# Abstract Algebra – II Rings and Algebras (环理论与代数)

## 2.1 Definitions and Examples

November 26, 2012

# Outline

## Definition and examples

# Definition and examples

## Definition

*A* (commutative) ring (环; with unit $1$) *is a set* $R$ *together with two operations* $+\colon R \times R \to R$ *and* $\cdot\colon R \times R \to R$ *that make* $(R, +)$ *an abelian group with neutral element* $0$, $(R, \cdot)$ *an (abelian) semi-group with neutral element* $1$, *compatible in the sense*

$$ba = ab \tag{1}$$

$$a(b + c) = ab + ac \tag{2}$$

## Example

1. The ring of integers is the set $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$ together with the addition $+$ and multiplication $\cdot$.

# Examples

2. The cyclic groups $\mathbb{Z}/(n)$ where $n > 0$ is a positive integer, inherit a multiplication, because $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ imply $ac \equiv bd \pmod{n}$. Note that some of these rings have zero-divisors, e.g. $n = 6$, $2 \cdot 3 \equiv 0 \pmod{6}$.
3. Let $R$ be any ring and consider the polynomials in one variable denoted $R[x]$. These are the finite sequences under the operation of component-wise addition and polynomial multiplication, i.e.

$$(a_0 + a_1 x + \cdots + a_m x^m)(b_0 + b_1 x + \cdots + b_n x^n) = \sum_{k=0}^{m+n} \sum_{l=\max(0,k-n)}^{\min(m,k)} a_l b_{k-l} x^k$$

Since $R \subset R[x]$ is compatible with the original structure (subring), the neutral element is $0 \in R$, the unit is $1 \in R$ and we denote $\deg(a_0 + \cdots + a_n x^n) := n$ if $a_n \neq 0$ the degree of the polynomial. The degree of the 0-polynomial is $-\infty$.

# Examples II

4. Further rings are the rational $\mathbb{Q}$, real $\mathbb{R}$, and complex numbers $\mathbb{C}$, and these are not only rings, but also *fields (域)*.
5. Given two rings $R$ and $S$, we can consider their direct sum (product) $R \oplus S$ with component-wise operation, i.e. $(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)$ and correspondingly for addition. The neutral elements are obviously $0 = (0, 0)$ and $1 = (1, 1)$, respectively. Also the inverses are $-1 = (-1, -1)$ or $-(a, b) = (-a, -b)$, in general. We can also do that with more than 2 rings. Note that the correpsonding rings have plenty of zero-divisors, even if the factors are integral (i.e. have no zero-divisors).

# Algebra (代数)

A very similar notion is that of an algebra. This is defined as follows:

## Definition

*An* (associative) algebra *over a field $F$ is a vector space $A/F$ together with an $F$-bilinear operation $\cdot : A \otimes A \to A$ (that is associative).*
*Rings are called commutative unital algebras over $\mathbb{Z}$.*

## Example

0. Note that the rings, e.g. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, are (unital commutative) $\mathbb{Z}$-algebras.

# Examples of Algebras I

1. Given a vector space $V$ over a field $F$, then its endomorphisms $\mathrm{End}(V) := \{(\phi\colon V \to V) : \mathit{linear}\}$ are not only a vector space over $F$, but indeed a unital algebra under matrix multiplication. A more particular example are the $n \times n$-matrices with entries in $F$ denoted as $\mathrm{Mat}_n(F)$. Note that this algebra is not commutative. It is therefore not a commutative ring.
2. The direct sum (product) also works for algebras.
   In this way the endomorphisms of a vector space have two multiplicative structures, one as endomorphisms (composition) and another one as a vector space with a particular identification to $F^{n^2}$ (thus being a direct sum of copies of the base field).

# Examples of Algebras II

3. Remember the quaternions $\mathbb{H} = \mathbb{R}(i, j, k)$. This is not a commutative ring, because $wz \neq zw$ for arbitrary $w, z \in \mathbb{H}$. Nevertheless it is a vector space over $\mathbb{R}$ and the multiplication is $\mathbb{R}$-linear. Therefore this is an $\mathbb{R}$-algebra. (Note that in Exercise **??** you have proven that $(\mathbb{H}, \cdot)$ is indeed associative, moreover $\mathbb{H}^* = \mathbb{H} \setminus 0$ is a group.) Because all elements (except for 0) are invertible, this is called a division algebra (可分代数).
4. Remember that the structure of $\mathbb{H}$ essentially arises from that of $Q := \langle i, j : i^4 = 1, i^2 = j^2, iji^{-1} = j^{-1} \rangle$. The generalization is the following: Given a (discrete / finite) (semi)-group $G$ together with a field $F$, then the group algebra (群的代数) $F[G]$ is the vector space $\langle \delta_g \in G \rangle_F$ together with the $F$-bilinear operation $*\colon F[G] \times F[G] \to F[G] : \delta_g * \delta_h = \delta_{gh}$ for all $g, h \in G$ (and $F$-linearly extended).

# Examples of Algebras III

5. Given two algebras $A$ and $B$ over the same field $F$, we can consider their tensor product (张量积) $A \otimes B$ that is spanned by the elements $\langle a \otimes b : a \in A, b \in B \rangle_F$ and define a multiplication as $(a_1 \otimes b_1)(a_2 \otimes b_2) := (a_1 a_2) \otimes (b_1 b_2)$ and $F$-linear extension. An example of that is the tensor product of (square) matrices which obeys the law $\mathrm{End}(F^m) \otimes \mathrm{End}(F^n) \cong \mathrm{End}(F^{mn})$ as induced by the tensor product of the underlying vector spaces $F^m \otimes F^n \cong F^{mn}$.
6. Consider the real vector space $\mathbb{R}^3$ together with the vector product $\times : \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3$. This operation is also bilinear and therefore $(\mathbb{R}^3, \times)$ is an algebra over $\mathbb{R}$. Note however that this algebra is not associative, because $(a \times b) \times c \neq a \times (b \times c)$ for all $a, b, c \in \mathbb{R}^3$. It fulfills however another nice property which makes it a Lie algebra (李代数).

Note that many of the notions introduced in the further sections have analogs for algebras.

# Exercises

## Exercise

Let $(A, +, \cdot)$ be any (unital) algebra with neutral elements $0$ (w.r.t. addition) and $1$ (w.r.t. multiplication). Show that $0a = 0 = a0$ for every $a \in A$.

## Exercise

Let $(R, +, \cdot)$ be a set with two monoidal operations $+$ and $\cdot$ neither of which need to be commutative, but both are associative, $\cdot$ is distributive over $+$, i.e.

$$(a + b)c = ac + bc,$$
$$a(b + c) = ab + ac,$$

and $+$ has inverse elements $-a \in R$ for every $a \in R$. Show that $(R, +, \cdot)$ is a (non-necessarily commutative) ring, i.e. $+$ is abelian.
Hint: Consider products $(a + b)(c + d)$.

## Exercise

a. Given an abelian group $(A, +)$. Show that its group-endomorphisms $\mathrm{End}(A, +)$ form a unital non-commutative associative ring.

b. Given any ring $(R, +, \cdot)$. Show that $(R, +, \cdot)$ embeds canonically into $\mathrm{End}(R, +)$.

## Exercise

a. Given the semi-group algebra $F[G] = \langle \delta_g : g \in G \rangle_F$ with the multiplication $\delta_g * \delta_h = \delta_{gh}$ show that this is associative as long as $G$ is a semi-group.

b. Given the polynomial multiplication as defined in the lecture, i.e.

$$(a_0 + a_1 x + \cdots + a_m x^m)(b_0 + b_1 x + \cdots + b_n x^n) := \sum_{k=0}^{m+n} \sum_{i+j=k} a_i b_j x^k$$

show that it is associative.

## Exercise

Let $\alpha \in \mathbb{C}$ be a zero of a non-trivial polynomial over $\mathbb{Z}$. Show that $\mathbb{Z}[\alpha] = \langle 1, \alpha, \alpha^2, \ldots \rangle_{\mathbb{Z}}$ is a ring together with an embedding $e\colon \mathbb{Z} \to \mathbb{Z}[\alpha] : n \mapsto n \cdot 1$.

a. Show that the Gaussian integers $\mathbb{Z}[\mathrm{i}] = \{a + b\mathrm{i} : a, b \in \mathbb{Z}\}$ form a ring. Find its units, i.e. those elements $u \in R := \mathbb{Z}[\mathrm{i}]$ that have a multiplicative inverse $v \in R$, i.e. $uv = 1 = vu$. Show that these elements form a group (under multiplication).

b. Show that also $\mathbb{Z}[\sqrt{-2}] \subset \mathbb{C}$ form a subring of the complex numbers. Find its units.

c. What happens when $\alpha \in \mathbb{C}$ is transcendental over $\mathbb{Q}$, i.e. not root of any non-trivial polynomial?

## Exercise

Let $R$ be a commutative ring (not necessarily with unit). Show that $R^1 := \mathbb{Z} \ltimes R$ with operations $(m, a) + (n, b) := (m + n, a + b)$ and $(m, a)(n, b) := (mn, ab + mb + na)$ is a unital ring. What is its multiplicative identity?