Monday, September 23, 2024 3:48 PM

Fields

A field K is a set "K" together with two operations:

$$+: K\times K \to K \quad \text{and} \quad \cdot : K\times K \to K$$

satisfying:

Given $x, y \in K$ we have: (Field Axioms)

1. $(x+y)+z = x+(y+z)$
2. $x+y = y+x$
3. There is an element $0 \in K$ such that $x+0 = x \quad \forall x \in K$
4. For any $x \in K$, there is an element $y \in K$ such that $x+y=0$. We define $-x := y$ and we write $z-x$ instead of $z+(-x)$.
5. $(x\cdot y)z = x\cdot(y\cdot z)$
6. $x\cdot y = y\cdot x$
7. There is an element $1 \in K$ such that: $1\cdot x = x \quad \forall x \in K$
8. For every $x \neq 0$, $\exists x^{-1} \in K$ such that $x\cdot x^{-1} = 1$

   we write $\frac{x}{y}$ instead of $x\cdot y^{-1}$.
9. $x\cdot(y+z) = xy + xz$

Given K, L fields.

$f: K \to L$ is a homomorphism

$$f(x+y) = f(x)+f(y)$$
$$f(xy) = f(x)\cdot f(y)$$

If $f: K\to L$ has an inverse $f^{-1}: L \to K$ which is also a homomorphism, we say $f: K \to L$ is an isomorphism.

An automorphism is an isomorphism with equal domain and codomain. i.e. $f: K \xrightarrow{\sim} K$

Ex: (The Rational numbers):

$$\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$$

$$\frac{a}{b}+\frac{c}{d} = \frac{a\cdot d + b\cdot c}{bd} \qquad \frac{a}{b}\cdot\frac{c}{d} = \frac{a\cdot c}{b\cdot d}$$

$$\frac{a}{b} + \boxed{\frac{0}{1}} = \frac{a}{b} \qquad \frac{a}{b}\cdot\boxed{\frac{1}{1}} = \frac{a}{b}$$

"0" $\frac{0}{1}$ "1" $\frac{1}{1}$ $\quad \frac{a}{b} \xrightarrow{+} -\frac{a}{b}$

$$\frac{a}{b}\times\frac{b}{a} = \boxed{\frac{1}{1}} \qquad \frac{a}{b} \xrightarrow{\cdot} \frac{b}{a}$$

Ex: $\mathbb{Z}_p = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \dots, \overline{p-1}\}$ $\quad \mathbb{Z} = \bigcup_{k\in\mathbb{Z}} \bar{k}$

$$\bar{k} = \{k + n\cdot p \ ; \ n \in \mathbb{Z}\}$$

$\bar{k} + \bar{\ell} = \overline{k+\ell}$ $\quad \bar{k} \neq \bar{\ell} \quad \bar{k} \cap \bar{\ell} = \emptyset$

$\bar{k}\cdot\bar{\ell} = \overline{k\cdot\ell}$ $\quad a^{p-1} \equiv 1 \pmod p$ Fermat's little theorem

p is prime

$$\bar{a}\cdot\bar{a}^{p-2} = \bar{1}$$

Ex: Rational functions

polynomial with rational coef.

$$\mathbb{Q}(t) = \left\{\frac{p(t)}{q(t)} \ ; \ p(t), q(t) \in \mathbb{Q}[t], \ q(t) \neq 0\right\}$$

$$t, \ \frac{t-1}{t+1}, \ \frac{t^2-2t+3}{t-1}, \ \frac{t^3+t^2+1}{t^5-t^4+2} \in \mathbb{Q}(t)$$

$$\frac{p(t)}{q(t)} + \frac{r(t)}{s(t)} = \frac{p(t)s(t) + q(t)r(t)}{q(t)s(t)}$$

$$\frac{p(t)}{q(t)}\cdot\frac{r(t)}{s(t)} = \frac{p(t)r(t)}{q(t)s(t)}$$

Proposition: $x, y \in K$

a. $x\cdot 0 = 0$

b. $x\cdot z = y\cdot z$ and $z \neq 0$ then $x = y$ (Cancellation Law)

c. $x\cdot y = 0 \Rightarrow x = 0$ or $y = 0$

d. $x^2 = y^2 \Rightarrow x = \pm y$

Proof: a. $x + x\cdot 0 = x\cdot(\underbrace{1+0}_{1}) = x$

$\therefore x\cdot 0 = 0$

b. $x = x\cdot z\cdot z^{-1} = y\cdot z\cdot z^{-1} = y\cdot 1 = y$

$\therefore x = y$.

10. Ordered

Let K be a field. We say K is an ordered field if there is a subset $P \subseteq K$ (positive elements) with the following properties:

(i) $x, y \in P \Rightarrow x+y \in P, \ x\cdot y \in P$

(ii) For any $x \in K$, only one of the following occurs: $x = 0$, $x \in P$, $-x \in P$ $\qquad 1\cdot 1 = 1 \ ; \ x^2 \in P$

$x = 0, \ 0\cdot 0 = 0$

$x \in -P, \ -n\cdot -n = n^2 \in P$

$x \in P, \ n\cdot n \in P$ $\quad -P = \{-x \ ; \ x \in P\}$ "negative element"

$$1^2 = 1 \in P$$

Ex: $\mathbb{Q}$

$$P = \left\{\frac{a}{b} \in \mathbb{Q} \ ; \ a\cdot b \in \mathbb{N}\right\}$$

Ex: $\mathbb{Z}_p$, $\underbrace{\bar{1}+\bar{1}+\dots+\bar{1}}_{p} = \bar{0} \notin P$

$\mathbb{Z}_p$ is not ordered

Ex: $\mathbb{Q}(t)$

$$P = \left\{\frac{p(t)}{q(t)} \ ; \text{ the leading coeff. of } p(t)\cdot q(t) \text{ is positive}\right\}$$

$$\frac{t}{1}, \ \frac{2t^2+1}{t^3-t+2}, \ \frac{-t^3+t^2+1}{-t^2+2t+1}$$

$2t^5 \qquad t^5$

We write $x > y$ if $x - y \in P$ $\quad (y < x)$ $\qquad x \in P \Leftrightarrow x > 0$

$x \in -P \quad x < 0$

$x \geq y \quad (y \leq x) \qquad x - y \in P$ or $x = y$

Proposition: Let K be an ordered field, and $x, y, z \in K$:

I. $x < y$ and $y < z \Rightarrow x < z$

II. Only one of the following happens: $x = y$, $x > y$, $x < y$

III. $x < y \Rightarrow x+z < y+z$

IV. $z > 0$, $x < y \Rightarrow xz < yz$

$z < 0$, $x < y \Rightarrow xz > yz$

Let K be an ordered field.

$f: \mathbb{N} \to K$ is an increasing injective

$$n \mapsto (\underbrace{1+1+\dots+1}_{n})$$

So we can view $\mathbb{N}$ as subset of K

$$f(\mathbb{N}) \subseteq K$$

we write $\mathbb{N} \subseteq K$

When $\underbrace{1+1+\dots+1}_{p} = 0$, we say K has characteristic "p"

if $\underbrace{1+1+\dots+1}_{p}$ is never zero, we say K has characteristic zero

Ex: $\mathbb{Q}$

$\underbrace{1+1+\dots+1}_{} \neq 0$ $\qquad (\mathbb{Z}_p) \quad \underbrace{\bar{1}+\bar{1}+\dots+\bar{1}}_{p} = \bar{0}$

$$g: \mathbb{Q} \to K$$
$$\frac{a}{b} \to f(a)\cdot f(b)^{-1}$$

$$\mathbb{N} \subseteq \mathbb{Q} \subseteq K$$

Every ordered field "contains" $\mathbb{N}$ and $\mathbb{Q}$.

Proposition K an ordered field.

$$x \geq -1 \Rightarrow (1+x)^n \geq 1 + n\cdot x \quad \forall n \in \mathbb{N}$$

Proof: We use induction on $n \in \mathbb{N}$.

$n = 1$

$(1+x) \geq 1+x$ ✓

~~$n = k$~~

$n = k+1$ $\qquad 1 + (k+1)x$

$1 + kx + x$

$$(1+x)^{k+1} = (1+x)(1+x)^k \geq (1+kx)(1+x)$$
$$= 1 + x + kx + kx^2$$
$$\geq 1 + x + kx$$
$$= 1 + (k+1)\cdot x$$