MATH 433

Applied Algebra

Lecture 25:
Rings and fields (continued).
Vector spaces over a field.

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 $x, y, z \in R$.

Basic properties of rings

Let R be a ring.

- The zero $0 \in R$ is unique.
- For any $x \in R$, the negative $-x$ is unique.
- $-(-x) = x$ for all $x \in R$.
- $x0 = 0x = 0$ for all $x \in R$.
- $(-x)y = x(-y) = -xy$ for all $x, y \in R$.
- $(-x)(-y) = xy$ for all $x, y \in R$.
- $x(y - z) = xy - xz$ for all $x, y, z \in R$.
- $(y - z)x = yx - zx$ for all $x, y, z \in R$.

Unity and units

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, $xa = 0 \implies x = 0$.

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).

rings $\supset$ domains $\supset$ integral domains $\supset$ fields
$\supset$ division rings $\supset$

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

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

Vector spaces over a field

Definition. Given a field F, a **vector space** V over F is an additive abelian group endowed with a mixed operation $\phi : F \times V \to V$ called **scalar multiplication** or **scaling**.

Elements of V and F are referred to respectively as **vectors** and **scalars**. The scalar multiple $\phi(\lambda, v)$ is denoted λv.

The scalar multiplication is to satisfy the following axioms:

(V1) for all $v \in V$ and $\lambda \in F$, λv is an element of V;
(V2) $\lambda(v + w) = \lambda v + \lambda w$ for all $v, w \in V$ and $\lambda \in F$;
(V3) $(\lambda + \mu)v = \lambda v + \mu v$ for all $v \in V$ and $\lambda, \mu \in F$;
(V4) $\lambda(\mu v) = (\lambda\mu)v$ for all $v \in V$ and $\lambda, \mu \in F$;
(V5) $1v = v$ for all $v \in V$.

(Almost) all linear algebra developed for vector spaces over $\mathbb{R}$ can be generalized to vector spaces over an arbitrary field F. This includes: linear independence, span, basis, dimension, determinants, matrices, eigenvalues and eigenvectors.

Examples of vector spaces over a field F:

- The space F^n of n-dimensional coordinate vectors $(x_1, x_2, \ldots, x_n)$ with coordinates in F.
- The space $\mathcal{M}_{n,m}(F)$ of $n \times m$ matrices with entries in F.
- The space $F[X]$ of polynomials $p(X) = a_0 + a_1 X + \cdots + a_n X^n$ in variable X with coefficients in F.
- Any field F' that is an extension of F (i.e., $F \subset F'$ and the operations on F are restrictions of the corresponding operations on F'). In particular, $\mathbb{C}$ is a vector space over $\mathbb{R}$ and over $\mathbb{Q}$, $\mathbb{R}$ is a vector space over $\mathbb{Q}$.

Finite fields

Theorem 1 Any finite field F has nonzero characteristic.

Proof: Consider a sequence $1, 1+1, 1+1+1, \ldots$ Since F is finite, there are repetitions in this sequence. Clearly, the difference of any two elements is another element of the sequence. Hence the sequence contains 0 so that the characteristic of F is nonzero.

Theorem 2 The number of elements in a finite field F is p^k, where p is a prime number.

Sketch of the proof: Let p be the characteristic of F. By the above, $p > 0$. Therefore p is a prime number. Let F' be the set of all elements $1, 1+1, 1+1+1, \ldots$ Clearly, F' consists of p elements. One can show that F' is a subfield (canonically identified with $\mathbb{Z}_p$). It follows that F has p^k elements, where $k = \dim F$ as a vector space over F'.