# MATH 415

## Modern Algebra I

**Lecture 15:**
**Fields (continued).**
**Advanced algebraic structures.**

# 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).

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

# 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.

# 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 $F$.

| $+$ | $0$ | $1$ | $a$ | $b$ |
|---|---|---|---|---|
| $0$ | $0$ | $1$ | $a$ | $b$ |
| $1$ | $1$ | $0$ | $b$ | $a$ |
| $a$ | $a$ | $b$ | $0$ | $1$ |
| $b$ | $b$ | $a$ | $1$ | $0$ |

| $\times$ | $0$ | $1$ | $a$ | $b$ |
|---|---|---|---|---|
| $0$ | $0$ | $0$ | $0$ | $0$ |
| $1$ | $0$ | $1$ | $a$ | $b$ |
| $a$ | $0$ | $a$ | $b$ | $1$ |
| $b$ | $0$ | $b$ | $1$ | $a$ |

**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 $1 + 1$. By Lagrange's Theorem, the order of 1 in the additive group $F$ is a divisor of 4. Since that order equals the characteristic of the field $F$, it is a prime number. Hence the order is 2 so that $1 + 1 = 0$. 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.

# 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 $\lambda v$.

The scalar multiplication is to satisfy the following axioms:

**(V0)** for all $v \in V$ and $\lambda \in F$, $\lambda v$ is an element of $V$;
**(V1)** $\lambda(v + w) = \lambda v + \lambda w$ for all $v, w \in V$ and $\lambda \in F$;
**(V2)** $(\lambda + \mu)v = \lambda v + \mu v$ for all $v \in V$ and $\lambda, \mu \in F$;
**(V3)** $\lambda(\mu v) = (\lambda\mu)v$ for all $v \in V$ and $\lambda, \mu \in F$;
**(V4)** $1v = v$ 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 $p(x) = a_0 + a_1 X + \cdots + a_n X^n$ 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 $\mathbb{Q}$.

*Counterexample.* • Consider the abelian group $V = \mathbb{Z}$ with the following scalar multiplication over the field $F = \mathbb{Q}$ ("selective scaling"):

$$\lambda \odot v = \begin{cases} \lambda v & \text{if } \lambda v \in \mathbb{Z}, \\ v & \text{otherwise} \end{cases} \quad \text{for any } v \in \mathbb{Z} \text{ and } \lambda \in \mathbb{Q}.$$

The group $(\mathbb{Z}, +)$ with the scalar multiplication $\odot$ is not a vector space over $\mathbb{Q}$. One reason is that the distributive law $(\lambda + \mu) \odot v = \lambda \odot v + \mu \odot v$ does not hold.
For example, let $\lambda = \mu = 1/2$ and $v = 1$. Then $(\frac{1}{2} + \frac{1}{2}) \odot v = 1 \odot v = v = 1$ while $\frac{1}{2} \odot v + \frac{1}{2} \odot v = v + v = 2$.

*Remark.* The essential information about the scalar multiplication $\odot$ used in the above counterexample is that $1 \odot v = v$ and $\frac{1}{2} \odot v$ is an integer. It follows that the additive group $\mathbb{Z}$, in principle, cannot be made into a vector space over $\mathbb{Q}$.

# Linear independence over $\mathbb{Q}$

Since the set $\mathbb{R}$ of real numbers and the set $\mathbb{Q}$ of rational numbers are fields, we can regard $\mathbb{R}$ as a vector space over $\mathbb{Q}$. Real numbers $r_1, r_2, \ldots, r_n$ are said to be **linearly independent over** $\mathbb{Q}$ if they are linearly independent as vectors in that vector space.

*Example.* 1 and $\sqrt{2}$ are linearly independent over $\mathbb{Q}$.

Assume $a \cdot 1 + b\sqrt{2} = 0$ for some $a, b \in \mathbb{Q}$. We have to show that $a = b = 0$.

Indeed, $b = 0$ as otherwise $\sqrt{2} = -a/b$, a rational number. Then $a = 0$ as well.

In general, two nonzero real numbers $r_1$ and $r_2$ are linearly independent over $\mathbb{Q}$ if $r_1/r_2$ is irrational.

# Linear independence over $\mathbb{Q}$

*Example.* $1$, $\sqrt{2}$, and $\sqrt{3}$ are linearly independent over $\mathbb{Q}$.

Assume $a + b\sqrt{2} + c\sqrt{3} = 0$ for some $a, b, c \in \mathbb{Q}$.
We have to show that $a = b = c = 0$.

$$a + b\sqrt{2} + c\sqrt{3} = 0 \implies a + b\sqrt{2} = -c\sqrt{3}$$
$$\implies (a + b\sqrt{2})^2 = (-c\sqrt{3})^2$$
$$\implies (a^2 + 2b^2 - 3c^2) + 2ab\sqrt{2} = 0.$$

Since 1 and $\sqrt{2}$ are linearly independent over $\mathbb{Q}$, we obtain $a^2 + 2b^2 - 3c^2 = 2ab = 0$. In particular, $a = 0$ or $b = 0$.

Then $a + c\sqrt{3} = 0$ or $b\sqrt{2} + c\sqrt{3} = 0$. However 1 and $\sqrt{3}$ are linearly independent over $\mathbb{Q}$ as well as $\sqrt{2}$ and $\sqrt{3}$. Thus $a = b = c = 0$.

# Finite fields

**Theorem 1** Any finite field $F$ has nonzero characteristic.

*Proof:* Consider a sequence $1, 1+1, 1+1+1, \dots$ 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 $1, 1+1, 1+1+1, \dots$ 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 $F'$.

# Algebra over a field

*Definition.* An **algebra** $A$ over a field $F$ (or $F$-**algebra**) is a vector space over $F$ with a multiplication which is a bilinear operation on $A$. That is, the product $xy$ is both a linear function of $x$ and a linear function of $y$.

To be precise, the following axioms are to be satisfied:

**(A0)** for all $x, y \in A$, the product $xy$ is an element of $A$;
**(A1)** $x(y+z) = xy + xz$ and $(y+z)x = yx + zx$ for $x, y, z \in A$;
**(A2)** $(\lambda x)y = \lambda(xy) = x(\lambda y)$ for all $x, y \in A$ and $\lambda \in F$.

An $F$-algebra is **associative** if the multiplication is associative. An associative algebra is both a vector space and a ring.

An $F$-algebra $A$ is a **Lie algebra** if the multiplication (usually denoted $[x, y]$ and called **Lie bracket** in this case) satisfies:

**(Antisymmetry)**: $[x, y] = -[y, x]$ for all $x, y \in A$;
**(Jacobi's identity)**: $[[x, y], z] + [[y, z], x] + [[z, x], y] = 0$ for all $x, y, z \in A$.

*Examples of associative algebras:*

- The space $\mathcal{M}_n(F)$ of $n \times n$ matrices with entries in $F$.
- The space $F[X]$ of polynomials $p(x) = a_0 + a_1 X + \cdots + a_n X^n$ with coefficients in $F$.
- The space of all functions $f : S \to F$ on a set $S$ taking values in a field $F$.
- Any field $F'$ that is an extension of a field $F$ is an associative algebra over $F$.

*Examples of Lie algebras:*

- $\mathbb{R}^3$ with the cross product is a Lie algebra over $\mathbb{R}$.
- Any associative algebra $A$ with a Lie bracket (called the **commutator**) defined by $[x, y] = xy - yx$.

# Complex numbers as an $\mathbb{R}$-algebra

Complex numbers can be defined as a certain 2-dimensional algebra over the field $\mathbb{R}$. We have a distinguished basis $\mathbf{1}, i$. Hence every complex number $z$ is uniquely represented as $z = x\mathbf{1} + yi$, where $x, y \in \mathbb{R}$.

Since multiplication is a bilinear function, it is enough to define $z_1 \cdot z_2$ in the case $z_1, z_2 \in \{\mathbf{1}, i\}$. We set $\mathbf{1} \cdot \mathbf{1} = \mathbf{1}$, $\mathbf{1} \cdot i = i \cdot \mathbf{1} = i$ and $i \cdot i = -\mathbf{1}$.

Because of bilinearity of the product, it is easy to check that $\mathbf{1} \cdot z = z \cdot \mathbf{1}$, $z_1 \cdot z_2 = z_2 \cdot z_1$ and $(z_1 \cdot z_2) \cdot z_3 = z_1 \cdot (z_2 \cdot z_3)$.