MATH 433

Applied Algebra

Lecture 24:
Ring and fields (continued).

Rings

Definition. A **ring** is a set R, together with two binary operations usually called **addition** and **multiplication** and denoted accordingly, such that

- R is an Abelian group under addition,
- R is a semigroup under multiplication,
- multiplication distributes over addition.

The complete list of axioms is as follows:
(R1) for all $x, y \in R$, $x + y$ is an element of R;
(R2) $(x + y) + z = x + (y + z)$ for all $x, y, z \in R$;
(R3) there exists an element, denoted 0, in R such that $x + 0 = 0 + x = x$ for all $x \in R$;
(R4) for every $x \in R$ there exists an element, denoted $-x$, in R such that $x + (-x) = (-x) + x = 0$;
(R5) $x + y = y + x$ for all $x, y \in R$;
(R6) for all $x, y \in R$, xy is an element of R;
(R7) $(xy)z = x(yz)$ for all $x, y, z \in R$;
(R8) $x(y+z) = xy+xz$ and $(y+z)x = yx+zx$ for all $x, y, z \in R$.

Examples of rings

Informally, a ring is a set with three arithmetic operations: addition, subtraction and multiplication. Subtraction is defined by $x - y = x + (-y)$.

- Real numbers $\mathbb{R}$.
- Integers $\mathbb{Z}$.
- $2\mathbb{Z}$: even integers.
- $\mathbb{Z}_n$: congruence classes modulo n.
- $\mathcal{M}_n(\mathbb{R})$: all $n \times n$ matrices with real entries.
- $\mathcal{M}_n(\mathbb{Z})$: all $n \times n$ matrices with integer entries.
- All functions $f : S \to \mathbb{R}$ on a nonempty set S.
- **Zero ring**: any additive Abelian group with trivial multiplication: $xy = 0$ for all x and y.
- Trivial ring $\{0\}$.

Examples of rings

In examples below, real numbers $\mathbb{R}$ can be replaced by a more general ring of coefficients.

• $\mathbb{R}[X]$: polynomials in variable X with real coefficients.
$p(X) = c_0 + c_1 X + c_2 X^2 + \cdots + c_n X^n$, where each $c_i \in \mathbb{R}$.

• $\mathbb{R}(X)$: rational functions in variable X with real coefficients.
$r(X) = \frac{a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n}{b_0 + b_1 X + b_2 X^2 + \cdots + b_m X^m}$, where $a_i, b_j \in \mathbb{R}$ and $b_m \neq 0$.

• $\mathbb{R}[X, Y]$: polynomials in variables X, Y with real coefficients.
$\mathbb{R}[X, Y] = \mathbb{R}[X][Y]$.

• $\mathbb{R}[[X]]$: formal power series in variable X with real coefficients.
$p(X) = c_0 + c_1 X + c_2 X^2 + \cdots + c_n X^n + \ldots$, where $c_i \in \mathbb{R}$.
Multiplication is well defined. For example,

$$(1 - X)(1 + X + X^2 + X^3 + X^4 + \ldots) = 1.$$

From rings to fields

A ring R is called a **domain** if it has no zero-divisors, that is, $xy = 0$ implies $x = 0$ or $y = 0$.

A ring R is called a **ring with identity** if there exists an identity element for multiplication (denoted 1).

A **division ring** is a nontrivial ring with identity in which every nonzero element has a multiplicative inverse.

A ring R is called **commutative** if the multiplication is commutative.

An **integral domain** is a nontrivial commutative ring with identity and no zero-divisors.

A **field** is an integral domain in which every nonzero element has a multiplicative inverse (equivalently, a commutative division ring).

$$\begin{aligned} \text{rings} \supset \text{domains} &\supset \text{integral domains} \supset \text{fields} \\ &\supset \text{division rings} \supset \end{aligned}$$

Fields

Definition. A **field** is a set F, together with two binary operations called **addition** and **multiplication** and denoted accordingly, such that

- F is an Abelian group under addition,
- $F \setminus \{0\}$ is an Abelian group under multiplication,
- multiplication distributes over addition.

In other words, the field is a commutative ring with identity ($1 \neq 0$) such that any nonzero element has a multiplicative inverse.

Examples. • Real numbers $\mathbb{R}$.

- Rational numbers $\mathbb{Q}$.
- Complex numbers $\mathbb{C}$.
- $\mathbb{Z}_p$: congruence classes modulo p, where p is prime.
- $\mathbb{R}(X)$: rational functions in variable X with real coefficients.

Basic properties of fields

- The zero 0 and the unity 1 are unique.
- For any $a \in F$, the negative $-a$ is unique.
- For any $a \neq 0$, the inverse a^{-1} is unique.
- $-(-a) = a$ for all $a \in F$.
- $0 \cdot a = 0$ for all $a \in F$.
- $ab = 0$ implies that $a = 0$ or $b = 0$.
- $(-1) \cdot a = -a$ for all $a \in F$.
- $(-1) \cdot (-1) = 1$.
- $(-a)b = a(-b) = -ab$ for all $a, b \in F$.
- $(a - b)c = ac - bc$ for all $a, b, c \in F$.

Characteristic of a field

A field F is said to be of nonzero characteristic if $\underbrace{1+1+\cdots+1}_{n \text{ summands}} = 0$ for some positive integer n.

The smallest integer with this property is called the **characteristic** of F. Otherwise the field F has characteristic 0.

The fields $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ have characteristic 0.
The field $\mathbb{Z}_p$ (p prime) has characteristic p.
In general, any finite field has nonzero characteristic.
Any nonzero characteristic is prime since

$$(\underbrace{1+\cdots+1}_{n \text{ summands}})(\underbrace{1+\cdots+1}_{m \text{ summands}}) = \underbrace{1+\cdots+1}_{nm \text{ summands}}.$$

Problem. Let $F = \{0, 1, a, b\}$ be a field consisting of 4 elements, where 0 denotes the additive identity element, 1 denotes the multiplicative identity element, and a, b denote the remaining two elements. Fill in the addition and multiplication tables for the field F.

Solution:

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\times$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Problem. Let $F = \{0, 1, a, b\}$ be a field consisting of 4 elements, where 0 denotes the additive identity element, 1 denotes the multiplicative identity element, and a, b denote the remaining two elements. Fill in the addition and multiplication tables for the field F.

Remarks on solution. First we fill in the multiplication table. Since $0x = 0$ and $1x = x$ for every $x \in F$, it remains to determine only a^2, b^2, and $ab = ba$. Using the fact that $\{1, a, b\}$ is a multiplicative group, we obtain that $ab = 1$, $a^2 = b$, and $b^2 = a$.

As for the addition table, we have $x + 0 = x$ for every $x \in F$. Next step is to determine $1 + 1$. Assuming $1 + 1 = a$, we obtain $a + 1 = b$ and $b + 1 = 0$. This is a contradiction: the characteristic of F turns out to be 4, not a prime! Hence $1 + 1 \neq a$. Similarly, $1 + 1 \neq b$. By deduction, $1 + 1 = 0$. Then $x + x = 1x + 1x = (1 + 1)x = 0x = 0$ for all $x \in F$. The rest is filled in using the cancellation ("sudoku") rules.