Rings and fields I

Abdennour Kitouni, Anatoliy Malyarenko and Sergei Silvestrov

November 26, 2015

Abstract

Contents of the lecture.

- ☞ Rings and fields.
- ☞ Integral domains.
- ☞ Fermat's and Euler's theorems.

The definition of a ring

Definition 1. A **ring** R is a set with two binary operations, addition $+$ and multiplication $\cdot$, such that

1. $(R,+)$ is an abelian group.
2. Multiplication is associative, i.e., for every a, b, $c \in R$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
3. For every a, b, $c \in R$, the **left distributive law**, $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$ and the **right distributive law** $(a+b) \cdot c = (a \cdot c) + (b \cdot c)$ hold.

It is customary to use ab instead of $a \cdot b$.

This term was probably coined by D. Hilbert, in 1897, when he wrote *Zahlring*. One of the meanings of the word *ring*, in German as in English, is collection, as in the phrase "a ring of thieves."

Examples of rings

Example 1. The structure $(\mathbb{Z},+,\cdot)$ is a ring. The structure $(2\mathbb{Z},+,\cdot)$ is a ring. The structures $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, and $(\mathbb{C},+,\cdot)$ are rings. The $n \times n$ matrices over $\mathbb{Q}$ (or $\mathbb{R}$, or $\mathbb{C}$) form a ring.

Example 2. For each positive integer n the set $\mathbb{Z}_n$ of integers modulo n with addition and multiplication modulo n is a ring.

Example 3. Let A be an abelian group and let $\mathrm{Hom}(A)$ be the set of all homomorphisms $\varphi\colon A \mapsto A$. Define addition in $\mathrm{Hom}(A)$ by $(\varphi+\psi)(a) = \varphi(a)+\psi(a)$. This makes $\mathrm{Hom}(A)$ an abelian group. Let multiplication in $\mathrm{Hom}(A)$ be given by composition of functions. Then $\mathrm{Hom}(A)$ with addition and multiplication is a ring.

Elementary properties of rings

The additive identity element of a ring is called the **zero element** and denoted 0. If R is a ring, $a \in R$ and $n \in \mathbb{Z}$, then $n \cdot a$ has its usual meaning for abelian groups. For example, $n \cdot a = a+a+\cdots+a$ (n summands) when $n > 0$.

Theorem 1. *Let R be a ring. Then*

- $0 \cdot a = a \cdot 0 = 0$ *for all $a \in R$;*
- $(-a)b = a(-b) = -(ab)$ *for all a, $b \in R$;*
- $(-a)(-b) = ab$ *for all a, $b \in R$;*
- $(n \cdot a)b = a(n \cdot b) = n \cdot (ab)$ *for all $n \in \mathbb{Z}$ and all a, $b \in R$;*
- $\left(\sum_{i=1}^{n} a_j\right)\left(\sum_{j=1}^{m} b_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j$ *for all a_i, $b_j \in R$.*

Homomorphisms and isomorphisms

Definition 2. Let R and R' be rings. A function $\varphi\colon R \mapsto R'$ is a **homomorphism of rings** provided that for all a, $b \in R$,

$$\varphi(a+b) = \varphi(a)+\varphi(b) \qquad \text{and} \qquad \varphi(ab) = \varphi(a)\varphi(b).$$

When the context is clear then we shall frequently write “homomorphism" in place of “homomorphism of rings". A homomorphism of rings is, in particular, a homomorphism of the underlying abelian groups. Consequently the same terminology is used: an **isomorphism of rings** is a homomorphism of rings which is a one-to-one correspondence.

The **kernel** of a homomorphism of rings $\varphi\colon R \mapsto R'$ is its kernel as a map of abelian groups, that is, $\mathrm{Ker}(\varphi) = \varphi^{-1}(\{0\})$.

Example 4. The canonical map $\mathbb{Z} \mapsto \mathbb{Z}_m$ that maps $a \in \mathbb{Z}$ to its remainder modulo m is a homomorphism of rings.

Rings having special properties

Definition 3. If $ab = ba$ for all a, b in a ring R, then R is said to be a **commutative ring**.

Example 5. The rings $(\mathbb{Z}, +, \cdot)$, $(2\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, and $(\mathbb{C}, +, \cdot)$ are commutative. If $n \geq 2$, then the set $M_n(\mathbb{Q})$ of $n \times n$ matrices over $\mathbb{Q}$ (or the set $M_n(\mathbb{R})$, or the set $M_n(\mathbb{C})$) form a non-commutative ring.

Definition 4. If a ring R contains an element 1 such that $1a = a1 = a$ for all $a \in R$, then R is said to be a **ring with unity**.

Example 6. The rings $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $M_n(\mathbb{Q})$, $M_n(\mathbb{R})$, and $M_n(\mathbb{C})$ are rings with unity. The structure $(2\mathbb{Z}, +, \cdot)$ is a ring without unity.

Definition 5. An element a in a ring R with unity $1 \neq 0$ is said to be **invertible** or to be a **unit** in R if there exist an element $a^{-1} \in R$ such that $a^{-1}a = aa^{-1} = 1$. The element a^{-1} is called a **multiplicative inverse** of a.

The set of units in a ring R with unity $1 \neq 0$ forms a group under multiplication.

Example 7. The set of units in the ring $(\mathbb{Z}, +, \cdot)$ is the multiplicative group $\{\pm 1\}$. The set of units in the ring $(\mathbb{Q}, +, \cdot)$ (or $(\mathbb{R}, +, \cdot)$, or $(\mathbb{C}, +, \cdot)$) is the multiplicative group $\mathbb{Q}^\times$ (or $\mathbb{R}^\times$, or $\mathbb{C}^\times$). The set of units in the ring $M_n(\mathbb{Q})$ (or $M_n(\mathbb{R})$, or $M_n(\mathbb{C})$) is the multiplicative group $GL(n, \mathbb{Q})$ (or $GL(n, \mathbb{R})$, or $GL(n, \mathbb{C})$).

Definition 6. A ring D with unity $1 \neq 0$ in which every nonzero element is a unit is called a **division ring**, or **skew field**.

Definition 7. A **field** is a commutative division ring.

The derivation of the mathematical usage of the English term *field* (first used by E. H. Moore in 1893 in his article classifying the finite fields) as well as the German term *Körper* and the French term *corps* is as follows. Each word denotes a “realm" or a “collection of things". The word *domain* abbreviates the usual English translation *integral domain* of the German word *Integritätsbereich*, a collection of integers.

Example 8. The structures $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, and $(\mathbb{C}, +, \cdot)$ are both division rings and fields. The rings $M_n(\mathbb{Q})$, $M_n(\mathbb{R})$, and $M_n(\mathbb{C})$ are not division rings.

Subrings and subfields

Definition 8. Let R be a ring and S a nonempty subset of R that is closed under the operations of addition and multiplication in R. If S is itself a ring under these operations then S is called a **subring** of R. We denote this as $S \leq R$. We write $S < R$ if $S \leq R$ and $S \neq R$.

Example 9. $2\mathbb{Z} < \mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$. We also have $M_n(\mathbb{Q}) \leq M_n(\mathbb{R}) \leq M_n(\mathbb{C})$.

Definition 9. Let E be a field and F a nonempty subset of E that is closed under the operations of addition and multiplication in E. If F is itself a field under these operations then F is called a **subfield** of E. We denote this as $E \leq F$. We write $E < F$ if $E \leq F$ and $E \neq F$.

Example 10. $\mathbb{Q} < \mathbb{R} < \mathbb{C}$.

Divisors of 0 and cancellation

Definition 10. Two elements a and b of a ring R are called **divisors of 0** if $a \neq 0$, $b \neq 0$, but $ab = 0$.

Example 11. The rings $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, and $(\mathbb{C}, +, \cdot)$ do not have the divisors of 0. In the ring $\mathbb{Z}_n$, the divisors of 0 are precisely those nonzero elements that are not relatively prime to n.

Theorem 2. *A ring R has no zero divisors if and only if both the **right cancellation law***

$$ab = ac \Rightarrow b = c$$

*and the **left cancellation law***

$$ba = ca \Rightarrow b = c$$

hold in R.

Integral domains

Definition 11. A commutative ring R with unity $1 \neq 0$ and no zero divisors is called an **integral domain**.

Every field F is an integral domain since $ab = 0$ and $a \neq 0$ imply that $b = 1b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0$. The converse is not true. For example, the integral domain $\mathbb{Z}$ is not a field. However, for any prime p the integral domain $\mathbb{Z}_p$ is a field. It follows from the following result.

Theorem 3. *Every finite integral domain D is a field.*

Proof. Let 0, 1, a_1, $\ldots$, a_n be all the elements in D. For any $a \in D \setminus \{0\}$, consider the elements $a1$, aa_1, $\ldots$, aa_n. If $aa_i = aa_j$, then $a_i = a_j$ by the left cancellation law, therefore all these elements are distinct. None of these elements is 0, because D has no 0 divisors. It follows that $a1$, aa_1, $\ldots$, aa_n are elements 1, a_1, $\ldots$, a_n in some order, so that either $a1 = 1$, that is, $a = 1$, or $aa_i = 1$ for some i. Thus, a has a multiplicative inverse. □

The characteristic of a ring

Definition 12. Let R be a ring. If there is a least positive integer n such that $n \cdot a = 0$ for all $a \in R$, then R is said to have **characteristic n**. If no such n exists R is said to have **characteristic 0**.

The next theorem claims that if the ring has unity, it suffices to examine only $a = 1$.

Theorem 4. *Let R be a ring with unity and characteristic n. If $n > 0$, then n is the least positive integer such that $n \cdot 1 = 0$.*

Proof. If k is the least positive integer such that $k \cdot 1 = 0$, then for all $a \in R$: $k \cdot a = k \cdot (1a) = (k \cdot 1)a = 0a = 0$. □

Little theorem of Fermat

Theorem 5. *If $a \in \mathbb{Z}$ and p is a prime not dividing a, then p divides $a^{p-1} - 1$.*

Proof. If $(F, +, \cdot)$ is a field, then $(F \setminus \{0\}, \cdot)$ is a group. In the particular case of $F = \mathbb{Z}_p$, the elements 1, 2, $\ldots$, $p-1$ form a group of order $p-1$ under multiplication modulo p. If a is one of these elements, then $a^{p-1} = 1$ in $\mathbb{Z}_p$ by a corollary to Lagrange's theorem. Because $\mathbb{Z}_p$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ both as groups and as rings (check!), for any integer $a \notin 0 + p\mathbb{Z}$ we have $a^{p-1} \equiv 1 (\bmod p)$. □

Corollary 1. *If $a \in \mathbb{Z}$, then for any prime p, $a^p \equiv a (\bmod p)$.*

Example 12. Compute the remainder of 2^{10} when divided by 3. Using Fermat's theorem, we have

$$2^{10} = (2^2)^5 \equiv 1^5 \equiv 1 (\bmod 3).$$

Euler's theorem

Lemma 1. *The set*

$$G_n = \{\, r \in \mathbb{Z}_n \colon r \text{ and } n \text{ are relatively prime} \,\}$$

is a multiplicative group.

Definition 13. The **Euler phi-function** is

$$\varphi(n) = |G_n|.$$

Theorem 6 (Euler's theorem)**.** *If a is an integer relatively prime to m, then*

$$a^{\varphi(n)} \equiv 1 (\bmod n).$$

Proof. Since $|G_n| = \varphi(n)$, a corollary to Lagrange's theorem gives $a^{\varphi(n)} = 1$ in G_n. In congruence notation, this says the assertion of the theorem. □

Linear congruences

Theorem 7. *Let m be a positive integer, and let $a, b \in \mathbb{Z}_m$. Let d be the greatest common divisor of a and m. If d divides b then the equation $ax = b$ in $\mathbb{Z}_m$ has d solutions $x_0, x_1, \ldots, x_{d-1}$, where*

$$x_t = \left(\frac{b}{d}\right)\bar{x} + \left(\frac{n}{d}\right)t \tag{1}$$

in $\mathbb{Z}_m$ and $\bar{x}$ is the inverse to a/d in $G_{n/d}$. Otherwise there are no solutions.

Proof. Clearly if $ax = b$ then d divides b, so there are no solutions if d does not divide b.

Suppose d divides b. Since a/d and m/d are relatively prime, $\bar{x}$ exists by Lemma 1. Multiplying both sides of (1) by a, we get

$$ax_t = b\left(\frac{a}{d}\right)\bar{x} + m\left(\frac{a}{d}\right)t \tag{2}$$

in $\mathbb{Z}$. By the definition of $\bar{x}$, we have $(a/d)\bar{x} = 1 + (km/d)$ for some k, so substituting for $(a/x)\bar{x}$ in (2) yields

$$ax_t = b + km\left(\frac{b}{d}\right) + m\left(\frac{a}{d}\right)t.$$

Both fractions are integers, so it follows immediately that $ax_t = b$ in $\mathbb{Z}_m$ and hence x_t is a solution.

It remains to show that the d solutions above are distinct modulo m. But this is obvious since $x_0 < x_1 < \cdots < d_{d-1}$ and $x_{d-1} - x_0 = (m/d)(d-1) < m$. □

Example of a linear congruence

Example 13. Solve the linear congruence $91x \equiv 98 (\mathrm{mod}\, 119)$.

Solution. The greatest common divisor of 91 and 119 is 7. So there are 7 solutions modulo 119. We use cancellation to simplify the congruence to $13x \equiv 14 (\mathrm{mod}\, 17)$. We have $-4x \equiv -3 \equiv -20 (\mathrm{mod}\, 17)$. Therefore, in terms of the original modulus, the solution is

$$5 + 119\mathbb{Z}, \quad 22 + 119\mathbb{Z}, \quad 39 + 119\mathbb{Z}, \quad 56 + 119\mathbb{Z},$$

$$73 + 119\mathbb{Z}, \quad 90 + 119\mathbb{Z}, \quad 107 + 119\mathbb{Z}.$$

□