離散数学及び演習
講義10　2016. 6.30（木）

多項式
（教科書　pp.151-156）
環
（教科書　pp.157-161）

代数系（algebraic system）

多項式（polynomial）

- 係数a_n, a_{n-1}, …, a_1, $a_0 \in \mathbf{R}$ と変数 $x \in \mathbf{R}$ についての $\mathbf{R}$ 上の（1 変数）多項式
  - $P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$
  - $n=0$ のとき
    $P(x) = a_0$　… 定数多項式（constant polynomial）
  - a_n, a_{n-1}, …, a_1, $a_0 = 0$ のとき
    $P(x) = 0$　… 零多項式（zero polynomial）
  - a_i　… i 次の係数（coefficient）

多項式の次数（degree）

- $\mathbf{R}$ 上の多項式
  $P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$
  の次数 $\deg(P(x))$
  - $a_n \neq 0$ のとき　$\deg(P(x)) = n$
  - $P(x) = 0$ のとき　$\deg(P(x)) = 0$

例：$\deg(5x^3 - x + 1) = 3$
$\deg(a_0) = 0$

- n 次多項式 $P(x)$ $(\neq 0)$ において，$a_n \neq 0$

モニックな多項式（monic polynomial）

- $\mathbf{R}$ 上の n 次多項式 $P(x)$ はモニックである
  - n 次の係数 $a_n = 1$

例：$x^3 - x + 1$

多項式の基本的性質

$\mathbf{R}[x]$：$\mathbf{R}$ 上のすべての 1 変数多項式からなる集合

任意の $P(x)$, $S(x) \in \mathbf{R}[x]$ に対して，

- $P(x) + S(x) \in \mathbf{R}[x]$
- $P(x) - S(x) \in \mathbf{R}[x]$
  - $0 - S(x) = -S(x) \in \mathbf{R}[x]$
- $P(x) \cdot S(x) \in \mathbf{R}[x]$
- 一般に，$P(x) / S(x) \notin \mathbf{R}[x]$
  - $\mathbf{R}[x]$ は加法，減法，乗法について閉じている．
  - $\mathbf{R}[x]$ は除法について閉じていない．
    - 剰余のある除法

除法定理（division theorem）

任意の $P(x)$, $S(x) \in \mathbf{R}[x]$（$P(x) \neq 0$）に対して，
組（$Q(x)$, $R(x)$）$\in \mathbf{R}[x]^2$ が唯一存在して，
$S(x) = Q(x) \cdot P(x) + R(x)$
（ $0 \leq \deg(R(x)) < \deg(P(x))$ ）

- $Q(x)$ … 商（quotient）
- $R(x)$ … 剰余（remainder）

例: $x^3 - x + 1 = (x+2) \cdot (x^2 - 2x + 3) + (-5)$
$3x^4 - 2x^3 + 5x - 7 = (3x^2 + x - 8) \cdot (x^2 - x + 3) + (-6x + 17)$

因数（factor）

$P(x)$, $S(x) \in \mathbf{R}[x]$ に対して，

- $P(x)$ は $S(x)$ の因数（factor）である
  $P(x)$ は $S(x)$ を割り切る（divide）
  （$S(x)$ は $P(x)$ で割り切れる（divisible））
  … $P(x) \mid S(x)$
  - ある $Q(x) \in \mathbf{R}[x]$ が存在して，$S(x) = Q(x) \cdot P(x)$

例:

- $x - 1 \mid x^2 - 1$　　（$x-1$ は x^2-1 の因数）
  - $x^2 - 1 = (x+1)(x-1)$
- 任意の $c \in \mathbf{R} - \{0\}$ に対して，$cx - c \mid x^2 - 1$
  - $x^2 - 1 = (1/c \cdot x + 1/c)(c \cdot x - c)$
  - 一般に，因数 $P(x)$ に対して，$cP(x)$ $(c \in \mathbf{R} - \{0\})$ も因数である．

定理

$P(x)$, $S(x) \in \mathbf{R}[x]$ に対して，
$S(x) \neq 0$ かつ $P(x) \mid S(x)$ ならば，
$\deg(P(x)) \leq \deg(S(x))$

特に，$P(x)$, $S(x) \in \mathbf{R}[x]$ がモニックで，
$P(x) \neq S(x)$ かつ $P(x) \mid S(x)$ ならば，
$\deg(P(x)) < \deg(S(x))$

公因数（共通因数）

$P(x)$, $S(x) \in \mathbf{R}[x]$ に対して，

- $D(x) \in \mathbf{R}[x]$ は $P(x)$, $S(x)$ の公因数（共通因数）（common factor）である
  - $D(x) \mid P(x)$ かつ $D(x) \mid S(x)$．
- $D(x) \in \mathbf{R}[x]$ は $P(x)$, $S(x)$ の最大公因数（最大共通因数）（greatest common factor）である
  … $D(x) = \gcd(P(x), S(x)) = (P(x), S(x))$
  - $D(x)$ は $P(x)$, $S(x)$ のモニックな公因数で，かつ，
    $P(x)$, $S(x)$ の任意の公因数 $D'(x)$ に対して，
    $D'(x) \mid D(x)$ （$D'(x)$ は $D(x)$ の因数）．

例: x^2-1 の因数 : $1, x-1, x+1, x^2-1, c, cx-c, cx+c, cx^2-c$ $(c \neq 0)$
x^3-1 の因数 : $1, x-1, x^2+x+1, x^3-1,$
$c, cx-c, cx^2+cx+c, cx^3-c$ $(c \neq 0)$

- x^2-1 と x^3-1 の公因数 : $1, x-1, c, cx-c$ $(c \neq 0)$
- x^2-1 と x^3-1 の最大公因数 : $x-1$

定理

- 任意の $P(x)$, $S(x) \in \mathbf{R}[x]$ に対して，
  $\gcd(P(x), S(x)) = \gcd(S(x), P(x))$.
- 任意の $P(x)$, $S(x) \in \mathbf{R}[x]$ に対して，
  $\gcd(P(x), 0) = P(x)$.
  特に，$\gcd(0, 0) = 0$.

- モニックな多項式 $P(x)$, $S(x) \in \mathbf{R}[x]$ の最大公因数は
  $P(x)$, $S(x)$ の公因数の中で最大次数である．

互いに素

- $P(x)$, $S(x) \in \mathbf{R}[x]$ は互いに素である
  （relatively prime, coprime）
  - $\gcd(P(x), S(x)) = 1$

定理

任意の $P(x)$, $S(x) \in \mathbf{R}[x]$ に対して,
$X(x)$, $Y(x) \in \mathbf{R}[x]$ が存在して,
$P(x) \cdot X(x) + S(x) \cdot Y(x) = \gcd(P(x), S(x))$.

13

系

任意の $P(x)$, $S(x)$, $T(x) \in \mathbf{R}[x]$ に対して,
$\gcd(P(x), S(x)) = 1$ かつ $P(x) \mid S(x) \cdot T(x)$ ならば,
$P(x) \mid T(x)$.

14

定理（Euclid の互除法の原理）

任意の $P(x)$, $Q(x)$, $R(x)$, $S(x) \in \mathbf{R}[x]$に対して,
$S(x) = Q(x) \cdot P(x) + R(x)$ ならば,
$\gcd(S(x), P(x)) = \gcd(P(x), R(x))$.

例: $\gcd(x^4+x^3+3x^2+2x+2,\ x^3-2x^2-2x-3)$
$= \gcd(x^3-2x^2-2x-3,\ 11(x^2+x+1))$
- $x^4+x^3+3x^2+2x+2 = (x+3)(x^3-2x^2-2x-3)+11(x^2+x+1)$

$= \gcd(x^3-2x^2-2x-3,\ x^2+x+1)$
$= \gcd(x^2+x+1,\ 0)$
- $x^3-2x^2-2x-3 = (x-3)(x^2+x+1)$

$= x^2+x+1$

15

既約多項式（reduced polynomial）

$P(x) \in \mathbf{R}[x]$ は既約多項式である
- $P(x)$ はモニックであり，かつ，そのモニックな因数は
  1 と $P(x)$だけである

例: $x+c$
x^2+1, x^2+x+1, x^2-x+1
- 一般に，$b^2-4c<0$ のとき，x^2+bx+c は既約多項式.

16

定理

$S(x) \in \mathbf{R}[x]$, $\deg(S(x)) \geq 1$ ならば,
既約多項式 $P(x) \in \mathbf{R}[x]$ が存在して,
$\deg(P(x)) \leq \deg(S(x))$ かつ $P(x) \mid S(x)$.

17

定理

既約多項式は無限に存在する.

18

定理

任意の $S(x)$, $T(x) \in \mathbf{R}[x]$ と任意の既約多項式 $P(x) \in \mathbf{R}[x]$ に対して, $P(x) \mid S(x) \cdot T(x)$ ならば, $P(x) \mid S(x)$ または $P(x) \mid T(x)$.

19

既約因数分解の一意性定理

任意の $P(x) \in \mathbf{R}[x]$ は既約多項式 $D_1(x)$, $D_2(x)$, …, $D_r(x) \in \mathbf{R}[x]$ と $c \in \mathbf{R}$ に対して,

$$P(x) = c \cdot D_1(x) \cdot D_2(x) \cdot \ldots \cdot D_r(x)$$

の形(既約多項式の積の形)で表すことができ, その表現は積の順序を除けば一意である.

例: $2x^6 - 30x^4 - 28x^3 + 72x^2 + 48x - 64$
$= 2 \cdot (x-4) \cdot (x-1)^2 \cdot (x+2)^3$

20

整数と多項式の対応

整数	約数	自然数	素数	絶対値
多項式	因数	モニックな多項式	既約多項式	次数

- 両者に共通な性質がある理由は？
- 他にも共通な性質を示す数学的構造はあるか？
- 本質的に共通な性質は何か？
  - 数学的構造(代数系)の公理化

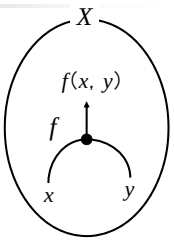
21

2 項演算(binary operator)

- 集合 X 上の 2 項演算 f
  - 関数 $f : X^2 \to X$

例: 加法 $+$: $\mathbf{Z}^2 \to \mathbf{Z}$, $\mathbf{R}[x]^2 \to \mathbf{R}[x]$
乗法 $\cdot$: $\mathbf{Z}^2 \to \mathbf{Z}$, $\mathbf{R}[x]^2 \to \mathbf{R}[x]$

- 関数値 $f(x, y) \in X$ の記法
  - $f(x, y)$ … 前置記法(prefix notation)
    (ポーランド記法(Polish notation))
    例: $+\ 5\ 3$, $\cdot\ P(x)\ S(x)$
  - $x\ f\ y$ … 中置記法(infix notation)
    例: $5+3$, $P(x) \cdot S(x)$
  - $x\ y\ f$ … 後置記法(postfix notation)
    (逆ポーランド記法(reverse Polish notation))
    例: $5\ 3\ +$, $P(x)\ S(x)\ \cdot$
    - 世界初の科学技術計算用電卓 HP-35(1972)
    - プログラミング言語Forth(1971)



22

代数系(algebraic system)

- 代数系
  - 組 $(X, f_1, f_2, \ldots, f_n)$
  - X は集合　… 基礎集合(basic set)
  - $f_i : X^2 \to X$ $(i = 1, 2, \ldots, n)$
    - f_i は X 上の 2 項演算 (X は演算 f_i について閉じている)

例:
- $(\mathbf{Z}, +, \cdot)$
- $(\mathbf{R}[x], +, \cdot)$
- 集合 A に対して, $(\mathbf{P}(A), \cup, \cap)$
- 束 L に対して, $(L, +, \cdot)$
  - $+$ … 結び, $\cdot$ … 交わり
- 演算が明らかなとき … 単に代数系 X

23

環(ring)

- 代数系 $(R, +, \cdot)$ は環である
  - 次の(1)～(7)が成り立つ.

(1) 任意の $x, y, z \in R$ に対して, $x + (y + z) = (x + y) + z$
(加法の結合則(associative law))

(2) $c \in R$ が存在して, 任意の $x \in R$ に対して, $x + c = c + x = x$
(加法の単位元の存在)
- c … 加法の単位元(unit element, identity element)(零元)

c は x と無関係に存在

(3) 任意の $x \in R$ に対して, $y \in R$ が存在して, $x + y = y + x = c$
(加法の逆元の存在)
- $y = -x$ … x の加法の逆元(inverse element)

y は x に依存して存在

(4) 任意の $x, y \in R$ に対して, $x + y = y + x$
(加法の交換則(commutative law))

24

環（続き）

- 代数系$(R, +, \cdot)$は環である
  - 次の(1)～(7)が成り立つ.

(5) 任意の $x, y, z \in R$ に対して, $x\cdot(y\cdot z) = (x\cdot y)\cdot z$
（乗法の結合則(associative law)）

(6) $e \in R$ が存在して, 任意の $x \in R$ に対して, $x\cdot e = e\cdot x = x$
（乗法の単位元の存在）

- e … 乗法の単位元(unit element, identity element)

e は x と無関係に存在

(7) 任意の $x, y, z \in R$ に対して,
$x\cdot(y+z) = (x\cdot y)+(x\cdot z)$,
$(x+y)\cdot z = (x\cdot z)+(y\cdot z)$
（分配則(distributive law)）

- 条件(1)～(7) … 環の公理(axiom)

環（続き2）

- 代数系 R は環である
  - R 上に 2 つの演算(加法, 乗法)が定義されている.
    (2 つの演算は R 上で閉じている)
  - 次の(1)～(7)(環の公理)が成り立つ.

(1) 加法の結合則
(2) 加法の単位元の存在
(3) 加法の逆元の存在
(4) 加法の交換則
(5) 乗法の結合則
(6) 乗法の単位元の存在
(7) 分配則

- 乗法の交換則, 乗法の逆元の存在は必ずしも成り立たない.

環（続き3）

- 環の単位元を明示するとき … $(R, +, \cdot, c, e)$

例:

- $(\mathbf{Z}, +, \cdot, 0, 1)$ … 整数環
- $(\mathbf{Q}, +, \cdot, 0, 1)$ … 有理数環
- $(\mathbf{R}, +, \cdot, 0, 1)$ … 実数環
- $(\mathbf{C}, +, \cdot, 0, 1)$ … 複素数環
- $(\mathbf{R}[x], +, \cdot, 0, 1)$ … 多項式環
- $(\mathbf{Z}[i], +, \cdot, 0, 1)$ … Gauss 整数環
  - $\mathbf{Z}[i] = \{ x+yi \mid x, y \in \mathbf{Z} \}$

可換環（commutative ring）

- 代数系$(R, +, \cdot)$は可換環である
  - $(R, +, \cdot)$は環で, かつ, 次の(8)が成り立つ.

(8) 任意の $x, y \in R$ に対して, $x\cdot y = y\cdot x$
（乗法の交換則(commutative law)）

非可換環（続き）

例: $(M(n), +, \cdot, O, E)$ … 行列環

- $M(n)$: すべての n 次実正方行列からなる集合 $(n \geq 2)$
- $+$: 行列の和, $\cdot$: 行列の積
- $O = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$, $E = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$
- 一般に, $A, B \in M(n)$に対して, $A\cdot B \neq B\cdot A$.

整数を法とする演算

- $p \in \mathbf{Z}$ を法とする
  完全剰余系 $\mathbf{Z}_p = \{0, 1, \ldots, p-1\}$
- $+_p : \mathbf{Z}_p{}^2 \to \mathbf{Z}_p$
  - $x +_p y = \mathrm{mod}(x+y, p)$

例: $2 +_5 4 = 1$

- $\mathrm{mod}(2+4, 5) = 1$

- $\cdot_p : \mathbf{Z}_p{}^2 \to \mathbf{Z}_p$
  - $x \cdot_p y = \mathrm{mod}(x\cdot y, p)$

例: $3 \cdot_5 4 = 2$

- $\mathrm{mod}(3\cdot 4, 5) = 2$

加算表($p=5$)

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

乗算表($p=5$)

$\cdot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

定理

$p \in \mathbf{Z}$ に対して，次の(1)，(2)が成り立つ．

(1)　$x +_p y \equiv x + y \pmod{p}$

(2)　$x \cdot_p y \equiv x \cdot y \pmod{p}$

- 一般に，$+_p$，$\cdot_p$ に関する式 P と，P に現れる $+_p$，$\cdot_p$ をそれぞれ $+$，$\cdot$ で置き換えて得られる式 Q に対して，
  $P \equiv Q \pmod{p}$．

例：$(x +_p y) \cdot_p z \equiv (x+y) \cdot z \pmod{p}$

証明

$p \in \mathbf{Z}$ に対して，

(1)　$x +_p y \equiv x + y \pmod{p}$

(2)　$x \cdot_p y \equiv x \cdot y \pmod{p}$

---

(1)　$x +_p y = \mathrm{mod}(x+y, p)$ だから，$q \in \mathbf{Z}$ が存在して，
$x + y = q \cdot p + (x +_p y)$．
ゆえに，$(x +_p y) - (x + y) = -q \cdot p$
$-q \in \mathbf{Z}$ だから，$x +_p y \equiv x + y \pmod{p}$

定理

$p \in \mathbf{Z}$ に対して，代数系 $(\mathbf{Z}_p, +_p, \cdot_p)$ は可換環である．

証明

$p \in \mathbf{Z}$ に対して，代数系 $(\mathbf{Z}_p, +_p, \cdot_p)$ は可換環である．

- (1)～(8)「可換環の公理が成り立つ」を示す．

---

(1)　加法の結合則は成り立つ

- 「任意の $x, y, z \in \mathbf{Z}_p$ に対して，$(x +_p y) +_p z = x +_p (y +_p z)$」を示す．

任意の $x, y, z \in \mathbf{Z}_p$ に対して，
定理から，$(x +_p y) +_p z \equiv (x+y) + z \pmod{p}$
同様に，$x +_p (y +_p z) \equiv x + (y+z) \pmod{p}$
$(x+y) + z = x + (y+z)$ だから，
$(x +_p y) +_p z \equiv x +_p (y +_p z) \pmod{p}$．
$(x +_p y) +_p z$，$x +_p (y +_p z) \in \mathbf{Z}_p$ だから，
$(x +_p y) +_p z = x +_p (y +_p z)$．

証明（続き）

$p \in \mathbf{Z}$ に対して，代数系 $(\mathbf{Z}_p, +_p, \cdot_p)$ は可換環である．

---

(2)　加法の単位元は存在する

- 「$c \in \mathbf{Z}_p$ が存在して，任意の $x \in \mathbf{Z}_p$ に対して，$x +_p c = c +_p x = x$」を示す．

$0 \in \mathbf{Z}_p$ を考える．
任意の $x \in \mathbf{Z}_p$ に対して，
$x +_p 0 = 0 +_p x = x$ だから，
0 は加法の単位元である．

加算表 $(p=5)$

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

証明（続き2）

$p \in \mathbf{Z}$ に対して，代数系 $(\mathbf{Z}_p, +_p, \cdot_p)$ は可換環である．

---

(3)　加法の逆元は存在する

- 「任意の $x \in \mathbf{Z}_p$ に対して，$y \in \mathbf{Z}_p$ が存在して，$x +_p y = y +_p x = c$」を示す．
- (2)から，$c = 0$．

任意の $x \in \mathbf{Z}_p = \{0, 1, \ldots, p-1\}$ に対して，

$$-x = \begin{cases} p - x & (x \neq 0) \\ 0 & (x = 0) \end{cases}$$

とおくと，$-x \in \mathbf{Z}_p$．
このとき，

$$x +_p (-x) = \begin{cases} \mathrm{mod}(x + (p-x), p) = 0 & (x \neq 0) \\ \mathrm{mod}(0+0, p) = 0 & (x = 0) \end{cases}$$

同様に，$(-x) +_p x = 0$．
ゆえに，$x +_p (-x) = (-x) +_p x = 0$ だから，
x に対して，$-x$ は加法の逆元である．

加算表 $(p=5)$

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

証明（続き3）

$p \in \mathbf{Z}$ に対して，代数系（$\mathbf{Z}_p$，$+_p$，$\cdot_p$）は可換環である．

（4） 加法の交換則は成り立つ
- 「任意の $x, y \in \mathbf{Z}_p$ に対して，$x +_p y = y +_p x$ 」を示す．

任意の $x, y \in \mathbf{Z}_p$ に対して，
$x +_p y = \mathrm{mod}(x+y,\ p) = \mathrm{mod}\,(y+x,\ p) = y +_p x$

（5） 乗法の単位元は存在する
- 「$e \in \mathbf{Z}_p$ が存在して，任意の $x \in \mathbf{Z}_p$ に対して，$x \cdot_p e = e \cdot_p x = x$ 」を示す．

$1 \in \mathbf{Z}_p$ を考える．
任意の $x \in \mathbf{Z}_p$ に対して，
$x \cdot_p 1 = 1 \cdot_p x = x$ だから，1 は乗法の単位元である．

（6） 乗法の結合則は成り立つ
加法の結合則と同様に示せる．

証明（続き4）

$p \in \mathbf{Z}$ に対して，代数系（$\mathbf{Z}_p$，$+_p$，$\cdot_p$）は可換環である．

（7） 分配則は成り立つ
- 「任意の $x, y, z \in \mathbf{Z}_p$ に対して，
  $(x +_p y) \cdot_p z = (x \cdot_p z) +_p (y \cdot_p z)$，
  $x \cdot_p (y +_p z) = (x \cdot_p y) +_p (x \cdot_p z)$ 」を示す．

任意の $x, y, z \in \mathbf{Z}_p$ に対して，
定理から，$(x +_p y) \cdot_p z \equiv (x+y) \cdot z \pmod{p}$
同様に，$(x \cdot_p z) +_p (y \cdot_p z) \equiv x \cdot z + y \cdot z \pmod{p}$
$(x+y) \cdot z = x \cdot z + y \cdot z$ だから，
$(x +_p y) \cdot_p z \equiv (x \cdot_p z) +_p (y \cdot_p z) \pmod{p}$．
$(x +_p y) \cdot_p z$，$(x \cdot_p z) +_p (y \cdot_p z) \in \mathbf{Z}_p$ だから，
$(x +_p y) \cdot_p z = (x \cdot_p z) +_p (y \cdot_p z)$．
同様に，$x \cdot_p (y +_p z) = (x \cdot_p y) +_p (x \cdot_p z)$．

証明（続き5）

$p \in \mathbf{Z}$ に対して，代数系（$\mathbf{Z}_p$，$+_p$，$\cdot_p$）は可換環である．

（8） 乗法の交換則は成り立つ
加法の交換則と同様に示せる．

定理

環$(R, +, \cdot)$に対して，次の(1)～(3)が成り立つ．
（1） 加法の単位元は唯一である．
（2） 加法の逆元は唯一である．
（3） 乗法の単位元は唯一である．

証明

環$(R, +, \cdot)$に対して，
（1） 加法の単位元は唯一である．
- 単位元が 2 つあると仮定して，それらが一致することを示す．

$c, c' \in R$ はともに加法の単位元であると仮定する．
c' は加法の単位元だから，任意の $x \in R$ に対して，
$x + c' = c' + x = x$.
ここで，$x = c$ とおくと，$c + c' = c' + c = c$.
また，c は加法の単位元だから，任意の $x \in R$ に対して，
$x + c = c + x = x$.
ここで，$x = c'$ とおくと，$c' + c = c + c' = c'$.
ゆえに，$c = c'$. したがって，加法の単位元は唯一である．

証明（続き）

環$(R, +, \cdot)$に対して，
（2） 加法の逆元は唯一である．
- 逆元が 2 つあると仮定して，それらが一致することを示す．

任意の$x \in R$ に対して，$y, y' \in R$はともに加法の逆元であるとする．
y は加法の逆元だから，$x + y = y + x = c$.
y' は加法の逆元だから，$x + y' = y' + x = c$.
このとき，

$$\begin{aligned} y &= y + c \\ &= y + (x + y') \\ &= (y + x) + y' \quad \text{（加法の結合則）} \\ &= c + y' \\ &= y' \end{aligned}$$

ゆえに，乗法の逆元は唯一である．

定理

環$(R, +, \cdot, c, e)$と任意の$x \in R$に対して，
次の(1)，(2)が成り立つ．
(1)　$c \cdot x = x \cdot c = c$
(2)　$-(-x) = x$

43

証明

環$(R, +, \cdot, c, e)$と任意の$x \in R$に対して，
(1)　$c \cdot x = x \cdot c = c$

$c \cdot x = c \cdot x + c$　（加法の単位元）
$= c \cdot x + (c \cdot x + (-c \cdot x))$　（加法の逆元）
$= (c \cdot x + c \cdot x) + (-c \cdot x)$　（加法の結合則）
$= (c + c) \cdot x + (-c \cdot x)$　（分配則）
$= c \cdot x + (-c \cdot x)$　（加法の単位元）
$= c$　（加法の逆元）
同様に，$x \cdot c = c$を示すことができる．

44

証明(続き)

環$(R, +, \cdot, c, e)$と任意の$x \in R$に対して，
(2)　$-(-x) = x$

$-(-x)$ は $-x$ の加法の逆元である．
一方，$-x$ は x の加法の逆元だから，$x + (-x) = c$.
加法の交換則から，$(-x) + x = c$.
ゆえに，x も $-x$ の加法の逆元である．
ところが，加法の逆元は唯一だから，$-(-x) = x$.

45

まとめ

- 今回の講義
  - 多項式
  - 環
- 次回の講義
  - 環(続き)(教科書　pp.161-163)
  - 群(教科書　pp.168-170)
- 今回の演習
  - 多項式
  - 環

46