# 環の基本

## 1 導入

この講義の核心は、**環とは「加法については可換群、乗法については閉包と結合法則のみ、そして分配法則で二つの演算が結びつく」最小限の構造である**という見方だ。

群は 1 種類の演算を抽象化する。しかし整数では足し算と掛け算が同時に現れ、しかも $a(b+c)=ab+ac$ という分配法則で相互作用する。環はこの相互作用を公理として捉え、整数・多項式・行列を同じ枠組みで扱う。

## 2 用語と定義

### 2.1 環 Ring

集合 $R$ に加法 $+$ と乗法 $\cdot$ が定義されていて、以下を満たすとき $(R,+,\cdot)$ を環という：

1. $(R,+)$ は可換群（加法の閉包・結合・単位元 $0$・逆元 $-a$・可換性）
2. 乗法の閉包性：$a,b\in R \Longrightarrow ab\in R$
3. 乗法の結合法則：$(ab)c=a(bc)$
4. 分配法則：$a(b+c)=ab+ac$、$(a+b)c=ac+bc$

さらに乗法の単位元 $1$ が存在するとき単位元付環（または単純に環）という。$ab=ba$ が常に成立するとき可換環という。

Ring with unity

Commutative ring

### 2.2 零因子と整域 Zero divisor / Integral domain

$a\neq 0$、$b\neq 0$ だが $ab=0$ となる元を零因子という。零因子のない可換環（ただし $1\neq 0$）を整域という。

Zero divisor

Integral domain

**直感**：整域では $ab=0 \Longrightarrow a=0$ または $b=0$ が成立し、「因数が 0 でなければ積は 0 にならない」という自然な性質が保証される。

## 3 方針

1. 加法と乗法の非対称性（加法には逆元あり、乗法には不要）が環の本質であることを確認する
2. 具体例の比較で零因子・整域・体の違いを把握する
3. イデアルと商環が群の正規部分群・剰余群に対応することを確認する

# 4 厳密な説明

## 4.1 1. なぜ加法は可換群で乗法はそうでないのか

整数では $a+b=b+a$ だが、行列の環 $M_n(\mathbb{R})$ では $AB \neq BA$ が一般に成立する。掛け算の可換性を要求しないことで行列も環の一例として取り込める。
また整数では 2 の乗法逆元 $1/2$ は存在しない。乗法に逆元を要求しないことで整数を環として扱える—これを要求すると体になる。

## 4.2 2. 主要な環の比較

| 環 | 可換 | 単位元 | 零因子 | 分類 |
|---|---|---|---|---|
| $\mathbb{Z}$ | ○ | 1 | なし | 整域 |
| $\mathbb{Z}/n\mathbb{Z}$（$n$ 合成数） | ○ | $[1]$ | あり | 環のみ |
| $\mathbb{Z}/p\mathbb{Z}$（$p$ 素数） | ○ | $[1]$ | なし | 体 |
| $\mathbb{R}[x]$（多項式環） | ○ | 1 | なし | 整域 |
| $M_n(\mathbb{R})$（$n \geq 2$） | × | $I$ | あり | 非可換環 |

**$\mathbb{Z}/6\mathbb{Z}$ の零因子の例**：$[2]\cdot[3]=[6]=[0]$ だが $[2]\neq[0]$、$[3]\neq[0]$。原因は $\gcd(2,6)=2\neq 1$ と $\gcd(3,6)=3\neq 1$。素数法では零因子が生じない。

## 4.3 3. 多項式環 $R[x]$

環 $R$ 上の多項式の集合 $R[x]$ も環をなす。$\mathbb{Z}[x]$ では整数係数の多項式が、$\mathbb{Z}/p\mathbb{Z}[x]$ では $\bmod p$ 係数の多項式が扱える。これが代数的符号理論（BCH符号など）の基盤となる。

## 4.4 4. イデアルと商環

$I \subseteq R$ が両側イデアルであるとは：

$$a,b\in I \Longrightarrow a-b\in I,\quad r\in R, a\in I \Longrightarrow ra\in I \text{ かつ } ar\in I$$

Ideal

**例**：$n\mathbb{Z}=\{nk \mid k\in\mathbb{Z}\}$ は $\mathbb{Z}$ のイデアル。
商環 $R/I$ は剰余類の集合に演算を誘導したものであり、$\mathbb{Z}/n\mathbb{Z}$ はその典型例（$I=n\mathbb{Z}$）である。
**対応の整理**：

| 群論 | 環論 |
|---|---|
| 部分群 | 部分環 |
| 正規部分群 | イデアル |
| 剰余群 | 商環 |
| 準同型定理 | 環準同型定理 |

## 4.5 5. 環の準同型

写像 $\varphi : R \to S$ が

$$\varphi(a+b)=\varphi(a)+\varphi(b),\quad \varphi(ab)=\varphi(a)\varphi(b),\quad \varphi(1_R)=1_S$$

を満たすとき環準同型という。$\ker\varphi=\{a\in R\mid \varphi(a)=0\}$ はイデアルになり、第一準同型定理 $R/\ker\varphi\cong \mathrm{Im}\,\varphi$ が成立する。

## 5 見分け方

- 足し算と掛け算の両方が出た → 環として整理
- $ab=0$ だが $a,b\neq 0$ → 零因子あり、整域でない（$n$ が合成数の $\mathbb{Z}/n\mathbb{Z}$）
- 乗法の逆元がすべての非零元に存在する → 体へ進む
- 商環を作りたい → イデアルを探す

## 6 どこまで成り立つか

環は最小限の二演算構造である。乗法の可換性を加えると可換環、零因子がないと整域、さらに乗法逆元が全ての非零元に存在すると体となる。算術の基本定理（素因数分解の一意性）は「主イデアル整域は UFD（一意分解整域）」という一般的事実の特殊例である。

## 7 最終形

$$(R,+,\cdot)\ \text{が[環/かん]} \iff (R,+)\ \text{は[可換群/かかんぐん]},\cdot\ \text{は[閉包/へいほう]+[結合/けつごう],[分配法則/ぶんぱいほうそく]}$$

$$ab=0 \Longrightarrow a=0\ \text{または}\ b=0 \iff \text{[整域/せいいき]([零因子/ぜろいんし]なし)}$$

$$R/\ker\varphi\cong \mathrm{Im}\,\varphi\quad \text{([第一準同型定理/だいいちじゅんどうけいていり])}$$

## 8 一言でいうと

環とは加法の可換群と乗法を分配法則で結んだ構造であり、整数・多項式・行列を統一する—零因子の有無が整域との境界線を引き、イデアルと商環が群の正規部分群・剰余群に完全に対応する。

## 9 関連リンク

→ 講義 群の基本 lecture math abstract-algebra
https://study.bem130.com/lecture/math/abstract-algebra/群の基本-講義/

→ 講義 **体の基本** lecture math abstract-algebra
https://study.bem130.com/lecture/math/abstract-algebra/体の基本-講義/

→ 講義 **準同型の基本** lecture math abstract-algebra
https://study.bem130.com/lecture/math/abstract-algebra/準同型の基本-講義/