Rings and Fields (II)

Thursday, 3 March 2022 12:06

Recall the unity of a ring (if exists) is the multiplicative identity 1. (Usually $1 \neq 0$)

Def: The (multiplicative) inverse x^{-1} of $x \in R$ is an element s.t. $xx^{-1} = x^{-1}x = 1$ (actually unique)

An element that has an multiplicative inverse is a unit.

$R^{\times} = \{\text{units in } R\}$.

If every nonzero element is a unit, then R is a division ring. If R is also commutative, then R is a field.

Examples: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields

- $\mathbb{Z}$ is not a field, $\mathbb{Z}^\times = \{\pm 1\}$
- $M_n(\mathbb{R})$, unity = identity matrix

(For $M_n(R)$, $\begin{pmatrix} 1_R & & 0 \\ & \ddots & \\ 0 & & 1_R \end{pmatrix}$)

Units of $M_n(\mathbb{R})$ are invertible matrices, i.e., $\det M \neq 0$.

(For comm rings R, the units of $M_n(R)$ are those $\det M \in R^\times$)

$MN = I \Rightarrow \det(M)\det(N) = 1_R$

- $\mathbb{R}[x]$, unity = $1 + 0x + \cdots$

units = $\{c : c \neq 0\}$ non-zero constant poly

- $\mathbb{Z}_4[x]$ $(1+2x)(1-2x)$

$= 1^2 - (2x)^2 = 1 - 4x^2 = 1$

Challenging question: Find $(\mathbb{R}[x])^\times$.

Prop: $a \in \mathbb{Z}_n$ is a unit $\Leftrightarrow \gcd(a,n) = 1$.

Proof: $\gcd(a,n) = 1$

$\Leftrightarrow ax + ny = 1 \quad x, y \in \mathbb{Z}$

$\Leftrightarrow ax = 1$ in $\mathbb{Z}_n$

$\Leftrightarrow a$ is a unit $\square$

$\mathbb{Z}_n^\times = \{a : \gcd(a,n) = 1\}$

Corollary: If p is a prime, then $\mathbb{Z}_p$ is a field. $\mathbb{F}_p$

(Converse is also true)

Another "multiplication" in R.

Let $n \in \mathbb{Z}$, $a \in R$.

Define $n \cdot a = \underbrace{a + \dots + a}_{n \text{ times}}$ if $n \geq 0$

$0 \cdot a = 0_R$

$(-n) \cdot a = -(a + \dots + a) = (-a) + \dots + (-a)$

Def: $(R_1, +_1, \cdot_1), (R_2, +_2, \cdot_2), \ldots (R_n, +_n, \cdot_n)$ are rings.

$R_1 \times \ldots \times R_n$ is the <u>direct product</u> of $R_1, \ldots, R_n$.

Underlying set: $\{(r_1, \ldots, r_n) : r_i \in R_i\}$.

Addition: $(r_1, \ldots, r_n) + (s_1, \ldots, s_n)$

$$= (r_1 +_1 s_1, \ldots, r_n +_n s_n)$$

Multiplication: $(r_1, \ldots, r_n) \cdot (s_1, \ldots, s_n)$

$$= (r_1 \cdot_1 s_1, \ldots, r_n \cdot_n s_n).$$

Def: R, R' are rings. $\varphi : R \to R'$ is a ring <u>homomorphism</u> if $\forall a, b \in R$

(1) $\varphi(a +_{R} b) = \varphi(a) +_{R'} \varphi(b)$

(2) $\varphi(a \cdot_{R} b) = \varphi(a) \cdot_{R'} \varphi(b)$

A homomorphism is an <u>isomorphism</u> if φ is bijective.

$\ker(\varphi) = \{a \in R : \varphi(a) = 0_{R'}\}$.

Example:

(1) $\varphi : \mathbb{Z} \to \mathbb{Z}_n$

$$a \mapsto a \pmod{n}$$

φ preserves addition

φ preserves multiplication

$$\begin{aligned}\varphi(ab) &= ab \pmod{n} \\ &= a \pmod{n} \cdot b \pmod{n} \\ &= \varphi(a)\varphi(b)\end{aligned}$$ $\square$

(2) $ev_a : \{f : \mathbb{R} \to \mathbb{R}\} \to \mathbb{R}$

$a \in \mathbb{R}$

$ev_a(f) = f(a)$

$ev_2(x^2+1) = 2^2+1 = 5$.

$$\begin{aligned} ev_a(f+g) &= (f+g)(a) \\ &= f(a)+g(a) \\ &= ev_a(f)+ev_a(g) \end{aligned}$$

Similarly for $\cdot$ $\square$

Non-example: $\varphi: \mathbb{Z} \to 2\mathbb{Z}$

$n \mapsto 2n$

φ is a <u>group</u> homomorphism.

$\varphi(m+n) = 2(m+n) = 2m+2n = \varphi(m)+\varphi(n)$

$\varphi(2\cdot 2) = \varphi(4) = 8$ Not a <u>ring</u>

$\varphi(2)\cdot\varphi(2) = 4\times 4 = 16$ homomorphism.

Exer: If p, q are distinct primes then $\mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$ as <u>rings</u>.

$\varphi: \mathbb{Z}_{pq} \to \mathbb{Z}_p \times \mathbb{Z}_q$

$n \pmod{pq} \mapsto (n \pmod p, n \pmod q)$

$$\varphi(nm) = (nm \pmod p, nm \pmod q)$$
$$= (n \pmod p \cdot m \pmod p, n \pmod q \cdot m \pmod q)$$
$$= (n \pmod p, n \pmod q) \cdot (m \pmod p, m \pmod q)$$
$$= \varphi(n) \cdot \varphi(m)$$

Bijectivity & group homomorphism granted from lectures on groups. □

Def: Let $(R, +, \cdot)$ be a ring, a subset S of R is a <u>subring</u> if $(S, +, \cdot)$ is a ring itself, i.e.

(1) $(S, +)$ is a subgp

(2) S is closed under $\cdot$ $\quad a, b \in S \Rightarrow a \cdot b \in S$

Foreshadowing: "Normal" subrings are called <u>ideals</u>.

Solve $x^2-3x+2=0$ over $\mathbb{R}$.

$\Rightarrow (x-2)(x-1)=0$

$\Rightarrow x-2=0$ or $x-1=0$

$\Rightarrow x=1$ or 2

Solve $x^2-3x+2=0$ (*) over $\mathbb{Z}_6$

So $1,2 \in \mathbb{Z}_6$ are sol'n to (*)

But $4^2-3\cdot 4+2$

$= 6 = 0$.

So $x=4$ is also a sol'n.

$$4^2 - 3\cdot 4 + 2$$
$$= (4-2)\cdot(4-1)$$
$$= 2\cdot 3 = 0 \text{ in } \mathbb{Z}_6$$

Caution: $ab=0$ doesn't imply $a=0$ or $b=0$.

Def: A non-zero element $a \in R$ is <u>zero divisor</u> if $ab=0$ for some $b \neq 0$.

If R is commutative with unity 1 and no zero divisors, then R is an <u>integral domain</u>.

Example: $\mathbb{Z}$ is an ID.

Example: Any field is an ID.

Prop: If $x \in R^\times$, then x is not a zero divisor.

Proof: Suppose $xy = 0$. Since $x \in R^\times$, x^{-1} exists, so $(x^{-1}x)y = x^{-1}0 = 0$

$$1y = 0 \qquad \square$$

Prop: $a \in \mathbb{Z}_n$ is a zero divisor $\iff \gcd(a,n) \neq 1$.

Proof: "$\Rightarrow$" $\gcd(a,n) = 1$

$\Rightarrow a$ is a unit

$\Rightarrow a$ is not a zero divisor

"$\Leftarrow$" $\gcd(a,n) = d \neq 1$.

$$a \cdot \left(\frac{n}{d}\right)$$
$$= \left(\frac{a}{d}\right) \cdot n = 0 \text{ in } \mathbb{Z}_n. \square$$

Corollary: $a \in \mathbb{Z}_n$ is either 0, a unit, or a zero divisor.

Def: A ring has <u>cancellation property</u> if $ab = ac$, $a \neq 0$
$\Rightarrow b = c$
& $ac = bc$, $c \neq 0 \Rightarrow a = b$.

Theorem: R has the CD $\Leftrightarrow$ R has no zero divisors.

Proof: "$\Rightarrow$" If a is a zero divisor, then $ab = 0$ for some $b \neq 0$.
Now $ab = a \cdot 0$ and $a \neq 0$, but $b \neq 0$.

"$\Leftarrow$" $ab = ac$, $a \neq 0$

$$a(b-c) = 0$$
$$b - c = 0$$
$$b = c$$

Similarly for $ac = bc \Rightarrow a = b$. □

Corollary: Every ID has cancellation property.

Proposition: Solving equations by factoring into linear factors works whenever R has cancellation property.

Prop: Every finite ID is a field.

Proof: Let R be a finite ID.

Let $a \neq 0$ in R, want to show inverse of a exists.

Consider $\varphi : R \to R$, $r \mapsto ar$.

φ is injective because $ar = as$, $a \neq 0$
$r = s$ by CP

φ is a map between two finite sets of the same size, so φ is bijective

$\therefore$ 1 is in the image of φ, i.e.

$\varphi(b) = 1 \Rightarrow ab = 1 \Rightarrow b = a^{-1}$. $\square$

Thm (Wedderburn): Every <u>finite</u> division ring is a field.

Corollary: For finite rings;

ID = division ring = field

Def: Let R be a ring with 1.

The <u>characteristic</u> of R is the smallest $n > 0$ s.t. $\underbrace{1 + \dots + 1}_{n \text{ times}} = 0$

$\operatorname{char} R = 0$ if no such n exists.

Example: $\operatorname{char} \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C} = 0$

$\operatorname{char} \mathbb{Z}_n = n$