Rings and Fields

부산대학교
PUSAN NATIONAL UNIVERSITY

Ring Structure

- **Def**

  Let R be a nonempty set on which we have two closed binary operations, denoted by + and ·. Then $(R,+,\cdot)$ is a ring if for all $a,b,c \in R$, the following conditions are satisfied:

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

  b) $\exists\ z\ (\in R)$ such that $a + z = z + a = a$

  c) For each $a \in R$, $\exists\ b$ with $a + b = b + a = z$

  d) $a + b = b + a$ ---------- abelian group with +

  e) $a\cdot(b+c) = a\cdot b + a\cdot c$ and $(b+c)\cdot a = b\cdot a + c\cdot a$

  f) $a\cdot(b\cdot c) = (a\cdot b)\cdot c$

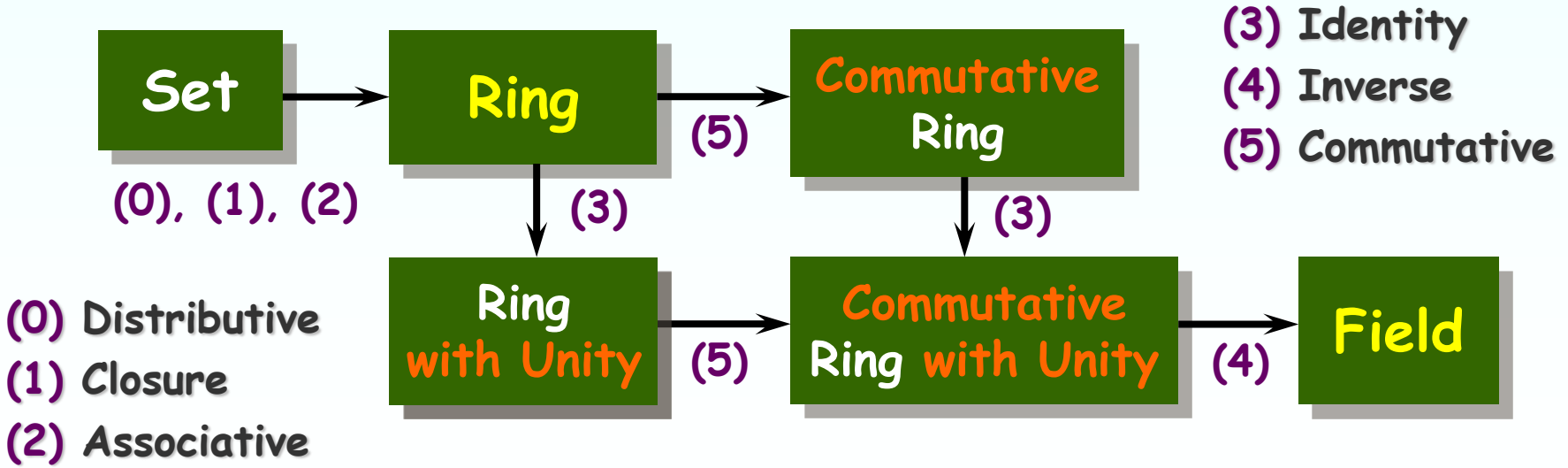
  $a(bc) = (ab)c$!!

Examples

Under the ordinary addition and multiplication, Z, Q, R, and C are rings.

Let $M_{2,2}(Z)$ be the set of all 2×2 matrices with integer entries. Then it is a ring under the ordinary matrix addition and matrix multiplication.

?



Commutative Ring with Unity

- Let $(R,+,\cdot)$ be a ring.

  Commutative Ring : $ab = ba$ for all $a,b \in R$

  Ring with Unity :

  $\exists\ u\ (\in R)$ such that $au = ua = a$ and $u \neq z$ for all $a \in R$. The u is called a unity or multiplicative identity.

  Commutative Ring with Unity :

  a commutative ring that has the unity. Note that the unity is unique.

An Example

- $(Z, \oplus, \otimes)$: $x \oplus y = x+y-1$ and $x \otimes y = x+y-xy$

  1) $\oplus$ and $\otimes$ are closed operators.
  2) $\oplus$ is associative.
  3) $\exists$ an additive identity $z = 1$ for $\oplus$.

     $x \oplus z = x+z-1 = x \;\; \therefore z = 1$

  4) The additive inverse of x is $2-x$.

     $x \oplus y = x+y-1 = 1 \;\; \therefore y = 2-x$

  5) $(Z, \oplus, \otimes)$ satisfies distributive law of $\otimes$ over $\oplus$.
     Operator $\otimes$ is associative and commutative.
  6) Unity (multiplicative identity) 0:

     $x \otimes u = x+u-xu = x \rightarrow u(1-x) = 0 \;\; \therefore u = 0$

Another Example

- $U = \{1,2\}$ and $R = P(U)$ (power set)

  For $A, B \subseteq U$,

  $A+B = A \Delta B = \{ x \mid x \in A$ or $x \in B$, but not both $\}$

  $A \cdot B = A \cap B$ = intersection of sets A, B

+	ϕ	{1}	{2}	U
ϕ	ϕ	{1}	{2}	U
{1}	{1}	ϕ	U	{2}
{2}	{2}	U	ϕ	{1}
U	U	{2}	{1}	ϕ

·	ϕ	{1}	{2}	U
ϕ	ϕ	ϕ	ϕ	ϕ
{1}	ϕ	{1}	ϕ	{1}
{2}	ϕ	ϕ	{2}	{2}
U	ϕ	{1}	{2}	U

Additive Identity : ϕ

Additive Inverse : itself

Unity : U

Commutative

{1},{2} : proper divisors of zero

Multiplicative Inverse & Unit

- **Def**

  Let R be a ring with unity u.

  If $a \in R$ and there exist $b \in R$ such that $ab = ba = u$, then

  b is called a multiplicative inverse of a and

  a is called a unit of R.

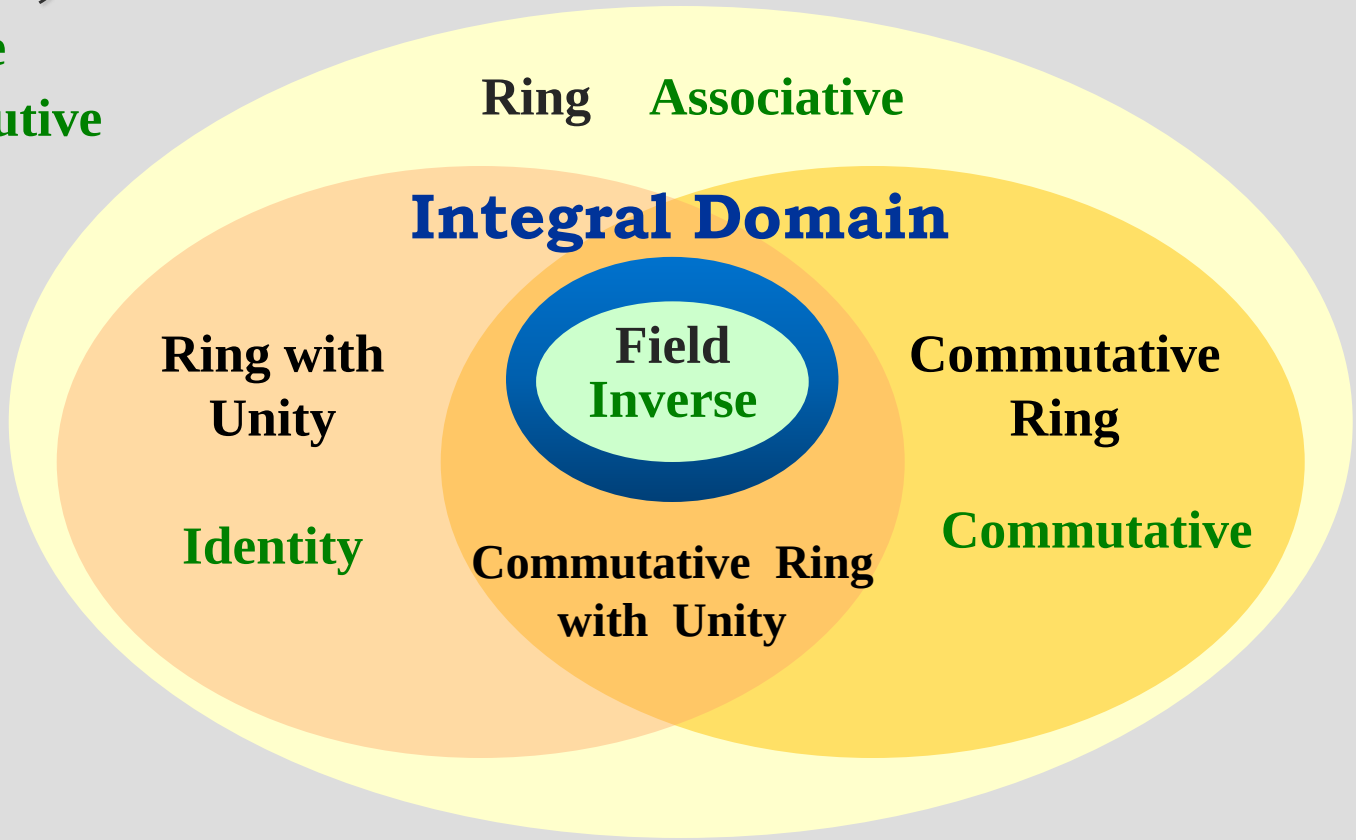
  (The b is also a unit of R.)

Integral Domain (with two binary operators)

$< K, \oplus, \otimes >$

Closure

Distributive



Integral Domain & Field

- **Def**

  Let R be a commutative ring with unity. Then

  (a) R is called an integral domain if R has no proper divisors of zero.

  (b) R is called a field if every nonzero element of R is a unit.

  $ab = z \rightarrow$ $a = z$ or $b = z$

  - $(Z,+,\cdot)$: an integral domain but not field (only 1 and –1 are units.)
  - $(Q,+,\cdot)$, $(R,+,\cdot)$, $(C,+,\cdot)$: integral domain & field

An Example

Let $M_{2,2}(Z)$ be the set of all 2X2 matrices with integer entries. Is it an integral domain under the ordinary matrix addition and matrix multiplication ?

No. Because it is not a commutative ring with unity.

AB = 0 ➔ A = 0 or B = 0 ?

$$\begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}=\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix},\quad \begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}^2=\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}$$

CA = CB ➔ A = B ?

$$\begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}=\begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}\begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}=\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}$$

Ring Properties (1)

- **Theorem 1** — Group $(R,+)$!!!

  In any ring $(R,+,\cdot)$,

  (a) the additive identity z is unique, and

  (b) the additive inverse of each ring element is unique.

  (Notation) $-a \equiv$ additive inverse of a

- **Theorem 2** (Cancellation of Addition)

  For all $a, b, c \in R$,

  (a) $a + b = a + c \rightarrow b = c$, and

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

Ring Properties (2)

- **Theorem 3**

  For any $a \in$ ring $(R, +, \cdot)$ with additive identity z, we have $az = za = z$.

  (Proof)

  $az + z = az = a(z + z) = az + az$

  By the cancellation law, $z = az$.

  Similarly, $za = z$.

  Thus z is a zero element for the multiplicative operation.

Ring Properties (3)

- **Theorem 4**

  Given a ring $(R,+,\cdot)$, for all $a,b \in R$,

  (a) $-(-a) = a$

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

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

  (Proof of (b))

  $ab + a(-b) = a[b + (-b)] = az = z$ &

  $ab + (-a)b = [a + (-a)]b = zb = z.$

  From the uniqueness of additive inverse,

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

Ring Properties (4)

- **Theorem 5**

  For a ring $(R,+,\cdot)$,

  (a) if R has a unity, then it is unique, and

  (b) if R has a unity, and x is a unit of R, then the multiplicative inverse of x is unique.

  (Notation) $x^{-1} \equiv$ multiplicative inverse of x

  (Proof)

  If u and v are unity's of R, then $u = uv = v$. Thus the unity is unique.

  Let a and b are multiplicative inverses of x. Then $a = au = a(xb) = (ax)b = ub = b$. Therefore, ...

Ring Properties (5)

- **Theorem 6**

  Let $(R,+,\cdot)$ be a commutative ring with unity. Then R is an integral domain if and only if, for all $a,b,c \in R$ where $a \neq z$, $ab = ac \rightarrow b = c$.

  (cancellation of multiplication)

  (Proof)

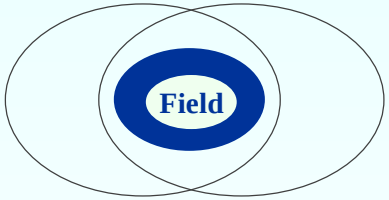
  ➡ If $ab = ac$, then $z = ab + (-(ab)) = ab + (-(ac)) = ab + a(-c) = a(b + (-c))$. Since R is an integral domain and $a \neq z$, $b + (-c) = z$. Therefore, $b = c$.

  ⬅ Conversely, let $ab = z$ for $a(\neq z), b \in R$. Since $az = z$, $ab = az$. Because R satisfies the multiplicative cancellation, $b = z$. Thus, R is an integral domain.

Ring Properties (6)

- **Theorem 7**

  If $(F,+,\cdot)$ is a field, then it is an integral domain.



(Proof)

Let $a\ (\neq z)$, $b \in F$ with $ab = z$. The nonzero element a has the unique inverse a^{-1}. Then $a^{-1}(ab) = a^{-1}z \rightarrow b = z$.

Thus F has no proper divisors of zero.

Therefore, a field is an integral domain.

Ring Properties (7)

- **Theorem 8**

  A finite integral domain $(D,+,\cdot)$ is a field.

  (Proof)

  Let $D = \{d_1, d_2, \ldots, d_n\}$.

  $dD = \{dd_1, dd_2, \ldots, dd_n\}$, for $d \in D$ and $d \neq z$.

  From closure and multiplicative cancellation, $dd_i \neq dd_j$ $(i \neq j)$ and thus $dD = D$.

  Then, $dd_k = u$ (unity) for some $1 \leq k \leq n$ and any d is a unit of D.

  Therefore, $(D,+,\cdot)$ is a field.

Polynomial Rings

Brief Introduction (1)

$(R,+,\cdot)$, $a,b \in R$

- commutative, unity integral domain

$(F,+,\cdot)$, $a,b \in F$

- division $a = qb + r$
- divisor (약수)
- prime p
- gcd (a,b)

$(R[x],+,\cdot)$, $f(x),g(x) \in R[x]$

- commutative, unity integral domain

$(F[x],+,\cdot)$, $f(x),g(x) \in F[x]$

- $f(x) = q(x)g(x) + r(x)$
- remainder theorem, root $f(x) = q(x)(x-a) + f(a)$
- divisor (factor)
- irreducible $f(x)$
- gcd $(f(x),g(x))$

Brief Introduction (2)

$(R, +, \cdot)$, $a, b \in R$

- $a \equiv b \bmod n$
- $(Z_n, +, \cdot)$ c.Ring.w-u
- $(Z_p, +, \cdot)$ Field

$(F[x], +, \cdot)$, $f(x), g(x) \in F[x]$

- $f(x) \equiv g(x) \bmod s(x)$
- $(F[x]/s(x), +, \cdot)$ c.Ring.w-u
- $(F[x]/s(x), +, \cdot)$
  irreducible $s(x)$ → Field

Galois Field

- **Theorem**

  A finite field F has order p^t, where p is a prime and $t \in Z^+$.

  A finite field of order p^t is denoted by $GF(p^t)$, where GF stands for Galois field.

(Note)

If $|F| = p$ and $\deg[s(x)] = t$, then $F[x]/s(x)$ contains p^t elements.

Galois Field

a) There is really only one field of order p^t, for each p,t, because any two finite fields of the same order are isomorphic.

b) These fields are discovered by Galois (1811-1832).

c) In practice, finite fields GF(2^n)'s have been studied.

Binary code : $b_7\ b_6\ b_5\ b_4\ b_3\ b_2\ b_1\ b_0$

$\leftrightarrow$ $b_7x^7+b_6x^6+b_5x^5+b_4x^4+b_3x^3+b_2x^2+b_1x^1+b_0$

Irreducible $s(x) = x^8+x^4+x^3+x+1$

at AES (Advanced Encryption Standard)

Report

- Exercises in Chapter 14,16 :
  - Total 16 problems

  - 14.1 : 4, 6, 7, 15
  - 14.2 : 16, 18
  - 14.3 : 8, 9, 19, 20
  - 16.1 : 5, 11, 19
  - 16.2 : 3, 11, 15

A Solution of an Exercise

- Make a ring $(R,+,\cdot)$
  - a) Determine the entries for the missing spaces
  - b) Commutative ?
  - c) Unity ? units ?
  - d) integral domain or field ?

+	s	t	x	y
s	s	t	x	y
t	t	s	y	x
x	x	y	s	t
y	y	x	t	s

·	s	t	x	y
s	□	□	□	□
t	□	t	□	□
x	□	t	□	y
y	□	□	s	□

$$xx = x(t+y) = xt+xy = t+y = x$$

$$yt = (t+x)t = tt+xt = t+t = s$$

$$yy = y(t+x) = yt+yx = s+s = s$$

$$tx = (x+y)x = xx+yx = x+s = x$$

$$ty = (x+y)y = xy+yy = y+s = y$$