Final: May 8, Friday, 9am

Midterms:

1. Feb 18, Wed
2. Mar 30, Mon

Homeworks

Due Thursday night

HW 1 due Jan 22

Fields

Examples:

(1) $\mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2$

More generally,

$\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$

p: prime number

(2) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

Defn A field is a tuple $(k, +, 0, \cdot, 1)$

Where:
- $(k, +, 0)$ is an additive abelian group

- $\cdot : k \times k \longrightarrow k$

  $(x, y) \longmapsto x \cdot y$

- $1 \in k \setminus \{0\}$

s.t.

(1) (Commutativity) $\forall x, y \in k$

$$x \cdot y = y \cdot x$$

(2) (Associativity) $\forall x, y, z \in k$

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z$$

(3) (Identity) $\forall x \in k$

$$x \cdot 1 = 1 \cdot x = x$$

(4) (Distributivity)

$\forall x, y, z \in k$

$$x \cdot (y + z) = x \cdot y + x \cdot z$$

$$(y + z) \cdot x = y \cdot x + z \cdot x$$

(5) (Multiplicative inverses)

$\forall x \in k \setminus \{0\} = k^{\times}$

$\exists x^{-1} \in k^{\times}$ s.t. $x \cdot x^{-1} = x^{-1} \cdot x = 1$

Rmk If we omit 5

then we get the notion

of a $\boxed{\text{Commutative ring}}$

Example: (Comm. rings)

1. $\mathbb{Z}$

2. $\mathbb{Z}/n\mathbb{Z}$, $\forall n \in \mathbb{Z} \setminus \{1,-1\}$

3. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$: comm ring

   w. co-ordinatewise addition

   & multiplication

This is <u>not</u> a field because

$$(1,0)\cdot(0,1) = (1\cdot 0, 0\cdot 1)$$
$$= (0,0)$$

Rmk: 1. In any commutative ring

$$0 \cdot x \overset{?}{=} 0$$

$$\|$$

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

$$\Downarrow$$

$$0\cdot x = 0\cdot x + 0\cdot x$$

$$\Downarrow -0\cdot x$$

$$0 = 0\cdot x.$$

(2) In any field

$$x\cdot y = 0 \Rightarrow x=0 \text{ or } y=0$$

Otherwise, if $x \neq 0$ then

$$x^{-1}\cdot 0 = x^{-1}(x\cdot y) = (x^{-1}\cdot x)\cdot y$$

$$0 = y = 1\cdot y$$

Example (4)

Rings of polynomials

$$\mathbb{Z}[x],\quad \mathbb{F}_2[x],\quad \mathbb{F}_3[x]$$

Def$^{\underline{n}}$ R : commutative ring

$(R, +, 0, \cdot, 1)$

$$R[x] = \left\{ (r_0, r_1, r_2, \ldots) : r_n \in R \ \forall n \geq 0 \text{ s.t. } r_m = 0 \ \forall \underbrace{m >> 0}_{\text{"sufficiently large"}} \right\}$$

Notation:

$$(r_0, r_1, r_2, \ldots) \longleftrightarrow r_0 + r_1 \cdot x + r_2 \cdot x^2 + \cdots + r_n \cdot x^n + \cancel{0 \cdot x^{n+1} + 0 \cdot x^{n+2} + \cdots}$$

An element of $R[x]$ is a polynomial with coefficients in R and will be denoted in the form $f(x), g(x), q(x), \ldots$

Def^n $f(x) \in R[x] \setminus \{0\}$

$0 \leftrightarrow (0, 0, \ldots, 0, \ldots)$

$$\deg(f(x)) = \max\{n : a_n \neq 0\}$$

$f(x) = a_0 + a_1 x + \cdots + a_n x^n + \cdots$

Example: $\cdot\ 1 \in R[x]$

$$1 = (1, 0, 0, \ldots)$$

$\cdot\ r \in R$

$$r \in R[x] \leftrightarrow (r, 0, 0, \ldots)$$

Constant polynomial with value r

$$\deg(r) = 0.$$

In fact $f(x) \in R[x]$ is constant

$$\Leftrightarrow \deg(f(x)) = 0$$

$\cdot\ r_0 + r_1 x = r_1 x + r_0$

deg 1 or linear polynomials

$\cdot\ r_0 + r_1 x + r_2 x^2$: quadratic or deg 2

Operations in $R[x]$

- $(r_0, r_1, \dots) + (s_0, s_1, \dots)$

$$= (r_0 + s_0, r_1 + s_1, \dots)$$

- $(r_0, r_1, \dots) \cdot (s_0, s_1, \dots)$

$$= \Big(r_0 s_0, r_0 s_1 + r_1 s_0, \dots, \overbrace{\sum_{k+l=n} r_k s_l}^{n\text{-th term}}, \dots\Big)$$

Notation

- $(r_0 + r_1 x + \dots + r_n x^n) + (s_0 + s_1 x + \dots + s_n x^n)$

$$= (r_0 + s_0) + (r_1 + s_1)x + \dots + (r_n + s_n)x^n$$

- $(r_0 + r_1 x + \dots + r_n x^n) \cdot (s_0 + s_1 x + \dots + s_n x^n)$

$$= r_0 r_1 + (r_0 s_1 + r_1 s_0)x + \dots + \Big(\sum_{k+l=m} r_k s_l\Big)x^m + \dots + r_n s_n x^{2n}$$

Need to check:

(1) Commutativity of $\circ$

$\Uparrow$

Commutativity of $\cdot$ in R

(2) Associativity of $\cdot$?? ✓

(3) $1 \cdot (r_0, r_1, \ldots) \overset{\checkmark}{=} (r_0, r_1, \ldots)$

$\parallel$

$(1, 0, \ldots 0)(r_0, r_1, \ldots) = (1 \cdot r_0, 1 \cdot r_1, 1 \cdot r_2, \ldots)$

$= (r_0, r_1, r_2, \ldots)$

(4) Distributivity ?? ✓

Rmk

$(r_0 + r_1 x + \ldots + r_n x^n) \cdot x^m$

$= r_0 x^m + r_1 x^{m+1} + \ldots + r_n x^{n+m}$

$\Downarrow$

$$(r_0 + r_1 x + \dots + r_n x^n) \cdot (s_m x^m + s_{m+1} x^{m+1})$$

$$\parallel$$

$$(r_0 + r_1 x + \dots + r_n x^n) \cdot s_m x^m$$

$$+$$

$$(\dots) \cdot s_{m+1} x^{m+1}$$

$$\begin{array}{ccccccc} r_0 s_m x^m & + & r_1 s_m x^{m+1} & + & r_2 s_m x^{m+2} & + & \\ & & + & & + & & \\ & & r_0 s_{m+1} x^{m+1} & + & r_1 s_{m+1} x^{m+2} & \dots & \end{array}$$

$$r_0 s_m x^m + (r_1 s_m + r_0 s_{m+1}) x^{m+1} + (r_2 s_m + r_1 s_{m+1}) x^{m+2}$$

Fact: $R[x]$ is a commutative ring