足し算とかけ算の構造

Sakaé Fuchino (渕野 昌)

Graduate School of System Informatics
Kobe University
(神戸大学大学院 システム情報学研究科)

fuchino@diamond.kobe-u.ac.jp
http://kurt.scitec.kobe-u.ac.jp/~fuchino/

(January 21, 2011 (17:08 JST) version)

神戸大学 2010 年度後期の講義

January 20, 2011

This presentation is typeset by pLaTeX with beamer class.

足し算とかけ算

- 自然数の全体 ($\mathbb{N}$)，整数の全体 ($\mathbb{Z}$)，有理数の全体 ($\mathbb{Q}$)，実数の全体 ($\mathbb{R}$) など，数の体系では，足し算 (加法，addition) とかけ算 (乗法，multiplication) の 2 つの基本演算が重要な役割をはたす．

- $\mathbb{Z}$ や $\mathbb{Q}$ や $\mathbb{R}$ での足し算や，$\mathbb{R} \setminus \{0\}$ （実数の全体から 0 を除いたもの）でのかけ算などの基本性質を抽出することで 群 の概念が得られたように，$\mathbb{Q}$ や $\mathbb{R}$ での足し算とかけ算の組の基本性質を抽出することで **環 (ring)** や **体 （たい，field; 独: Körper）** の概念が得られる．

足し算とかけ算

- 自然数の全体 ($\mathbb{N}$)，整数の全体 ($\mathbb{Z}$)，有理数の全体 ($\mathbb{Q}$)，実数の全体 ($\mathbb{R}$) など，数の体系では，足し算 (加法，addition) とかけ算 (乗法，multiplication) の 2 つの基本演算が重要な役割をはたす．

- $\mathbb{Z}$ や $\mathbb{Q}$ や $\mathbb{R}$ での足し算や，$\mathbb{R} \setminus \{0\}$（実数の全体から 0 を除いたもの）でのかけ算などの基本性質を抽出することで 群 の概念が得られたように，$\mathbb{Q}$ や $\mathbb{R}$ での足し算とかけ算の組の基本性質を抽出することで **環 (ring)** や **体（たい，field; 独: Körper）** の概念が得られる．

足し算とかけ算

- 自然数の全体 ($\mathbb{N}$)，整数の全体 ($\mathbb{Z}$)，有理数の全体 ($\mathbb{Q}$)，実数の全体 ($\mathbb{R}$) など，数の体系では，足し算 (加法，addition) とかけ算 (乗法，multiplication) の 2 つの基本演算が重要な役割をはたす.

- $\mathbb{Z}$ や $\mathbb{Q}$ や $\mathbb{R}$ での足し算や，$\mathbb{R} \setminus \{0\}$ （実数の全体から 0 を除いたもの）でのかけ算などの基本性質を抽出することで 群 の概念が得られたように，$\mathbb{Q}$ や $\mathbb{R}$ での足し算とかけ算の組の基本性質を抽出することで **環 (ring)** や **体 （たい，field; 独: Körper）** の概念が得られる.

環

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ などでの足し算とかけ算の組の基本性質を抽出することで 環 (ring) の概念が得られる:

- 集合 R と R 上の二項演算 $+$, $*$ の組が **環** であるとは，次の条件が満たされることである:
  - $(R, +)$ は アーベル群 である（$+$ に関する単位元を 0 であらわす）.
  - $(R, *)$ は 結合律 と 可換性 を満たし，単位元を持つ．つまり，ある R の要素 1 があって，すべての $a, b, c \in R$ に対し，
    (i) $a * (b * c) = (a * b) * c$,
    (ii) $a * b = b * a$,
    (iii) $1 * a = a$
    が成り立つ.
  - $+$ と $*$ に対して 分配律 が成り立つ．つまり，すべての $a, b, c \in R$ に対して，
    (iv) $(a + b) * c = a * c + b * c$
    が成り立つ.

環

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ などでの足し算とかけ算の組の基本性質を抽出することで 環 (ring) の概念が得られる:

- 集合 R と R 上の二項演算 $+$, $*$ の組が **環** であるとは，次の条件が満たされることである:
  - $(R, +)$ は アーベル群 である（$+$ に関する単位元を 0 であらわす）.
  - $(R, *)$ は 結合律 と 可換性 を満たし，単位元を持つ．つまり，ある R の要素 1 があって，すべての $a, b, c \in R$ に対し，
    (i) $a * (b * c) = (a * b) * c$,
    (ii) $a * b = b * a$,
    (iii) $1 * a = a$
    が成り立つ.
  - $+$ と $*$ に対して 分配律 が成り立つ．つまり，すべての $a, b, c \in R$ に対して，
    (iv) $(a + b) * c = a * c + b * c$
    が成り立つ.

環

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ などでの足し算とかけ算の組の基本性質を抽出することで 環 (ring) の概念が得られる:

- 集合 R と R 上の二項演算 $+$, $*$ の組が **環** であるとは，次の条件が満たされることである:
  - $(R, +)$ は アーベル群 である （$+$ に関する単位元を 0 であらわす）.
  - $(R, *)$ は 結合律 と 可換性 を満たし，単位元を持つ．つまり，ある R の要素 1 があって，すべての $a, b, c \in R$ に対し，
    (i) $a * (b * c) = (a * b) * c$,
    (ii) $a * b = b * a$,
    (iii) $1 * a = a$
    が成り立つ.
  - $+$ と $*$ に対して 分配律 が成り立つ．つまり，すべての $a, b, c \in R$ に対して，
    (iv) $(a + b) * c = a * c + b * c$
    が成り立つ.

環

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ などでの足し算とかけ算の組の基本性質を抽出することで 環 (ring) の概念が得られる:

- 集合 R と R 上の二項演算 $+$, $*$ の組が **環** であるとは，次の条件が満たされることである:
  - $(R, +)$ は アーベル群 である （$+$ に関する単位元を 0 であらわす）.
  - $(R, *)$ は 結合律 と 可換性 を満たし，単位元を持つ．つまり，ある R の要素 1 があって，すべての $a, b, c \in R$ に対し，
    (i) $a * (b * c) = (a * b) * c$,
    (ii) $a * b = b * a$,
    (iii) $1 * a = a$
    が成り立つ.
  - $+$ と $*$ に対して 分配律 が成り立つ．つまり，すべての $a, b, c \in R$ に対して，
    (iv) $(a + b) * c = a * c + b * c$
    が成り立つ.

環

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ などでの足し算とかけ算の組の基本性質を抽出することで 環 (ring) の概念が得られる:

- 集合 R と R 上の二項演算 $+$, $*$ の組が **環** であるとは，次の条件が満たされることである:
  - $(R, +)$ は アーベル群 である （$+$ に関する単位元を 0 であらわす）.
  - $(R, *)$ は 結合律 と 可換性 を満たし，単位元を持つ．つまり，ある R の要素 1 があって，すべての $a, b, c \in R$ に対し，
    (i) $a * (b * c) = (a * b) * c$,
    (ii) $a * b = b * a$,
    (iii) $1 * a = a$
    が成り立つ.
  - $+$ と $*$ に対して 分配律 が成り立つ．つまり，すべての $a, b, c \in R$ に対して,
    (iv) $(a + b) * c = a * c + b * c$
    が成り立つ.

環

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ などでの足し算とかけ算の組の基本性質を抽出することで 環 (ring) の概念が得られる:

- 集合 R と R 上の二項演算 $+$, $*$ の組が **環** であるとは，次の条件が満たされることである:
  - $(R, +)$ は アーベル群 である （$+$ に関する単位元を 0 であらわす）.
  - $(R, *)$ は 結合律 と 可換性 を満たし，単位元を持つ．つまり，ある R の要素 1 があって，すべての $a, b, c \in R$ に対し，
    (i) $a * (b * c) = (a * b) * c$,
    (ii) $a * b = b * a$,
    (iii) $1 * a = a$
    が成り立つ.
  - $+$ と $*$ に対して 分配律 が成り立つ．つまり，すべての $a, b, c \in R$ に対して,
    (iv) $(a + b) * c = a * c + b * c$
    が成り立つ.

環

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ などでの足し算とかけ算の組の基本性質を抽出することで 環 (ring) の概念が得られる:

- 集合 R と R 上の二項演算 $+$, $*$ の組が **環** であるとは，次の条件が満たされることである:
  - $(R, +)$ は アーベル群 である （$+$ に関する単位元を 0 であらわす）.
  - $(R, *)$ は 結合律 と 可換性 を満たし，単位元を持つ．つまり，ある R の要素 1 があって，すべての a, b, $c \in R$ に対し，
    (i) $a * (b * c) = (a * b) * c$,
    (ii) $a * b = b * a$,
    (iii) $1 * a = a$
    が成り立つ.
  - $+$ と $*$ に対して 分配律 が成り立つ．つまり，すべての a, b, $c \in R$ に対して，
    (iv) $(a + b) * c = a * c + b * c$
    が成り立つ.

環 (2/4)

▶ 集合 R と R 上の二項演算 $+, *$ の組が **環** であるとは，次の条件が満たされることである:

- ▷ $(R, +)$ は アーベル群 である（$+$ に関する単位元を 0 であらわす）.
- ▷ $(R, *)$ は 結合律と 可換性 を満たし，単位元 を持つ．つまり，ある R の要素 1 があって，すべての $a, b, c \in R$ に対し，
  - (i) $a * (b * c) = (a * b) * c$,
  - (ii) $a * b = b * a$,
  - (iii) $1 * a = a$ が成り立つ.
- ▷ $+$ と $*$ に対して 分配律 が成り立つ．つまり，すべての $a, b, c \in R$ に対して,
  - (iv) $(a + b) * c = a * c + b * c$ が成り立つ.

▶ (ii) により，(iii) と (iv) から，すべての $a, b, c \in R$ に対して,

(iii)' $a * 1 = a$

(iv)' $a * (b + c) = a * b + a * c$

が成り立つことがわかる.

環 (2/4)

▶ 集合 R と R 上の二項演算 $+, *$ の組が **環** であるとは，次の条件が満たされることである:

- ▷ $(R, +)$ は アーベル群 である（$+$ に関する単位元を 0 であらわす）.
- ▷ $(R, *)$ は 結合律と 可換性 を満たし，単位元 を持つ．つまり，ある R の要素 1 があって，すべての $a, b, c \in R$ に対し，
  - (i) $a * (b * c) = (a * b) * c$,
  - (ii) $a * b = b * a$,
  - (iii) $1 * a = a$ が成り立つ.
- ▷ $+$ と $*$ に対して 分配律 が成り立つ．つまり，すべての $a, b, c \in R$ に対して,
  - (iv) $(a + b) * c = a * c + b * c$ が成り立つ.

▶ (ii) により，(iii) と (iv) から，すべての $a, b, c \in R$ に対して,

(iii)' $a * 1 = a$

(iv)' $a * (b + c) = a * b + a * c$

が成り立つことがわかる.

環 (3/4)

▶ 集合 R と R 上の二項演算 $+, *$ の組が **環** であるとは，次の条件が満たされることである:

- ▷ $(R, +)$ は アーベル群 である（$+$ に関する単位元を 0 であらわす）.
- ▷ $(R, *)$ は 結合律と 可換性 を満たし，単位元 を持つ．つまり，ある R の要素 1 があって，すべての $a, b, c \in R$ に対し，
  - (i) $a * (b * c) = (a * b) * c$,
  - (ii) $a * b = b * a$,
  - (iii) $1 * a = a$ が成り立つ.
- ▷ $+$ と $*$ に対して 分配律 が成り立つ．つまり，すべての $a, b, c \in R$ に対して，
  - (iv) $(a + b) * c = a * c + b * c$ が成り立つ.

▶ $a \in R$ の $+$ に関する逆元を $-a$ と書くことにする.

▶ すべての $a \in R$ に対し，$0 * a = 0$ である.
[$0 * a = (0 + 0) * a = 0 * a + 0 * a$ この両辺に $-(0 * a)$ を足せば $0 * a = 0$ が得られる．]

▶ すべての $a \in R$ に対し，$(-1) * a = -a$ である．[$(-1) * a + a = (-1) * a + 1 * a = (-1 + 1) * a = 0 * a = 0$]

環 (3/4)

▶ 集合 R と R 上の二項演算 $+, *$ の組が **環** であるとは，次の条件が満たされることである:

- ▷ $(R, +)$ は アーベル群 である（$+$ に関する単位元を 0 であらわす）.
- ▷ $(R, *)$ は 結合律と 可換性 を満たし，単位元 を持つ．つまり，ある R の要素 1 があって，すべての $a, b, c \in R$ に対し，
  - (i) $a * (b * c) = (a * b) * c$,
  - (ii) $a * b = b * a$,
  - (iii) $1 * a = a$ が成り立つ.
- ▷ $+$ と $*$ に対して 分配律 が成り立つ．つまり，すべての $a, b, c \in R$ に対して,
  - (iv) $(a + b) * c = a * c + b * c$ が成り立つ.

▶ $a \in R$ の $+$ に関する逆元を $-a$ と書くことにする.

▶ すべての $a \in R$ に対し，$0 * a = 0$ である.
[$0 * a = (0 + 0) * a = 0 * a + 0 * a$ この両辺に $-(0 * a)$ を足せば $0 * a = 0$ が得られる．]

▶ すべての $a \in R$ に対し，$(-1) * a = -a$ である．[$(-1) * a + a = (-1) * a + 1 * a = (-1 + 1) * a = 0 * a = 0$]

環 (3/4)

- 集合 R と R 上の二項演算 $+, *$ の組が **環** であるとは，次の条件が満たされることである:
  - $(R, +)$ は アーベル群 である（$+$ に関する単位元を 0 であらわす）.
  - $(R, *)$ は 結合律と 可換性 を満たし，単位元 を持つ．つまり，ある R の要素 1 があって，すべての $a, b, c \in R$ に対し，
    - (i) $a * (b * c) = (a * b) * c$,
    - (ii) $a * b = b * a$,
    - (iii) $1 * a = a$ が成り立つ.
  - $+$ と $*$ に対して 分配律 が成り立つ．つまり，すべての $a, b, c \in R$ に対して,
    - (iv) $(a + b) * c = a * c + b * c$ が成り立つ.

- $a \in R$ の $+$ に関する逆元を $-a$ と書くことにする.
- すべての $a \in R$ に対し，$0 * a = 0$ である.

[$0 * a = (0 + 0) * a = 0 * a + 0 * a$ この両辺に $-(0 * a)$ を足せば $0 * a = 0$ が得られる．]

- すべての $a \in R$ に対し，$(-1) * a = -a$ である．[$(-1) * a + a = (-1) * a + 1 * a = (-1 + 1) * a = 0 * a = 0$]

環 (3/4)

- 集合 R と R 上の二項演算 $+, *$ の組が **環** であるとは，次の条件が満たされることである:
  - $(R, +)$ は アーベル群 である（$+$ に関する単位元を 0 であらわす）.
  - $(R, *)$ は 結合律と 可換性 を満たし，単位元 を持つ．つまり，ある R の要素 1 があって，すべての $a, b, c \in R$ に対し，
    - (i) $a * (b * c) = (a * b) * c$,
    - (ii) $a * b = b * a$,
    - (iii) $1 * a = a$ が成り立つ.
  - $+$ と $*$ に対して 分配律 が成り立つ．つまり，すべての $a, b, c \in R$ に対して,
    - (iv) $(a + b) * c = a * c + b * c$ が成り立つ.

- $a \in R$ の $+$ に関する逆元を $-a$ と書くことにする.
- すべての $a \in R$ に対し，$0 * a = 0$ である.

[$0 * a = (0 + 0) * a = 0 * a + 0 * a$ この両辺に $-(0 * a)$ を足せば $0 * a = 0$ が得られる．]

- すべての $a \in R$ に対し，$(-1) * a = -a$ である．[$(-1) * a + a = (-1) * a + 1 * a = (-1 + 1) * a = 0 * a = 0$]

環 (3/4)

▶ 集合 R と R 上の二項演算 $+, *$ の組が **環** であるとは，次の条件が満たされることである:

- ▷ $(R, +)$ は アーベル群 である（$+$ に関する単位元を 0 であらわす）.
- ▷ $(R, *)$ は 結合律と 可換性 を満たし，単位元 を持つ．つまり，ある R の要素 1 があって，すべての $a, b, c \in R$ に対し，
  - (i) $a * (b * c) = (a * b) * c$,
  - (ii) $a * b = b * a$,
  - (iii) $1 * a = a$ が成り立つ.
- ▷ $+$ と $*$ に対して 分配律 が成り立つ．つまり，すべての $a, b, c \in R$ に対して，
  - (iv) $(a + b) * c = a * c + b * c$ が成り立つ.

▶ $a \in R$ の $+$ に関する逆元を $-a$ と書くことにする.

▶ すべての $a \in R$ に対し，$0 * a = 0$ である.
[$0 * a = (0 + 0) * a = 0 * a + 0 * a$ この両辺に $-(0 * a)$ を足せば $0 * a = 0$ が得られる．]

▶ すべての $a \in R$ に対し，$(-1) * a = -a$ である．[$(-1) * a + a = (-1) * a + 1 * a = (-1 + 1) * a = 0 * a = 0$]

環 (3/4)

▶ 集合 R と R 上の二項演算 $+, *$ の組が **環** であるとは，次の条件が満たされることである:

- ▷ $(R, +)$ は アーベル群 である（$+$ に関する単位元を 0 であらわす）.
- ▷ $(R, *)$ は 結合律と 可換性 を満たし，単位元 を持つ．つまり，ある R の要素 1 があって，すべての $a, b, c \in R$ に対し，
  - (i) $a * (b * c) = (a * b) * c$,
  - (ii) $a * b = b * a$,
  - (iii) $1 * a = a$ が成り立つ.
- ▷ $+$ と $*$ に対して 分配律 が成り立つ．つまり，すべての $a, b, c \in R$ に対して,
  - (iv) $(a + b) * c = a * c + b * c$ が成り立つ.

▶ $a \in R$ の $+$ に関する逆元を $-a$ と書くことにする.

▶ すべての $a \in R$ に対し，$0 * a = 0$ である.
[$0 * a = (0 + 0) * a = 0 * a + 0 * a$ この両辺に $-(0 * a)$ を足せば $0 * a = 0$ が得られる．]

▶ すべての $a \in R$ に対し，$(-1) * a = -a$ である．[$(-1) * a + a = (-1) * a + 1 * a = (-1 + 1) * a = 0 * a = 0$]

環 (4/4)

▶ 集合 R と R 上の二項演算 $+, *$ の組が **環** であるとは，次の条件が満たされることである:

- ▷ $(R, +)$ は アーベル群 である（$+$ に関する単位元を 0 であらわす）.
- ▷ $(R, *)$ は 結合律と 可換性 を満たし，単位元 を持つ．つまり，ある R の要素 1 があって，すべての $a, b, c \in R$ に対し，
  - (i) $a * (b * c) = (a * b) * c$,
  - (ii) $a * b = b * a$,
  - (iii) $1 * a = a$ が成り立つ.
- ▷ $+$ と $*$ に対して 分配律 が成り立つ．つまり，すべての $a, b, c \in R$ に対して，
  - (iv) $(a + b) * c = a * c + b * c$ が成り立つ.

▶ $(-1) * (-1) = 1$ である．$[(-1) * (-1) + (-1) = (-1) * (-1) + 1 * (-1) = (-1 + 1) * (-1) = 0 * (-1) = 0]$

▶ すべての $a, b \in R$ に対して，$(-a) * (-b) = a * b$ である．$[(-a) * (-b) = (-1) * a * (-1) * b = ((-1) * (-1)) * a * b = 1 * a * b = a * b]$

環 (4/4)

▶ 集合 R と R 上の二項演算 $+, *$ の組が **環** であるとは，次の条件が満たされることである:

- ▷ $(R, +)$ は アーベル群 である（$+$ に関する単位元を 0 であらわす）.
- ▷ $(R, *)$ は 結合律と 可換性 を満たし，単位元 を持つ．つまり，ある R の要素 1 があって，すべての $a, b, c \in R$ に対し，
  - (i) $a * (b * c) = (a * b) * c$,
  - (ii) $a * b = b * a$,
  - (iii) $1 * a = a$ が成り立つ.
- ▷ $+$ と $*$ に対して 分配律 が成り立つ．つまり，すべての $a, b, c \in R$ に対して，
  - (iv) $(a + b) * c = a * c + b * c$ が成り立つ.

▶ $(-1) * (-1) = 1$ である．$[(-1) * (-1) + (-1) = (-1) * (-1) + 1 * (-1) = (-1 + 1) * (-1) = 0 * (-1) = 0]$

▶ すべての $a, b \in R$ に対して，$(-a) * (-b) = a * b$ である．$[(-a) * (-b) = (-1) * a * (-1) * b = ((-1) * (-1)) * a * b = 1 * a * b = a * b]$

環 (4/4)

▶ 集合 R と R 上の二項演算 $+, *$ の組が **環** であるとは，次の条件が満たされることである:

- ▷ $(R, +)$ は アーベル群 である（$+$ に関する単位元を 0 であらわす）.
- ▷ $(R, *)$ は 結合律と 可換性 を満たし，単位元 を持つ．つまり，ある R の要素 1 があって，すべての $a, b, c \in R$ に対し，
  - (i) $a * (b * c) = (a * b) * c$,
  - (ii) $a * b = b * a$,
  - (iii) $1 * a = a$ が成り立つ.
- ▷ $+$ と $*$ に対して 分配律 が成り立つ．つまり，すべての $a, b, c \in R$ に対して，
  - (iv) $(a + b) * c = a * c + b * c$ が成り立つ.

▶ $(-1) * (-1) = 1$ である．$[(-1) * (-1) + (-1) = (-1) * (-1) + 1 * (-1) = (-1 + 1) * (-1) = 0 * (-1) = 0]$

▶ すべての $a, b \in R$ に対して，$(-a) * (-b) = a * b$ である．$[(-a) * (-b) = (-1) * a * (-1) * b = ((-1) * (-1)) * a * b = 1 * a * b = a * b]$

環 (4/4)

▶ 集合 R と R 上の二項演算 $+, *$ の組が **環** であるとは，次の条件が満たされることである:

- ▷ $(R, +)$ は アーベル群 である（$+$ に関する単位元を 0 であらわす）.
- ▷ $(R, *)$ は 結合律と 可換性 を満たし，単位元 を持つ．つまり，ある R の要素 1 があって，すべての $a, b, c \in R$ に対し，
  - (i) $a * (b * c) = (a * b) * c$,
  - (ii) $a * b = b * a$,
  - (iii) $1 * a = a$ が成り立つ.
- ▷ $+$ と $*$ に対して 分配律 が成り立つ．つまり，すべての $a, b, c \in R$ に対して，
  - (iv) $(a + b) * c = a * c + b * c$ が成り立つ.

▶ $(-1) * (-1) = 1$ である．$[(-1) * (-1) + (-1) = (-1) * (-1) + 1 * (-1) = (-1 + 1) * (-1) = 0 * (-1) = 0]$

▶ すべての $a, b \in R$ に対して，$(-a) * (-b) = a * b$ である．$[(-a) * (-b) = (-1) * a * (-1) * b = ((-1) * (-1)) * a * b = 1 * a * b = a * b]$

環の例

- $\mathbb{N}$ は足し算とかけ算を 2 つの演算としてみたとき環でない（演習）.

- $\mathbb{Z}$ や $\mathbb{Q}$ や $\mathbb{R}$ は足し算とかけ算を 2 つの演算として環である.

- マイナスの数とマイナスの数をかけるとプラスの数になることの説明: $\mathbb{R}$ は環になっている，あるいは環になるように構成されているから.

- $\mathbb{Q}[X]$ で，変数 X を持つ $\mathbb{Q}$ 上の多項式全体を考える．たとえば，$2X^4 + \frac{2}{5}X - \frac{4}{15}$ は $\mathbb{Q}[X]$ の要素である．$\mathbb{Q}$ の要素も 0 次の多項式と考えて $\mathbb{Q}[X]$ の要素とする.

  $\mathbb{Q}[X]$ は多項式の普通の足し算とかけ算により環になる．$\mathbb{Z}[X]$, $\mathbb{R}[X]$ も同様.

- $n \in \mathbb{N}$, $n > 0$ として，$\mathbb{Z}_n$ は $\mod n$ に関する足し算とかけ算により環になる．$\mathbb{Z}_n$ の要素のすべては，$0, 1, \ldots, n-1$ の同値類である.

環の例

- $\mathbb{N}$ は足し算とかけ算を 2 つの演算としてみたとき環でない（演習）.

- $\mathbb{Z}$ や $\mathbb{Q}$ や $\mathbb{R}$ は足し算とかけ算を 2 つの演算として環である.

- マイナスの数とマイナスの数をかけるとプラスの数になることの説明: $\mathbb{R}$ は環になっている，あるいは環になるように構成されているから.

- $\mathbb{Q}[X]$ で，変数 X を持つ $\mathbb{Q}$ 上の多項式全体を考える．たとえば，$2X^4 + \frac{2}{5}X - \frac{4}{15}$ は $\mathbb{Q}[X]$ の要素である．$\mathbb{Q}$ の要素も 0 次の多項式と考えて $\mathbb{Q}[X]$ の要素とする.

  $\mathbb{Q}[X]$ は多項式の普通の足し算とかけ算により環になる．$\mathbb{Z}[X]$, $\mathbb{R}[X]$ も同様.

- $n \in \mathbb{N}$, $n > 0$ として，$\mathbb{Z}_n$ は $\mod n$ に関する足し算とかけ算により環になる．$\mathbb{Z}_n$ の要素のすべては，$0, 1, \ldots, n-1$ の同値類である.

環の例

- $\mathbb{N}$ は足し算とかけ算を 2 つの演算としてみたとき環でない（演習）.

- $\mathbb{Z}$ や $\mathbb{Q}$ や $\mathbb{R}$ は足し算とかけ算を 2 つの演算として環である.

- マイナスの数とマイナスの数をかけるとプラスの数になることの説明: $\mathbb{R}$ は環になっている，あるいは環になるように構成されているから.

- $\mathbb{Q}[X]$ で，変数 X を持つ $\mathbb{Q}$ 上の多項式全体を考える．たとえば，$2X^4 + \frac{2}{5}X - \frac{4}{15}$ は $\mathbb{Q}[X]$ の要素である．$\mathbb{Q}$ の要素も 0 次の多項式と考えて $\mathbb{Q}[X]$ の要素とする.

  $\mathbb{Q}[X]$ は多項式の普通の足し算とかけ算により環になる．$\mathbb{Z}[X]$, $\mathbb{R}[X]$ も同様.

- $n \in \mathbb{N}$, $n > 0$ として，$\mathbb{Z}_n$ は $\mod n$ に関する足し算とかけ算により環になる．$\mathbb{Z}_n$ の要素のすべては，$0, 1, \ldots, n-1$ の同値類である.

環の例

- $\mathbb{N}$ は足し算とかけ算を 2 つの演算としてみたとき環でない（演習）.

- $\mathbb{Z}$ や $\mathbb{Q}$ や $\mathbb{R}$ は足し算とかけ算を 2 つの演算として環である.

- マイナスの数とマイナスの数をかけるとプラスの数になることの説明: $\mathbb{R}$ は環になっている，あるいは環になるように構成されているから.

- $\mathbb{Q}[X]$ で，変数 X を持つ $\mathbb{Q}$ 上の多項式全体を考える．たとえば，$2X^4 + \frac{2}{5}X - \frac{4}{15}$ は $\mathbb{Q}[X]$ の要素である．$\mathbb{Q}$ の要素も 0 次の多項式と考えて $\mathbb{Q}[X]$ の要素とする.

  $\mathbb{Q}[X]$ は多項式の普通の足し算とかけ算により環になる．$\mathbb{Z}[X]$, $\mathbb{R}[X]$ も同様.

- $n \in \mathbb{N}$, $n > 0$ として，$\mathbb{Z}_n$ は $\mod n$ に関する足し算とかけ算により環になる．$\mathbb{Z}_n$ の要素のすべては，$0, 1, \ldots, n-1$ の同値類である.

環の例

- $\mathbb{N}$ は足し算とかけ算を 2 つの演算としてみたとき環でない（演習）.

- $\mathbb{Z}$ や $\mathbb{Q}$ や $\mathbb{R}$ は足し算とかけ算を 2 つの演算として環である.

- マイナスの数とマイナスの数をかけるとプラスの数になることの説明: $\mathbb{R}$ は環になっている，あるいは環になるように構成されているから.

- $\mathbb{Q}[X]$ で，変数 X を持つ $\mathbb{Q}$ 上の多項式全体を考える．たとえば，$2X^4 + \frac{2}{5}X - \frac{4}{15}$ は $\mathbb{Q}[X]$ の要素である．$\mathbb{Q}$ の要素も 0 次の多項式と考えて $\mathbb{Q}[X]$ の要素とする.

  $\mathbb{Q}[X]$ は多項式の普通の足し算とかけ算により環になる．$\mathbb{Z}[X]$, $\mathbb{R}[X]$ も同様.

- $n \in \mathbb{N}$, $n > 0$ として，$\mathbb{Z}_n$ は $\mod n$ に関する足し算とかけ算により環になる．$\mathbb{Z}_n$ の要素のすべては，$0, 1, \ldots, n-1$ の同値類である.

環の例

- $\mathbb{N}$ は足し算とかけ算を 2 つの演算としてみたとき環でない（演習）.

- $\mathbb{Z}$ や $\mathbb{Q}$ や $\mathbb{R}$ は足し算とかけ算を 2 つの演算として環である.

- マイナスの数とマイナスの数をかけるとプラスの数になることの説明: $\mathbb{R}$ は環になっている，あるいは環になるように構成されているから.

- $\mathbb{Q}[X]$ で，変数 X を持つ $\mathbb{Q}$ 上の多項式全体を考える．たとえば，$2X^4 + \frac{2}{5}X - \frac{4}{15}$ は $\mathbb{Q}[X]$ の要素である．$\mathbb{Q}$ の要素も 0 次の多項式と考えて $\mathbb{Q}[X]$ の要素とする.

  $\mathbb{Q}[X]$ は多項式の普通の足し算とかけ算により環になる．$\mathbb{Z}[X]$, $\mathbb{R}[X]$ も同様.

- $n \in \mathbb{N}$, $n > 0$ として，$\mathbb{Z}_n$ は $\mod n$ に関する足し算とかけ算により環になる．$\mathbb{Z}_n$ の要素のすべては，$0, 1, \ldots, n-1$ の同値類である.

環の例

- $\mathbb{N}$ は足し算とかけ算を 2 つの演算としてみたとき環でない（演習）.

- $\mathbb{Z}$ や $\mathbb{Q}$ や $\mathbb{R}$ は足し算とかけ算を 2 つの演算として環である.

- マイナスの数とマイナスの数をかけるとプラスの数になることの説明: $\mathbb{R}$ は環になっている，あるいは環になるように構成されているから.

- $\mathbb{Q}[X]$ で，変数 X を持つ $\mathbb{Q}$ 上の多項式全体を考える．たとえば，$2X^4 + \frac{2}{5}X - \frac{4}{15}$ は $\mathbb{Q}[X]$ の要素である．$\mathbb{Q}$ の要素も 0 次の多項式と考えて $\mathbb{Q}[X]$ の要素とする.

  $\mathbb{Q}[X]$ は多項式の普通の足し算とかけ算により環になる．$\mathbb{Z}[X]$, $\mathbb{R}[X]$ も同様.

- $n \in \mathbb{N}$, $n > 0$ として，$\mathbb{Z}_n$ は $\mod n$ に関する足し算とかけ算により環になる．$\mathbb{Z}_n$ の要素のすべては，$0, 1, \ldots, n-1$ の同値類である.

環の例

- $\mathbb{N}$ は足し算とかけ算を 2 つの演算としてみたとき環でない（演習）.

- $\mathbb{Z}$ や $\mathbb{Q}$ や $\mathbb{R}$ は足し算とかけ算を 2 つの演算として環である.

- マイナスの数とマイナスの数をかけるとプラスの数になることの説明: $\mathbb{R}$ は環になっている，あるいは環になるように構成されているから.

- $\mathbb{Q}[X]$ で，変数 X を持つ $\mathbb{Q}$ 上の多項式全体を考える．たとえば，$2X^4 + \frac{2}{5}X - \frac{4}{15}$ は $\mathbb{Q}[X]$ の要素である．$\mathbb{Q}$ の要素も 0 次の多項式と考えて $\mathbb{Q}[X]$ の要素とする.

  $\mathbb{Q}[X]$ は多項式の普通の足し算とかけ算により環になる．$\mathbb{Z}[X]$, $\mathbb{R}[X]$ も同様.

- $n \in \mathbb{N}$, $n > 0$ として，$\mathbb{Z}_n$ は $\mod n$ に関する足し算とかけ算により環になる．$\mathbb{Z}_n$ の要素のすべては，$0, 1, \ldots, n-1$ の同値類である.

環の例

- $\mathbb{N}$ は足し算とかけ算を 2 つの演算としてみたとき環でない（演習）.

- $\mathbb{Z}$ や $\mathbb{Q}$ や $\mathbb{R}$ は足し算とかけ算を 2 つの演算として環である.

- マイナスの数とマイナスの数をかけるとプラスの数になることの説明: $\mathbb{R}$ は環になっている，あるいは環になるように構成されているから.

- $\mathbb{Q}[X]$ で，変数 X を持つ $\mathbb{Q}$ 上の多項式全体を考える．たとえば，$2X^4 + \frac{2}{5}X - \frac{4}{15}$ は $\mathbb{Q}[X]$ の要素である．$\mathbb{Q}$ の要素も 0 次の多項式と考えて $\mathbb{Q}[X]$ の要素とする.

  $\mathbb{Q}[X]$ は多項式の普通の足し算とかけ算により環になる．$\mathbb{Z}[X]$, $\mathbb{R}[X]$ も同様.

- $n \in \mathbb{N}$, $n > 0$ として，$\mathbb{Z}_n$ は $\mod n$ に関する足し算とかけ算により環になる．$\mathbb{Z}_n$ の要素のすべては，$0, 1, \ldots, n-1$ の同値類である.

環の例

- $\mathbb{N}$ は足し算とかけ算を 2 つの演算としてみたとき環でない（演習）.

- $\mathbb{Z}$ や $\mathbb{Q}$ や $\mathbb{R}$ は足し算とかけ算を 2 つの演算として環である.

- マイナスの数とマイナスの数をかけるとプラスの数になることの説明: $\mathbb{R}$ は環になっている，あるいは環になるように構成されているから.

- $\mathbb{Q}[X]$ で，変数 X を持つ $\mathbb{Q}$ 上の多項式全体を考える．たとえば，$2X^4 + \frac{2}{5}X - \frac{4}{15}$ は $\mathbb{Q}[X]$ の要素である．$\mathbb{Q}$ の要素も 0 次の多項式と考えて $\mathbb{Q}[X]$ の要素とする.

  $\mathbb{Q}[X]$ は多項式の普通の足し算とかけ算により環になる．$\mathbb{Z}[X]$, $\mathbb{R}[X]$ も同様.

- $n \in \mathbb{N}$, $n > 0$ として，$\mathbb{Z}_n$ は $\mod n$ に関する足し算とかけ算により環になる．$\mathbb{Z}_n$ の要素のすべては，$0, 1, \ldots, n-1$ の同値類である.

体（たい）

- 環 $(R, +, *)$ が，条件
  - $(R \setminus \{0\}, *)$ は群である

を満たすとき，$(R, +, *)$ は **体 (たい，field; 独:Körper)** であるという．

- $(R, +, *)$ が体のとき，群の単位元の一意性の証明から，$*$ の単位元 1 は，$(R \setminus \{0\}, *)$ の群としての単位元でもある．

- $\mathbb{Q}, \mathbb{R}$ は，足し算とかけ算を 2 つの演算として体である．$\mathbb{Z}$ は足し算とかけ算に関して体ではない（演習）．

- $\mathbb{Z}_n$ が体になるのは，n が素数であるときである．
- 上の主張の証明には，次の初等数論の定理を用いる:

> n と m を互いに素な正の自然数とする（つまり，n と m の最大公約数は 1 とする）．このとき，$u, v \in \mathbb{Z}$ で，$un + vm = 1$ となるようなものが存在する．

体（たい）

- 環 $(R, +, *)$ が，条件
  - $(R \setminus \{0\}, *)$ は群である

を満たすとき，$(R, +, *)$ は **体 (たい，field; 独:Körper)** であるという．

- $(R, +, *)$ が体のとき，群の単位元の一意性の証明から，$*$ の単位元 1 は，$(R \setminus \{0\}, *)$ の群としての単位元でもある．

- $\mathbb{Q}, \mathbb{R}$ は，足し算とかけ算を 2 つの演算として体である．$\mathbb{Z}$ は足し算とかけ算に関して体ではない（演習）．

- $\mathbb{Z}_n$ が体になるのは，n が素数であるときである．
- 上の主張の証明には，次の初等数論の定理を用いる:

> n と m を互いに素な正の自然数とする（つまり，n と m の最大公約数は 1 とする）．このとき，$u, v \in \mathbb{Z}$ で，$un + vm = 1$ となるようなものが存在する．

体（たい）

- 環 $(R, +, *)$ が，条件
  - $(R \setminus \{0\}, *)$ は群である

を満たすとき，$(R, +, *)$ は **体 (たい，field; 独:Körper)** であるという．

- $(R, +, *)$ が体のとき，群の単位元の一意性の証明から，$*$ の単位元 1 は，$(R \setminus \{0\}, *)$ の群としての単位元でもある．

- $\mathbb{Q}$, $\mathbb{R}$ は，足し算とかけ算を 2 つの演算として体である．$\mathbb{Z}$ は足し算とかけ算に関して体ではない（演習）．

- $\mathbb{Z}_n$ が体になるのは，n が素数であるときである．
- 上の主張の証明には，次の初等数論の定理を用いる:

> n と m を互いに素な正の自然数とする（つまり，n と m の最大公約数は 1 とする）．このとき，$u, v \in \mathbb{Z}$ で，$un + vm = 1$ となるようなものが存在する．

体（たい）

- 環 $(R, +, *)$ が，条件
  - $(R \setminus \{0\}, *)$ は群である

を満たすとき，$(R, +, *)$ は **体 (たい，field; 独:Körper)** であるという．

- $(R, +, *)$ が体のとき，群の単位元の一意性の証明から，$*$ の単位元 1 は，$(R \setminus \{0\}, *)$ の群としての単位元でもある．

- $\mathbb{Q}$, $\mathbb{R}$ は，足し算とかけ算を 2 つの演算として体である．$\mathbb{Z}$ は足し算とかけ算に関して体ではない（演習）．

- $\mathbb{Z}_n$ が体になるのは，n が素数であるときである．
- 上の主張の証明には，次の初等数論の定理を用いる:

> n と m を互いに素な正の自然数とする（つまり，n と m の最大公約数は 1 とする）．このとき，$u, v \in \mathbb{Z}$ で，$un + vm = 1$ となるようなものが存在する．

$\mathbb{Z}_p$ と $\mathbb{Q}(X)$

- p を素数とするとき，$\mathbb{Z}_p$ は $0,\ldots,p-1$ の同値類を要素とする要素が有限の体（有限体）となる．

- $\mathbb{Z}_p$ は様々な応用を持つ（数学での応用だけでなく，コンピュータ科学，経済学などでの応用も含む）．

- $\{\frac{f(X)}{g(X)} : f(X),g(X) \in \mathbb{Q}[X],\ g(X) \neq 0\}$ を同値関係 $\frac{f(X)}{g'(X)} \sim \frac{f(X)'}{g'(X)} \Leftrightarrow f(X)g'(X) = f'(X)g(X)$ で割ったときの同値類の全体を $\mathbb{Q}(X)$ とあらわす．$\mathbb{Q}(X)$ には有理数に足し算やかけ算を導入するのと同じやりかたで $\mathbb{Q}[X]$ のかけ算や足し算の拡張を導入することができて，この足し算とかけ算により $\mathbb{Q}(X)$ は体になる．

$\mathbb{Z}_p$ と $\mathbb{Q}(X)$

- p を素数とするとき，$\mathbb{Z}_p$ は $0,\ldots,p-1$ の同値類を要素とする要素が有限の体（有限体）となる．

- $\mathbb{Z}_p$ は様々な応用を持つ（数学での応用だけでなく，コンピュータ科学，経済学などでの応用も含む）．

- $\{\frac{f(X)}{g(X)} : f(X),g(X) \in \mathbb{Q}[X],\ g(X) \neq 0\}$ を同値関係 $\frac{f(X)}{g'(X)} \sim \frac{f(X)'}{g'(X)} \Leftrightarrow f(X)g'(X) = f'(X)g(X)$ で割ったときの同値類の全体を $\mathbb{Q}(X)$ とあらわす．$\mathbb{Q}(X)$ には有理数に足し算やかけ算を導入するのと同じやりかたで $\mathbb{Q}[X]$ のかけ算や足し算の拡張を導入することができて，この足し算とかけ算により $\mathbb{Q}(X)$ は体になる．

$\mathbb{Z}_p$ と $\mathbb{Q}(X)$

- p を素数とするとき，$\mathbb{Z}_p$ は $0,\ldots,p-1$ の同値類を要素とする要素が有限の体（有限体）となる．

- $\mathbb{Z}_p$ は様々な応用を持つ（数学での応用だけでなく，コンピュータ科学，経済学などでの応用も含む）．

- $\{\frac{f(X)}{g(X)} : f(X),g(X) \in \mathbb{Q}[X],\ g(X) \neq 0\}$ を同値関係 $\frac{f(X)}{g'(X)} \sim \frac{f(X)'}{g'(X)} \Leftrightarrow f(X)g'(X) = f'(X)g(X)$ で割ったときの同値類の全体を $\mathbb{Q}(X)$ とあらわす．$\mathbb{Q}(X)$ には有理数に足し算やかけ算を導入するのと同じやりかたで $\mathbb{Q}[X]$ のかけ算や足し算の拡張を導入することができて，この足し算とかけ算により $\mathbb{Q}(X)$ は体になる．

$\mathbb{Z}_p$ と $\mathbb{Q}(X)$

- p を素数とするとき，$\mathbb{Z}_p$ は $0,\ldots,p-1$ の同値類を要素とする要素が有限の体（有限体）となる．

- $\mathbb{Z}_p$ は様々な応用を持つ（数学での応用だけでなく，コンピュータ科学，経済学などでの応用も含む）．

- $\{\frac{f(X)}{g(X)} : f(X),g(X)\in\mathbb{Q}[X],\ g(X)\neq 0\}$ を同値関係 $\frac{f(X)}{g'(X)}\sim\frac{f(X)'}{g'(X)} \Leftrightarrow f(X)g'(X)=f'(X)g(X)$ で割ったときの同値類の全体を $\mathbb{Q}(X)$ とあらわす．$\mathbb{Q}(X)$ には有理数に足し算やかけ算を導入するのと同じやりかたで $\mathbb{Q}[X]$ のかけ算や足し算の拡張を導入することができて，この足し算とかけ算により $\mathbb{Q}(X)$ は体になる．

Vielen Dank für Ihre Aufmerksamkeit!

These slides and their printer friendly version as well as some of the preprints mentioned in the lecture are downloadable from:
http://kurt.scitec.kobe-u.ac.jp/~fuchino/kobe/

アーベル群の復習

- $(R, +)$ がアーベル群であるとは，ある $0 \in R$ があって，

(a1) すべての $x, y, z \in R$ に対し，$(x + y) + z = x + (y + z)$ が成り立つ．（結合法則）

(a2) すべての $x \in R$ に対し，$0 + x = x + 0 = x$ となる．（単位元の存在）

(a3) すべての $x \in R$ に対し，$x + y = y + 1 = 0$ となるような $y \in R$ が存在する．（逆元の存在）

(a4) すべての実数 x, y に対し，$x + y = y + x$ である．（可換性）

- $(R, +)$ が群であるとは，$(R, +)$ が (a1), (a2), (a3) を満たすことだった．
- 可換性 (a4) のもとでは，(a2) と (a3) の条件式は，それぞれ $0 + x = 0$, $x + y = 0$ としても同じである．