Section 18 - Rings & fields

7/3 I

Def A ring is a set R with two binary operations $+$ & $\cdot$, such that

- R1: $(R, +)$ is an abelian group
- R2: $\cdot$ is associative
- R3: For $a, b, c \in R$

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{and}$$

$$(b + c) \cdot a = b \cdot a + c \cdot a.$$

R3 = "left/right distributive law".

Examples. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ with usual notions of $+$ & $\cdot$ are rings.

- For any integer n, $n\mathbb{Z} \subseteq \mathbb{Z}$ is a ring. $\{$
  Check that $\cdot$ is well-defined: If $a, b \in n\mathbb{Z}$, then $a = nr$, $b = ns$ for $r, s \in \mathbb{Z}$, so
  $$a \cdot b = nr \cdot ns = n(nrs),$$
  hence $a \cdot b \in n\mathbb{Z}$. Axioms R1, R2, R3 follow from $\mathbb{Z}$.
- Let R be a ring, $M_n(R) = \{(n \times n)\text{-matrices with entries in } R\}$
  Then usual matrix addition & multiplication makes $M_n(R)$ a ring. E.g. $M_n(\mathbb{Z})$, $M_n(\mathbb{Q})$, $M_n(\mathbb{R})$, $M_n(\mathbb{C})$.
- On $\mathbb{Z}_n$, define a product $\cdot_n$ by
  $$a \cdot_n b = \text{remainder of } ab \text{ divided by } n.$$
  Then $(\mathbb{Z}_n, +_n, \cdot_n)$ is a ring.
  Example: In $\mathbb{Z}_5$, $3 \cdot_5 3 = 4$, since $3 \cdot 3 = 9$, remainder of 9 divided by 5 is 4.

Notation: • Write ab instead of $a \cdot b$

• Write $0 \in R$ for additive identity in R $\quad (0+a = a+0 = a)$

• Write $-a$ for additive inverse of $a \in R$

• Write $n \cdot a = \overbrace{a + \cdots + a}^{n}$, $\quad (-n) \cdot a = \overbrace{(-a) + \cdots + (-a)}^{n}$

$0 \cdot a = 0$.

Here $n \in \mathbb{Z}^+$, not an element of R.

Thm Let R be a ring, $a, b \in R$. Then

(1) $0a = a0 = 0$

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

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

(Partial) **Proof** $0 = 0 + 0$, so

(1) $0a = (0+0)a \overset{R3}{=} 0a + 0a$.

$\Downarrow$

$0a + 0 = 0a + 0a$

$\Downarrow$ cancellation

$0 = 0a$.

(2) $(-a)b + ab = (-a + a)b = 0b = 0 = -ab + ab$

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

$\Downarrow$ cancellation

$(-a)b = -ab$

□

Homomorphisms Let R, R' be rings. A homomorphism from R to R' is a map $\phi : R \to R'$ such that for all $a, b \in R$,

(1) $\phi(a+b) = \phi(a) + \phi(b)$

(2) $\phi(ab) = \phi(a)\,\phi(b)$

Note: A ring homomorphism $\phi: R \to R'$ is also a homomorphism of groups $(R, +) \to (R', +')$. Hence

$$\text{Ker } \phi = \{x \in R \mid \phi(x) = 0\}$$

is a subgroup of $(R, +)$, and ϕ is one-to-one $\iff \text{Ker } \phi = \{0\}$.

Example: Recall group homomorphism $\phi: (\mathbb{Z}, +) \to (\mathbb{Z}_n, +_n)$

$\phi(k)$ = remainder of k divided by n.

This is a ring homomorphism, that is

$$\phi(k_1 k_2) = \phi(k_1)\phi(k_2)$$

Example: $\phi: \mathbb{Z} \to \mathbb{Z}_5$, $k_1 = 8$ $k_2 = 13$

$$\phi(8 \cdot 13) = \phi(104) = 4$$

$$\phi(8)\phi(13) = 3 \cdot_5 3 = 4 \qquad \text{(remainder of 9 by 5 is 4).}$$

Def A homomorphism $\phi: R \to R'$ which is bijective is an isomorphism.

Write $R \cong R'$.

Example: There is no (ring) isomorphism from $\mathbb{Z}$ to $2\mathbb{Z}$.

In $\mathbb{Z}$, have a multiplicative identity 1: $1a = a1 = a \quad \forall a \in \mathbb{Z}$.

In $2\mathbb{Z}$, have no multiplicative identity.

An interesting isomorphism

Def Let $R_1, \ldots, R_n$ be rings. The direct product ring is

$$R_1 \times \cdots \times R_n = \{(r_1, \ldots, r_n) \mid r_i \in R_i\}$$

$$(r_1, \ldots, r_n)(r_1', \ldots, r_n') = (r_1 r_1', \ldots, r_n r_n')$$

$$(r_1, \ldots, r_n) + (r_1', \ldots, r_n') = (r_1 + r_1', \ldots, r_n + r_n')$$

Def A ring R with a multiplicative identity element is a *ring with unity*. Write $1 \in R$ for this element, call it *unity*.

Thm Let R be a ring with unity $1 \in R$, $m, n \in \mathbb{Z}$. Then

$$(m \cdot 1)(n \cdot 1) = (mn) \cdot 1$$

Proof if $m, n \geq 0$: Associative law gives

$$(m \cdot 1)(n \cdot 1) = \overbrace{(1 + \cdots + 1)}^{m}\overbrace{(1 + \cdots + 1)}^{n} = \overbrace{(1)(1) + \cdots + (1)(1)}^{mn}$$

$$= \overbrace{1 + \cdots + 1}^{mn} = (mn) \cdot 1.$$

Example: Let $r, s \in \mathbb{Z}^+$ such that $\gcd(r, s) = 1$.

Then $\mathbb{Z}_{rs} \simeq \mathbb{Z}_r \times \mathbb{Z}_s$ as rings.

Know from group theory that $(\mathbb{Z}_{rs}, +)$ is cyclic, generated by 1 & $(\mathbb{Z}_r \times \mathbb{Z}_s, +)$ is cyclic, generated by $(1,1)$.

Have group isomorphism $\phi : \mathbb{Z}_{rs} \longrightarrow \mathbb{Z}_r \times \mathbb{Z}_s$ by

$$\phi(n \cdot 1) = n \cdot (1,1).$$

Need to check this is ring homomorphism, $\phi(ab) = \phi(a)\phi(b)$.

for all $a, b \in \mathbb{Z}_{rs}$.

Write $a = m \cdot 1$, $b = n \cdot 1$, $m, n \in \mathbb{Z}$. Then

$$\phi(ab) = \phi((m \cdot 1)(n \cdot 1)) = \phi((mn) \cdot 1) = mn \cdot (1,1) = (mn \cdot 1, mn \cdot 1)$$

$$\phi(a)\phi(b) = \phi(m \cdot 1)\phi(n \cdot 1) = m \cdot (1,1)\ n \cdot (1,1) = (m \cdot 1\, n \cdot 1,\ m \cdot 1\, n \cdot 1)$$

$$= (mn) \cdot 1, (mn) \cdot 1).$$

$$\phi(a)\phi(b) = \phi(ab).$$

Def A ring R is *commutative* if

$$ab = ba \qquad \forall\, a, b \in R.$$

Def Let R be a ring with unity 1. A *multiplicative inverse* for an element $a \in R$ is an element $a^{-1} \in R$ such that

$$a a^{-1} = a^{-1} a = 1.$$

An element $a \in R$ is a *unit* if it has a multiplicative inverse.

Example: In $\mathbb{Z}$, the units are 1 & -1,

If $|n| > 1$, then n has no multiplicative inverse in $\mathbb{Z}$

0 has no multiplicative inverse in $\mathbb{Z}$

$1 \cdot 1 = 1$ $\quad (-1)(-1) = 1$, so each of 1, -1 are units.

Def A ring R (with unity) is a *division ring* / *skew field* if all $x \in R \setminus \{0\}$ are units. A commutative division ring is a *field*.

Example $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields

$\mathbb{Z}_2$ is a field: Has unity 1, only one non-zero element $1 \in \mathbb{Z}_2$, which is a unit.

$\mathbb{Z}_3$ is a field: $\mathbb{Z}_3^* = \{1, 2\}$, and $(1)(1) = 1$, $(2)(2) = 1$,

so 1 & 2 are units

$\mathbb{Z}_4$ is not a field: $\mathbb{Z}_4^* = \{1, 2, 3\}$, multiplication table

	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Units are 1 & 3.

2 is not a unit, since the remainder of $2n$ divided by 4 is either 0 or 2.