afcs
ALGEBRAIC FOUNDATIONS of COMPUTER SCIENCE
lectures by Ferucio Laurentiu Tiplea

Rings and Fields

Part I

Prof.dr. Ferucio Laurențiu Țiplea

Spring 2022

Department of Computer Science
"Alexandru Ioan Cuza" University of Iași
Iași 700506, Romania

e-mail: ferucio.tiplea@uaic.ro

Outline

Definitions, examples, basic properties

Rings

Definition 1

A ring is an algebraic structure $(R, +, -, 0, \cdot)$ such that:

- $(R, +, -, 0)$ is a commutative group;
- $(R, \cdot)$ is a semigroup;
- $\cdot$ is left- and right-distributive over $+$.

Remark 2

Let $(R, +, -, 0, \cdot)$ be a ring.

1. *"$+$" and "$\cdot$" are usually called addition and multiplication;*
2. *0 is called the zero element of R. It is unique;*
3. *If $\cdot$ is commutative then the ring is called commutative;*
4. *We will usually denote rings just by their carrier sets. That is, we will often say "Let R be a ring".*

Basic properties

Prove the following properties!

Proposition 3

Let $(R, +, -, 0, \cdot)$ be a ring. Then:

1. $a0 = 0a = 0$, *for any* $a \in R$;
2. $(-a)b = a(-b) = -(ab)$, *for any* $a, b \in R$;
3. $(-a)(-b) = ab$, *for any* $a, b \in R$;
4. $a(b - c) = ab - ac$ *and* $(b - c)a = ba - ca$, *for any* $a, b, c \in R$;
5. $(\sum_{i=1}^{n} a_i)(\sum_{j=1}^{m} b_j) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i b_j$, *for any* $n, m \geq 1$ *and* $a_i, b_j \in R$, $1 \leq i \leq n$, *and* $1 \leq j \leq m$.

Basic properties

Prove the following properties!

Proposition 4

Let R be a ring. Then:

1. $(-m)a = -(ma)$;
2. $(m+n)a = ma + na$;
3. $m(a+b) = ma + mb$;
4. $(mn)a = m(na)$;
5. $m(ab) = (ma)b = a(mb)$;
6. $(ma)(nb) = (mn)(ab)$,

for any $a, b \in R$ and $m, n \geq 1$.

Binomial formula

Proposition 5

Let R be a commutative ring. Then, for any $a, b \in R$ and $n \geq 1$, the following formula holds

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^{n-k} b^k \ ,$$

where $C_n^k = \frac{n!}{k!(n-k)!}$ for any $0 \leq k \leq n$, $a^n b^0$ is taken a^n, and $a^0 b^n$ is taken b^n.

Proof.

By mathematical induction on $n \geq 1$. □

Binomial formula

Remark 6

Let R be a commutative ring.

1. *R does not need unity for the binomial formula to hold in R.*
2. *To apply the binomial formula for a and b, only $ab = ba$ is needed and not the commutativity of the whole ring.*
3. *Conventions "$a^n b^0$ is taken a" and "$a^0 b^n$ is taken b" are not required when the ring has unity.*

Rings with unity

Definition 7

A ring with unity/identity is an algebraic structure $(R, +, -, 0, \cdot, e)$ which satisfies:

- $(R, +, -, 0)$ is a commutative group;
- $(R, \cdot, e)$ is a monoid;
- $\cdot$ is left- and right-distributive over $+$.

The element e, also denoted by 1_R or 1, is called the unity/identity of R. It is unique.

Rings with unity

Prove the following result!

Proposition 8

If $(R, +, -, 0, \cdot, e)$ *is a ring with unity then* $e = 0$ *iff* $R = \{0\}$*.*

Definition 9

A ring with unity $(R, +, -, 0, \cdot, e)$ which satisfies $e = 0$ is called a trivial/null ring.

If R is a ring with unity, then the set

$$U(R) = \{a \in R | \exists b \in R: \; ab = ba = e\}$$

forms a group under multiplication (prove it!), called the group of units or the unit group of R. Its elements are called units of R.

Division rings

Definition 10

1. A division ring, also called a skew field, is an algebraic structure $(R, +, -, 0, \cdot, ', e)$ which satisfies:
    1.1 $(R, +, -, 0)$ is a commutative group;
    1.2 $(R, \cdot, e)$ is a monoid and $e \neq 0$;
    1.3 $'$ is a unary operation which satisfies $aa' = a'a = e$, for any $a \neq 0$;
    1.4 $\cdot$ is left- and right-distributive over $+$.
2. A commutative division ring is called a field.

Prove the following property!

Proposition 11

If R is a division ring, then $R - \{0\}$ forms a group under multiplication.

Cancellation law of multiplication

The cancellation law of multiplication holds in a ring R if

$$ac = bc \text{ or } ca = cb \text{ implies } a = b \text{ or } c = 0,$$

for any $a, b, c \in R$.

Proposition 12

Cancellation law of multiplication holds in any division ring.

There are important rings that are not division rings, but the cancellation law still holds. Two such examples are the rings of integers and polynomials.

Zero divisors and the cancellation law

Definition 13

An element $a \in R - \{0\}$ of a ring R is called a zero divisor if there exists $b \in R - \{0\}$ such that $ab = 0$ or $ba = 0$.

Example 14

In $\mathbb{Z}_6$, $2, 3 \not\equiv 0 \bmod 6$ but $2 \cdot 3 \equiv 0 \bmod 6$.

Prove the following properties!

Proposition 15

1. *In any ring R, the absence of zero divisors is equivalent to satisfying the law of cancellation.*
2. *Division rings do not have zero divisors.*

Integral domains

Definition 16

A commutative ring R with unity $e \neq 0$ and with no zero divisors is called an integral domain.

Proposition 17

1. *Any field is an integral domain.*
2. *Any finite integral domain is a field.*
3. *Let $p \geq 2$. $\mathbb{Z}_p$ is a field iff p is a prime.*

Proof.

See textbook [1], page 319. $\square$

Classes of rings

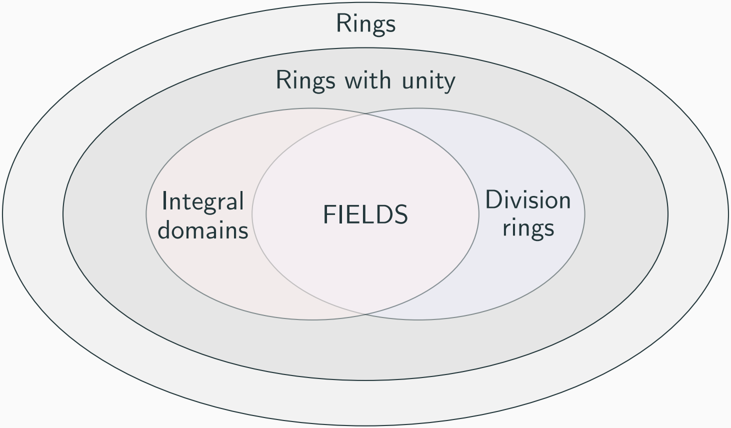

Figure 1: Relationships between classes of rings

Example 18

1. Let $(R, +, -, 0)$ be a commutative group. Define on R the binary operation $\cdot$ by $a \cdot b = 0$, for any $a, b \in R$. Then, $(R, +, -, 0, \cdot)$ is a ring.
2. $\mathbb{Z}$, together with addition and multiplication, form an integral domain, but not a field.
3. $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, together with addition and multiplication, form fields.
4. $n\mathbb{Z}$ is a commutative ring with no zero divisors. This ring has unity only if $n = -1$, $n = 0$, or $n = 1$ (for $n = 0$, the ring is null).
5. $\mathbb{Z}_n$ is a commutative ring with unity. If n is a prime, then $\mathbb{Z}_n$ is a field.

Homomorphism, subring, ideal

Homomorphisms

Definition 19

Let R_1 and R_2 be rings. A function $h : R_1 \to R_2$ is a ring homomorphism if, for any $a, b \in R_1$, the following hold:

1. $h(a + b) = h(a) + h(b)$;
2. $h(ab) = h(a)h(b)$.

The second property in the definition above may only be required for $a, b \in R_1 - \{0\}$. Indeed, if, for instance, $b = 0$, then

$$h(a0) = h(0) = 0 = h(a)0 = h(a)h(0).$$

If R_1 and R_2 have units e_1 and e_2, then the property

3. $h(e_1) = e_2$

is required too.

Subrings

Definition 20

Let R be a ring. A subring of R is a ring S such that $S \subseteq R$ and the operations of S are exactly the operations of R restricted to S.

Alternatively, $S \subseteq R$ nonempty defines a subring of R if:

1. $a - b \in S$, for any $a, b \in S$;
2. $ab \in S$, for any $a, b \in S$.

If R has unity e, then e must be in S too, and if R is a division ring, the second item should be replaced by "$ab^{-1} \in S$, for any $a, b \in S - \{0\}$".

Example 21

$n\mathbb{Z}$ is a subring of $\mathbb{Z}$, for any integer n (prove it!). The subset of odd integers do not form a subring of $\mathbb{Z}$ (prove it!).

Ideals

Definition 22

Let R be a ring and $J \subseteq R$.

1. R is called a left ideal in R if R is a subgroup of the additive group of R and $RJ \subseteq J$.
2. R is called a right ideal in R if R is a subgroup of the additive group of R and $JR \subseteq J$.
3. R is called an ideal in R if R is both a left and right ideal in R.
4. J is a proper ideal in R if it is an ideal in R and $J \neq \{0\}$ and $J \neq R$.

Prove the following result!

Proposition 23

A commutative ring with unity is a field if and only if it does not have proper ideals.

Characteristic of a ring

Characteristic of a ring

Definition 24

1. We say that a ring R has characteristic $n \geq 1$, if n is the smallest natural number such that $na = 0$, for any $a \in R$.
2. We say that a ring R has characteristic zero if does not exist $n \geq 1$ with $na = 0$ for any $a \in R$.

The characteristic of a ring R will be denoted by $char(R)$.

Remark 25

A ring with unity $e \neq 0$ cannot have the characteristic 1. Therefore, the only ring of characteristic 1 is the null ring.

Remark 26

If the characteristic of a ring R is $n > 1$, then the additive order of each non-zero element $a \in R$ divides n.

Characteristic of a ring: examples

Example 27

$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ has characteristic 6, which is the *lcm* of the orders of its non-zero elements:

- 1 has additive order 6;
- 2 has additive order 3;
- 3 has additive order 2;
- 4 has additive order 3;
- 5 has additive order 6.

Example 28

(1) $\mathbb{Z}_m$ has characteristic m, for any $m \geq 1$.

(2) $\mathbb{Z}$ is an integral domain of characteristic zero.

(3) $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields of characteristic zero.

Characteristic of a ring: basic properties

Theorem 29

Let $(R, +, -, 0, \cdot, e)$ be a ring with unity of characteristic $n \geq 1$. Then:

1. *n is the smallest non-zero natural number which satisfies $ne = 0$;*
2. *If $e \neq 0$ and R does not have zero divisors, then n is a prime. Moreover, all non-zero elements have the same additive order n.*

Proof.

See textbook [1], page 328. Just a few words on the second part of the second item. The additive order of a non-zero element of R cannot be 1 and divides n. As n is a prime, it must be n. $\square$

The first item above says that the characteristic n is the additive order of the unity!

Characteristic of a ring: basic properties

Corollary 30

The characteristic of an integral domain is zero or a prime number.

Proof.

From Theorem 29. □

Corollary 31

The characteristic of a finite field is a prime number.

Proof.

See textbook [1], page 328. □

Once more, when the characteristic is a prime p, all non-zero elements have the additive order p!

Characteristic of a ring: basic properties

Theorem 32

If a field has characteristic a prime p, then it contains a subfield isomorphic to the field $\mathbb{Z}_p$.

Proof.

See textbook [1], page 329. $\square$

Corollary 33

If a field has characteristic 0, then it contains a subfield isomorphic to the field $\mathbb{Q}$.

Proof.

See textbook [1], page 329. $\square$

Prime fields

A prime field is a field that does not possesses proper subfields (except for the trivial field).

Theorem 34

A field is prime if and only if it is isomorphic to $\mathbb{Z}_p$, for some prime p, or $\mathbb{Q}$.

Proof.

See textbook [1], page 329. $\square$

Show that no field can contain two distinct prime subfields!

Combining with the previous results we obtain that every field contains a prime subfield: if the field has characteristic a prime p, then the prime subfield is isomorphic to $\mathbb{Z}_p$; if the subfield has characteristic 0, its prime subfield is isomorphic to $\mathbb{Q}$.

Reading and exercise guide

Reading and exercise guide

It is highly recommended that you do all the exercises marked in red from the slides.

Course readings:

1. Pages 315-349 from textbook [1].

References

[1] Ferucio Laurențiu Țiplea. *Algebraic Foundations of Computer Science*. "Alexandru Ioan Cuza" University Publishing House, Iași, Romania, second edition, 2021.