Theory of Rings and Theory of Fields

CAS 701

Lei Lai

Nov 21, 2002

Definition of Ring

Ring $(D, +, \bar{}\ , 0, *)$:

$+ : D \times D \to D,$

$\bar{}\ : D \to D,$

$0 \in D,$

$* : D \times D \to D.$

- $(D, +, \bar{}\ , 0)$ is an abelian **group**
- Multiplicative associativity
- Left and right distributivity

Theory of Rings

T=(L, Γ)

L=(V, {0}, {+, $^{-}$, * }, Φ) Γ: Axioms

Name	Addition	Multiplication
Commutativity	**∀x,y. x+y = y+x**	
Associativity	**∀x,y,z. (x+y)+z = x+(y+z)**	**∀x,y,z. (x*y)*z = x*(y*z)**
Distributivity	**∀x,y,z. x*(y+z) = (x*y)+(x*z)**	**∀x,y,z. (x+y)*z = (x*z)+(y*z)**
Identity element	**∀x. 0+x = x**	*∀x. 1*x = x*
Inverse element	**∀x. $\bar{x}$+x = 0**	

Examples of Infinite Rings

- $(\mathbf{Z}, +^{Z}, {}^{-Z}, 0^{Z}, *^{Z}, 1^{Z})$ is a commutative ring with multiplicative identity.
- $(2\mathbf{Z}, +^{Z}, {}^{-Z}, 0^{Z}, *^{Z})$ is a ring without multiplicative identity.
- $(\mathbf{M}_{n\times n}, +^{M}, {}^{-M}, 0^{M}, *^{M}, 1^{M})$ is a non-commutative ring.
  - 0^{M} : zero matrix
  - 1^{M} : identity matrix

Example of Finite Rings(1)

- $(\mathbf{Z}_n, +, \bar{}, [0]_n, *, [1]_n)$ is a ring with n elements
  - $\mathbf{Z}_n = \{ [0]_n, [1]_n, [2]_n, ..., [n-1]_n \}$ is a set of equivalence classes under integers modulo n
    - $[a]_n = \{b \mid b \equiv a \ (\mathbf{mod}\ n)\} \quad (a, b \in \mathbf{Z})$
      $= \{a + kn \mid k \in \mathbf{Z}\}$
  - Definition of $+, \bar{}, *$ (modular arithmetic):
    - $[a]_n + [b]_n =_{def} [a +^Z b]_n$
    - $\overline{[a]_n} =_{def} [n -^Z a]_n$
    - $[a]_n * [b]_n =_{def} [a *^Z b]_n$

      $[8]_{12} + [6]_{12} = [2]_{12}$

      $\overline{[8]_{12}} = [12 -^Z 8]_{12} = [4]_{12}$

      $[8]_{12} * [6]_{12} = [0]_{12}$

Example of Finite Rings(2)

$(\mathbf{Z}_n, +, \bar{}, [0]_n, *, [1]_n)$ is a ring.

- Additive Commutativity:

  $[a]_n + [b]_n = [a + b]_n = [b + a]_n = [b]_n + [a]_n$
- Associativity:

  $([a]_n+[b]_n)+[c]_n=[a+b]_n+[c]_n=[(a+b)+c]_n=[a+(b+c)]_n=[a]_n+([b]_n+[c]_n)$

  $([a]_n*[b]_n)*[c]_n=[a*b]_n*[c]_n=[(a*b)*c]_n=[a*(b*c)]_n=[a]_n*([b]_n*[c]_n)$
- Distributivity:

  $[a]_n*([b]_n+[c]_n)=[a]_n*([b+c]_n)=[a*(b+c)]_n=[(a*b)+(a*c)]_n$
  $=[(a*b)]_n+(a*c)]_n=([a]_n*[b]_n)+([a]_n*[c]_n)$

  $([a]_n+[b]_n)*[c]_n=[a+b]_n*[c]_n=[(a+b)*c]_n=[(a*c)+(b*c)]_n$
  $=[a*c]_n+[b*c]_n =([a]_n*[c]_n)+([b]_n*[c]_n)$
- Additive Identity: $[a]_n + [0]_n = [a + 0]_n = [a]_n = [0 + a]_n = [0]_n + [a]_n$
- Multiplicative Identity: $[a]_n * [1]_n = [a * 1]_n = [a]_n = [1 * a]_n = [1]_n * [a]_n$
- Additive Inverse: $[a]_n + \overline{[a]}_n = [a + n - a]_n = [n]_n = [0]_n = \overline{[a]}_n + [a]_n$

Definition of Field

Field $(D, +, \bar{}\ , 0, *, {}^{-1}, 1)$:

$+ : D \times D \to D$,

$\bar{}\ : D \to D$,

$0 \in D$,

$* : D \times D \to D$,

$^{-1} : D \to D$,

$1 \in D$.

- $(D, +, \bar{}\ , 0, *)$ is a commutative **ring**
- $0 \neq 1$
- all elements of D except 0 have a multiplicative inverse.

Theory of Fields

$T=(L, \Gamma)$ $L=(V, \{0, 1\}, \{+, \bar{}\ , *, ^{-1}\}, \Phi)$ Γ: Axioms

Name	Addition	Multiplication
Commutativity	$\forall x,y.\ x+y = y+x$	$\forall x,y.\ x*y = y*x$
Associativity	$\forall x,y,z.\ (x+y)+z = x+(y+z)$	$\forall x,y,z.\ (x*y)*z = x*(y*z)$
Distributivity	$\forall x,y,z.\ x*(y+z) = (x*y)+(x*z)$	$\forall x,y,z.\ (x+y)*z = (x*z)+(y*z)$
Identity	$\forall x.\ 0+x = x$	$\forall x.\ 1*x = x$
Inverse	$\forall x.\ \bar{x}+x = 0$	$\forall x.\ (\neg(x=0) \rightarrow x*x^{-1} = 1)$
	$0 \neq 1$	

Examples of Fields

- $(\mathbf{C}, +^{C}, \bar{}^{C}, 0^{C}, *^{C}, {}^{-1}C, 1^{C})$
- $(\mathbf{Q}, +^{Q}, \bar{}^{Q}, 0^{Q}, *^{Q}, {}^{-1}Q, 1^{Q})$
- $(\mathbf{R}, +^{R}, \bar{}^{R}, 0^{R}, *^{R}, {}^{-1}R, 1^{R})$

Example of Finite Fields

- $(\mathbf{Z}_n, +, \bar{}, [0]_n, *, ^{-1}, [1]_n)$ is a field with n elements.
  - Definition of $^{-1}$:
    - $([a]_n)^{-1} =_{def} [a^{-1}]_n$, where $a *^Z a^{-1} \equiv 1 \pmod n$
      e.g. $([3]_5)^{-1} = [3^{-1}]_5 = [2]_5$
    - For a^{-1} to exist, n must be a prime number

  - Proof of new axioms:
    - Multiplicative Commutativity:

    $[a]_n * [b]_n = [a *^Z b]_n = [b *^Z a]_n = [b]_n * [a]_n$

    - Multiplicative Inverse:

    $[a]_n * ([a]_n)^{-1} = [a]_n * [a^{-1}]_n = [a *^Z a^{-1}]_n = [1]_n = ([a]_n)^{-1} * [a]_n$

Conclusion

- **Ring**: the objects possessing two binary operations related by the distributive laws.

- **Field**: the "smallest" mathematical structure in which we can perform all the arithmetic operations $+, -, \times, \div$.

References

1. D. Dummit, R. Foote, and B. Holland, *Abstract Algebra,* 1991.
2. http://mathworld.wolfram.com/Ring.html
3. http://mathworld.wolfram.com/Field.html
4. http://mathworld.wolfram.com/FieldAxioms.html