MATH 415
Modern Algebra I

Lecture 21:
Rings and fields.

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:

(A0) for all $x, y \in R$, $x + y$ is an element of R;
(A1) $(x + y) + z = x + (y + z)$ for all $x, y, z \in R$;
(A2) there exists an element, denoted 0, in R such that $x + 0 = 0 + x = x$ for all $x \in R$;
(A3) for every $x \in R$ there exists an element, denoted $-x$, in R such that $x + (-x) = (-x) + x = 0$;
(A4) $x + y = y + x$ for all $x, y \in R$;
(M0) for all $x, y \in R$, xy is an element of R;
(M1) $(xy)z = x(yz)$ for all $x, y, z \in R$;
(D) $x(y+z) = xy+xz$ and $(y+z)x = yx+zx$ for all $x, y, z \in R$.

From rings to fields

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

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

A **division ring** (or **skew field**) is a nontrivial ring with unity 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 unity and no divisors of zero.

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

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

Rings with unity

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

Lemma If $1 = 0$ then R is the trivial ring, $R = \{0\}$.

Proof. Let $x \in R$. Then $x1 = x$ and $x0 = 0$. Hence $x = 0$.

Suppose R is a non-trivial ring with unity. An element $x \in R$ is called **invertible** (or a **unit**) if it has a multiplicative inverse x^{-1}, i.e., $xx^{-1} = x^{-1}x = 1$. The set of all invertible elements of the ring R is denoted $R^\times$ or R^*.

Proposition 1 $R^\times$ is a group under multiplication.

Sketch of the proof. The unity is invertible: $1^{-1} = 1$. If x is invertible then x^{-1} is also invertible: $(x^{-1})^{-1} = x$. If x and y are invertible then so is xy: $(xy)^{-1} = y^{-1}x^{-1}$.

Proposition 2 Invertible elements cannot be divisors of zero.

Proof. Let $a \in R^\times$ and $x \in R$. Then $ax = 0 \implies a^{-1}(ax) = a^{-1}0 \implies (a^{-1}a)x = a^{-1}0 \implies x = 0$. Similarly, $xa = 0 \implies x = 0$.

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 unity ($1 \neq 0$) 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.

$+$	0	1	a	b
0				
1				
a				
b				

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

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.

$+$	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") laws.