

Math115A 1/12 notes

Vincent

2023-01-13

3.1 Definition

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

(F1) $a + b = b + a$, $a * b = b * a$

(F2) $(a + b) + c = a + (b + c)$; $(ab)c = a(bc)$

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

(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 $a + c = 0$, $bd = 1$

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

The element 0 is called the identity element for addition

The element 1 called the identity element for multiplication

The element c in (F4) with property $a + c = 0$ called the addition inverse of a .

The element d in (F4) with property $a*d = 1$ called the multiplication inverse of c

Examples:

1. The set R of all real numbers with the usual $+$, $*$ is a field.

2. The set Q of rational numbers with usual $+$, $*$ is a field

indeed, because the sum, product and inverses of rational numbers are rational numbers.

3. The set Z of integers with the usual $+$, $*$ 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 $z \in Z$ such that $2*d = 1$

4. Denote by Z_2 the set with two elements 0 and 1 on which we define the operations $+$ and $*$ as follows:

$0+0=0, 0+1=1, 1+0=1, 1+1=0, 0*0=0, 0*1=0, 1*0=0, 1*1=1$

Then one clearly has (F1) – (F5) satisfied! So $(Z_2, +, *)$ 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 Z_2 is the unique field with two elements.

3.4 Theorem (cancellation law in a field)

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

(1) if $a+b=c+b$ Then $a=c$

(2) if $ab=cb$ 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 to obtain:

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

So by (F2) $a+(b+d) = c+(b+d)$ so $a+0 = c+0$ Thus $a=c$.
 (2) has similar proof

3.5 Theorem:

The element 0 and 1 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 $1' * a = a \forall a \in F$ then $1' 1 = 1$

For uniqueness of addition and multiply inverse use cancellation thus.

3.6 Theorem

If $(F, +, \cdot)$ is a field then we have:

$$(1) a0 = 0a = 0, \forall a \in F$$

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

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

Proof:

(1) we have $a0 = a(0+0) = a0 + a0$. So by cancellation theorem, $a0 = 0$. Same for $0a = 0$

(2) Showing that $(-a)b = -(ab)$ amount to showing that $(-a)b$ is the additive inverse of ab (because of uniqueness of additive inverse in Theorem 3.5).

we have $(-a)b + ab = (-a+a)b = 0b = 0$

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

(3) Note that by (2) above we have $(-1)a = -a = a(-1)$. Thus, by using (F1) we have $(-a)(-b) = ((-1)a)(-b) = a((-1)(-b))$. Where we have used $(-1)(-b) = b$ which in turn follows from the fact that $(-1)(-1) = 1$.

Conclusion from now on, we can just write in a field $(F, +, \cdot)$ $-a$ for the additive inverse of $a \in F$

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

Vector Space

Definition: A vector 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 and for each $x \in V$ and $a \in F$ we have a unique element $ax \in V$ (scalar) such that the following conditions hold:

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

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

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

$$(VS4) \text{ For each } x \in V \text{ there exists } y \in V \text{ such that } x+y=0$$

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

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

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

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