# 115A/4, Winter 2023

## Linear Algebra

Lecture 3

Fr Jan 13

3.1 Definition A field $F$ is a set on which one has two operations $+$, $\cdot$, called addition and multiplication, are defined so that for each $x, y \in F$ corresponds a unique element in $F$ denoted $x+y$ ($x$ plus $y$) and a unique element denoted $x \cdot y$ ($x$ times $y$) such that the following properties are satisfied, for all elements $a, b, c \in F$:

(F1) $a+b = b+a$ ; $a \cdot b = b \cdot a$

(commutativity of addition and multipl.)

(F2) $(a+b)+c = a+(b+c)$ ; $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(associativity of addition & multiplication)

(F3) There exist distinct elements $0$ and $1$ in $F$ such that $0+a = a$ and $1 \cdot a = a$, $\forall a \in F$

(existence of identity elements for $+$ and $\cdot$)

(F4) For each $a \in F$ and each $b \in F$, $b \neq 0$ there exist elements $c \in F$, $d \in F$ such that

$a+c = 0$, $b \cdot d = 1$

(existence of inverse for addition & multipl.)

(F5) $a \cdot (b+c) = a \cdot b + a \cdot c$;
(distributivity of multiplication over addition)

The element $x+y$ called the sum of $x$ & $y$
$x \cdot y$ called the product of $x$ & $y$

The element $0$ (which reads "zero")
is called the identity element for addition
The element $1$ (reads "one")
called the identity element for multiplication

The element $c$ in (F4) with property $a+c=0$ called the additive inverse of $a$
The element $d$ in (F4) with property $a \cdot d = 1$ called the multiplicative inverse of $c$

3.2. Examples: (1) The set $\mathbb{R}$ of all real numbers with the usual $+, \cdot$ is a field
(2) The set $\mathbb{Q}$ of rational numbers with usual $+, \cdot$ is a field

Indeed, because the sum, product and inverses of rational numbers are rational numbers

(3) The set $\mathbb{Z}$ of integers with the usual $+$, $\cdot$ operations is not a field: properties (F1), (F2), (F3), (F5) are satisfied and also existence of additive inverse in (F4) but not the existence of multiplicative inverse: for instance $2 \in \mathbb{Z}$ doesn't have any $d \in \mathbb{Z}$ such that $2 \cdot d = 1$

(4) Denote by $\mathbb{Z}_2$ the set with two elements 0 and 1 on which we define the operations $+$ and $\cdot$ as follows:

$$0+0=0, \quad 0+1=1, \quad 1+0=1, \quad 1+1=0$$

$$0 \cdot 0 = 0, \quad 0 \cdot 1 = 0, \quad 1 \cdot 0 = 0, \quad 1 \cdot 1 = 1$$

Then one clearly has (F1)–(F5) satisfied! So $(\mathbb{Z}_2, +, \cdot)$ is a field. It is called the field with two elements

Note: • The additive inverse of 1 is 1 itself, because $1+1=0$.

• One can show that $\mathbb{Z}_2$ is the unique field with two elements (exercise!)

**3.3 Exercise** Let $\mathbb{Q}(\sqrt{2}) \stackrel{\text{def}}{=} \{x \in \mathbb{R} : x = a+b\sqrt{2}$ with $a,b \in \mathbb{Q}\}$

Show that $\mathbb{Q}(\sqrt{2})$ with the operations of addition and multiplication as real numbers ("inherited" from $\mathbb{R}$) is a field.

Proof: First of all, note that if $x = a+b\sqrt{2}$, $y = c+d\sqrt{2}$ with $a,b,c,d \in \mathbb{Q}$ then $x+y = (a+c)+(b+d)\sqrt{2}$ and $x \cdot y = (ac+2bd)+(ad+bc)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. Also, if $x,y,z \in \mathbb{Q}(\sqrt{2})$ then when we view them as real numbers we have (F1), (F2), (F5) satisfied (commutativity of $+$ & $\cdot$, associativity of $+$, and distributivity of multiplication over addition)

Also, since $0 = 0+0\cdot\sqrt{2}$ and $1 = 1+0\cdot\sqrt{2}$ we have $0, 1 \in \mathbb{Q}(\sqrt{2})$. Since $0,1$ satisfy (F3) for the real numbers, they satisfy it also for $\mathbb{Q}(\sqrt{2})$.

Finally, we have to check (F4), i.e. existence of additive and multiplicative inverse in $\mathbb{Q}(\sqrt{2})$. For addition,

If $x = a + b\sqrt{2}$ with $a, b \in \mathbb{Q}$

then $y = -a + (-b)\sqrt{2}$ is in $\mathbb{Q}$

and we have indeed $x + y = 0$.

So there exists indeed additive inverse for any $x \in \mathbb{Q}(\sqrt{2})$

If $x = a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, $x \neq 0$ means that $a \neq 0$ or $b \neq 0$

We try to find the inverse of $x$ as an element in $\mathbb{Q}(\sqrt{2})$:

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a - 2b^2}$$

($a - b\sqrt{2}$)

$$= \frac{a}{a - 2b^2} + \left(-\frac{b}{a - 2b^2}\right)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$$

because

$$\frac{a}{a - 2b^2}, \frac{-b}{a - 2b^2} \in \mathbb{Q}$$

3.4 Theorem (Cancellation laws in a field)

Let $(F, +, \cdot)$ be a field. For any $a, b, c \in F$ we have:

(1) If $a + b = c + b$ then $a = c$

(2) If $a \cdot b = c \cdot b$ and $b \neq 0$, then $a = c$

Proof (1). By (F4) there exists $d \in F$ such that $b + d = 0$.

Since $a + b = c + b$, we can add to both sides the element $d$ to obtain:

$$(a + b) + d = (c + b) + d$$

by (F2): $a + (b + d) = c + (b + d)$

$b + d = 0$ and $b + d = 0$

so $a + 0 = c + 0$

$a + 0 = a$ and $c + 0 = c$

Thus $a = c$.

(2) has similar proof (exercise)

3.5 Theorem The element 0 and 1 (identity for addition and multip.) in a field are unique. Also, the additive inverse of an element and

The multiplicative inverse of a $\neq 0$ element are unique.

**Proof** If $0' \in F$ is another element with the property that $0' + a = a$, $\forall\, a \in F$, then we have $0' + 0 = 0$. Since $+$ is commutative, $0 + 0' = 0' + 0$ and since $0$ is identity for addition we also have

$0 + 0' = 0'$ Thus $0' = 0$

similarly for multiplication:

If $1' \in F$ satisfies

$1' \cdot a = a \quad \forall\, a \in F$ then

$1' \cdot 1 = 1$

$= 1 \cdot 1' = 1'$ (by (F1))

& multiplic.

For uniqueness of additive inverse- we cancellation Thm. (exercise)

3.6. Theorem If $(F, +, \cdot)$ is a field Then we have:

(1) $a \cdot 0 = 0 \cdot a = 0$, $\forall a \in F$

(2) $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$ $\forall a, b \in F$

(3) $(-a) \cdot (-b) = a \cdot b$

Proof. (1) We have

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$$

so by cancellation Theorem

$a \cdot 0 = 0$. Same how $0 \cdot a = 0$

(2) Showing that $(-a) \cdot b = -(a \cdot b)$ amounts to showing that $(-a) \cdot b$ is the additive inverse of $a \cdot b$ (because of uniqueness of additive inverse in Thm 3.5).

We have

$$(-a) \cdot b + a \cdot b \overset{\text{by (F5)}}{=} (-a + a) \cdot b$$

$$= 0 \cdot b \overset{\text{by Thm 3.5}}{=} 0$$

Same for $a \cdot (-b) + ab = 0$ (exercise)

(3) Note first that by (2) above we have $(-1)\cdot a = -a = a\cdot(-1)$

Thus, by using (F1) (associativity of multipl.) we have

$$(-a)\cdot(-b) = ((-1)\cdot a)(-b)$$

$$= (a\cdot(-1))(-b) = a\cdot((-1)\cdot(-b))$$

(F1) ↑ ↑ (F2)

$(-1)\cdot(-b) = b$

$= a\cdot b$

where we have used $(-1)\cdot(-b) = b$ which in turn follows from the fact that

$(-1)\cdot(-1) = 1$

↳ indeed, this is true because

$(1+(-1))(-1) = 0\cdot(-1) = 0$

$1+(-1) = 0$

but also $= \underbrace{1\cdot(-1)}_{=-1} + (-1)\cdot(-1)$

so $0 = -1 + (-1)\cdot(-1)$ and adding 1 to both sides

get $(-1)\cdot(-1) = 1$

---

Conclusion from now on, we can

Just write in a field $(F, +, \cdot)$

$-a$ for the additive inverse of $a \in F$

(and similarly $-ab$, etc)

$\frac{1}{a}$ or $a^{-1}$ for multiplicative inverse of $a \neq 0$

$\frac{1}{-a}$ or $(-a)^{-1}$ or $-a^{-1}$

$(-a)(-b) = ab$

$a^n$ for $a \cdot a \cdot \cdots \cdot a$

$a^{-n}$ for $\frac{1}{a^n}$, or $(a^{-1})^n$ etc

# Vector spaces

**Definition.** A vector space (or linear space) $V$ over a field $F$ consists of a set $V$ on which two operations (called addition and scalar multiplication) are defined, so that for each

$x, y \in V$ we have a unique element $x + y$ in $V$ ($x$ plus $y$)

addition

and for each $x \in V$ and $a \in F$ we have a unique element $ax \in V$

scalar mult.

such that the following conditions hold:

(VS1) $x + y = y + x$, $\forall\, x, y \in V$ (commutativity of addition)

(VS2) $(x+y)+z = x+(y+z)$, $\forall\, x, y, z \in V$

(associativity of addition)

(VS3) There exists an element in $V$ denoted $0$ such that $x + 0 = x$, $\forall\, x \in V$

(The "zero element" or neutral element in $V$)

(VS4) For each $x \in V$ there exists $y \in V$ such that $x + y = 0$ (the "opposite of $x$")

(VS5) For each $x \in V$ we have $1x = x$

(VS6) For each $x \in V$, $a, b \in F$ we have $(ab)x = a(bx)$

(VS7) For each $x, y \in V$, $a \in F$ we have $a(x+y) = ax + ay$

(VS8) For each $x \in V$, $a, b \in F$ we have $(a+b)x = ax + bx$