}[T]$ can be written as $PQ + R$ where $\deg(R) \leqslant 1$.

(3) Show that the mapping $\mathbb{R}^2 \to \mathbb{C}$ sending $(a, b) \in \mathbb{R}^2$ to $a + bi$ is an $\mathbb{R}$-linear bijection.

(4) Let a, b, x and y be real numbers. Express $(a+bi)(x+yi)$ in terms of $u+vi$ with $(u, v) \in \mathbb{R}^2$. Check that the mapping $\mathbb{R} \to \mathbb{C}$ sending $a \in \mathbb{R}$ to $a + 0i$ is an injective mapping and also a morphism of unitary rings. Thus we can consider $\mathbb{R}$ as a unitary subring of $\mathbb{C}$.

(5) For any

$$F = \sum_{n \in \mathbb{N}} a_n T^n \in k[\![T]\!],$$

let

$$\iota(F) = \sum_{n \in \mathbb{N}} (-1)^n a_n T^n.$$

Show that $\iota : k[\![T]\!] \to k[\![T]\!]$ is an morphism of unitary rings and $\iota \circ \iota$ is the identity mapping. Deduce that ι is an isomorphism of unitary rings.

(6) Check that $\iota(k[T]) = k[T]$ and $\iota(P) = P$.

(7) For any $z = a + bi \in \mathbb{C}$, we define $\overline{z} = a - bi$. Show that the mapping $\mathbb{C} \to \mathbb{C}$ sending z to $\overline{z}$ is an isomorphism of unitary rings. We could use the result of the previous question.

(8) For any $z \in \mathbb{C}$, let $N(z) = z\overline{z}$. Show that $N(z)$ is a non-negative real number (in considering $\mathbb{R}$ as a unitary subring of $\mathbb{C}$), and it is positive whenever $z \neq 0$.

(9) Let z and w be elements of $\mathbb{C}$. Show that $N(zw) = N(z)N(w)$.

(10) Show that $\mathbb{C}$ is a field.

(11) Denote by $\mathbb{Z}[i]$ the subset of $\mathbb{C}$ that is composed of elements $a+bi$ with $(a, b) \in \mathbb{Z}^2$. Show that $\mathbb{Z}[i]$ is a unitary subring of $\mathbb{C}$.

(12) Show that, for any $z \in \mathbb{Z}[i]$, $N(z)$ is a natural number.

(13) Let z be an element of $\mathbb{Z}[i]^\times$. Show that $N(z) = 1$.

(14) Determine the set $\mathbb{Z}[i]^\times$.

14. We consider the morphism of unitary rings from $\mathbb{Z}[T]$ to $\mathbb{R}$ which sends $F \in \mathbb{Z}[T]$ to $F(\sqrt{2})$

(1) Show that
$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \,|\, (a, b) \in \mathbb{Z}^2\}$$
is a unitary subring of $\mathbb{R}$.

(2) Show that the mapping $N : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}$ which sends $a + b\sqrt{2}$ to $a^2 - 2b^2$ is a morphism of multiplicative monoid. We could inspire from the method of the previous exercice.

(3) Show that the invertible elements of $\mathbb{Z}[\sqrt{2}]$ are precisely those of the form $a + b\sqrt{2}$ with $a^2 - 2b^2 = 1$ or $a^2 - 2b^2 = -1$.

(4) Check that $(3, 2)$ is a solution of the equation $a^2 - 2b^2 = 1$ in $\mathbb{N}^2_{\geqslant 1}$.

(5) Let $\alpha = 3 + 2\sqrt{2}$. For any $n \in \mathbb{N}_{\geqslant 1}$, let $(a_n, b_n) \in \mathbb{N}^2$ such that
$$a_n + b_n\sqrt{2} = (3 + 2\sqrt{2})^n.$$
Show that the set of solutions of the equation $a^2 - 2b^2 = 1$ in $\mathbb{N}^2_{\geqslant 1}$ is precisely $\{(a_n, b_n) \,|\, n \in \mathbb{N}_{\geqslant 1}\}$.

15. For a fixed $n \in \mathbb{N}_{\geqslant 2}$, we denote by
$$\begin{array}{rccc} \gamma_n : & \mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ & x & \mapsto & \overline{x} \end{array}$$
the canonical quotient homomorphism.

(1) Let $a \in \mathbb{Z}$. Prove that the following statements are equivalent.

i. $\overline{a}$ is an invertible element in $\mathbb{Z}/n\mathbb{Z}$.
ii. $\overline{a}$ is not a zero divisor in $\mathbb{Z}/n\mathbb{Z}$.
iii. $\gcd(a, n) = 1$.

(2) Let $\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})$. Prove

$$\phi(n) = \#\{k \mid k \in [\![0, n-1]\!],\ \gcd(n, k) = 1\}.$$

In convention, we define $\phi(1) = 1$.

(3) Prove that the invertible elements of the ring $\mathbb{Z}/n\mathbb{Z}$ are those $\alpha \in \mathbb{Z}/n\mathbb{Z}$ which generate the additive group $\mathbb{Z}/n\mathbb{Z}$, which means $\mathbb{Z}/n\mathbb{Z} = \{k\alpha\}_{k\in\mathbb{Z}}$.

(4) Let $m, n \in \mathbb{N}_{\geqslant 2}$, and $\gcd(m, n) = 1$. Prove

$$\phi(mn) = \phi(m)\phi(n).$$

(5) Let $a \in \mathbb{Z}$, $\gcd(a, n) = 1$. Prove

$$a^{\phi(n)} \equiv 1 (\operatorname{mod} n).$$

(6) Let $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where $p_1, \ldots, p_k$ are distinct primes, and $\alpha_1, \ldots, \alpha_k \geqslant 1$. Prove

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

(7) For a prime p, prove that $\mathbb{Z}/p\mathbb{Z}$ is a field, and $\phi(p) = p - 1$. In this case, $\mathbb{Z}/p\mathbb{Z}$ is called the **finite field** of order p, usually denoted by $\mathbb{F}_p$.