代数系まとめ
代数系の定義と『いつもの』

@men_cotton

2024 年 1 月 29 日

定義と例

1　モノイド

1.1　モノイドの定義

3-tuple $(M, \cdot, e)$(ただし、$\cdot : M \times M \to M$, $e \in M$) であって、以下の条件を満たすもの。

- 結合法則
- 単位元の性質

2　群

2.1　群の定義 [1-p.20 2.1.1]

3-tuple $(G, \cdot, e)$(ただし、$\cdot : G \times G \to G$, $e \in G$) であって、以下の条件を満たすもの。

- $(G, \cdot, e)$ はモノイド
- 逆元が任意の元に存在

2.2　群の例

2.2.1　環の加法は可換群 [1-p.21 2.1.4]

例：$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

環 $(R, +, \cdot, 0_R, 1_R)$ に対し、$(R, +, 0_R)$ は可換群。

2.2.2　乗法群 [1-p.21 2.1.5], [1-p.25 2.1.13]

例：$\mathbb{Q} \setminus \{0\}, \mathbb{R} \setminus \{0\}, \mathbb{C} \setminus \{0\}, \mathrm{GL}_n(\mathbb{C})$

環 $(R, +, \cdot, 0_R, 1_R)$ に対し、可逆元（単元）全体の集合 $R^\times$ は、乗法に関して群となる。この $(R^\times, \cdot, 1_R)$ を乗法群という。

2.2.3　n 次対称群 [1-p.24 2.1.11]

n 次の置換全体からなる群 $\mathfrak{S}_n$

2.3　モノイドであって群ではない例

2.3.1　$(\mathbb{Z}, \cdot, 1)$ は群でない [1-p.21 2.1.5]

逆元が必ずしも存在しないから。例えば、$2n = 1$ となる $n \in \mathbb{Z}$ がない。

2.3.2　$(\{0, 1\}, \min, 1)$ は群でない [1-p.68 演習 2.1.1]

逆元が必ずしも存在しないから。例えば、$\min(x, 0) = 1$ となる $x \in \{0, 1\}$ がない。

2.3.3　$(\mathbb{R}, (a, b) \mapsto a + b + ab, 0)$ は群でない [1-p.68 演習 2.1.2]

逆元が必ずしも存在しないから。例えば、$-1+b+(-1)b = 0$ となる $b \in \mathbb{R}$ がない。

3　環

3.1　環の定義 [1-p.25 2.2.1]

5-tuple $(R, +, \cdot, 0_R, 1_R)$（ただし、$+, \cdot : R \times R \to R$, $0_R, 1_R \in R$）であって、以下の条件を満たすもの。

- $(R, +, 0_R)$ は可換群
- $(R, \cdot, 1_R)$ はモノイド
- 分配法則

3.2　環の例 [1-p.27 2.2.4], [2-p.5 1.2.1]

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

$\mathbb{C}[x]$　(変数が x の複素係数多項式)

3.3　環であって可換環でない例 [1-p.27 2.2.4], [2-p.3 1.1.6]

$\mathrm{M}_{n \geq 2}(\mathbb{R})$ (実数成分の正方行列)

$\mathbb{H}$ (4 元数環、4 元数体)

4　整域

4.1　整域の定義 [2-p.6 1.2.5(1)]

$\forall a \in R \setminus \{0\}, \forall b \in R \setminus \{0\}, ab \neq 0$ を満たす可換環 R

4.2　可換環であって整域でない例 [2-p.6 1.2.7]

$\mathbb{Z}/4\mathbb{Z}$　$(\because 2 \cdot 2 \equiv 0 \pmod 4)$

$\mathbb{C}[x]/(x^2) (\because x \cdot x \equiv 0 \pmod{x^2})$（dual number の環という）

5　体

5.1　体の定義

- 0 で割る以外の除算ができる可換環 [1-p.27 2.2.5]
- 非自明なイデアルを持たない可換環 [2-p.21 1.3.34]

5.2　体の例 [1-p.27 2.2.7]

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$

5.3　任意の体は整域 [2-p.6 1.2.6]

$\forall a \in R \setminus \{0\}, ab = 0$ とする。

$ab = 0 \implies a^{-1}ab = a^{-1}0 \implies b = 0$ の成立より、$a \in R \setminus \{0\}, b \in R \setminus \{0\}, ab = 0$ なる a, b はない。

5.4　整域であって体でない例 [1-p.27 2.2.6]

$\mathbb{Z}$　$(\because 0 \neq 1$ かつ $2 \neq 0$ なのに、$1/2 \notin \mathbb{Z})$

6　環上の加群・線形空間

6.1　体 K 上の線形空間の定義 [2-p.92 2.3.1]

4-tuple $(V, +, \cdot, 0_V)$(ただし、$+\colon V\times V \to V,\ \cdot\colon K\times V \to V,\ 0_V \in V$) であって、以下の条件を満たすもの。

- $(V, +, 0_V)$ が可換群
- $(\lambda\mu)v = \lambda(\mu v)$
- $1_K v = v$
- $(\lambda + \mu)v = \lambda v + \mu v$
- $\lambda(v + u) = \lambda v + \lambda u$

条件 2,3 は群の作用に対応している（体 K の V への作用)。条件 4,5 は分配法則に対応している。

6.1.1　左 R 加群の定義

上の定義では体 K を用いていたが、一般の非可換環 R を用いて、$\cdot\colon R \times V \to V$ だったら、左 R 加群である。右加群は $\cdot\colon V \times R \to V$ となる。

R が可換環の場合（特に体)、左でも右でも同じ。

6.2　環上の加群・線形空間の例

6.2.1　$\mathbb{Z}$ 加群 [2-p.93 2.3.3]

$2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}$ は、$\mathbb{Z}$ 加群である。

6.2.2　$\mathbb{C}[x]$ 加群

$\mathbb{C}^n$ は、$\mathbb{C}[x]$ 加群である。ただし、$A \in \mathrm{M}_n(\mathbb{C})$ で、

$$\cdot\colon \mathbb{C}[x] \times C^n \to C^n, \big(f(x), v\big) \mapsto f(A)v$$

である。

6.2.3　微分方程式の解空間

- $f(x), g(x)$ が解ならば $f(x) + g(x)$ も解である（加法について閉じている）
- $f(x)$ が解ならば $a \cdot f(x) (a \in \mathbb{R})$ も解である（実数倍について閉じている）

を満たすなら、その微分方程式の解の集合は、$\mathbb{R}$ 上の線形空間である。

6.2.4　体の準同型写像（特に、包含写像）[2-p.93 2.3.4(1)]

$\tau\colon \mathbb{F} \to \mathbb{F}'$ を用いて、$\cdot\colon \mathbb{F} \times \mathbb{F}' \to \mathbb{F}', (f, f') \mapsto \tau(f)f'$ とする。これによって $\mathbb{F}'$ は $\mathbb{F}$ 上の線形空間となる。

【確認】$(\mathbb{F}', +, 0)$ は（体の加法なので）可換群である。また、

$$\begin{aligned}
\tau(f_2)\tau(f_1)f' &= \tau(f_2 f_1)f' \quad (\because \text{準同型}) \\
\tau(1_{\mathbb{F}})f' &= 1_{\mathbb{F}'}f' \quad (\because \text{準同型}) \\
&= f' \\
\tau(f_2 + f_1)f' &= (\tau(f_2) + \tau(f_1))f' \quad (\because \text{準同型}) \\
&= \tau(f_2)f' + \tau(f_1)f' \quad (\because \mathbb{F}'\text{が環}) \\
\tau(f)(f_1' + f_2') &= \tau(f)f_1' + \tau(f)f_2' \quad (\because \mathbb{F}'\text{が環})
\end{aligned}$$

を満たす。

式変形に関して

1　単位元の一意性 [1-p.23 2.1.10(1)]

モノイドにおいて、$e = e \cdot e' = e'$

2　逆元の一意性 [1-p.23 2.1.10(2)]

群において、$b = b \cdot e = b \cdot (a \cdot b') = (b \cdot a) \cdot b' = e \cdot b' = b'$

3　$(a^{-1})^{-1} = a$ [1-p.23 2.1.10(4)]

$a \cdot a^{-1} = 0 = a^{-1} \cdot a$ を、a^{-1} を主体に考える

4　$a((bc)d) = (ab)(cd)$ [1-p.22 2.1.7]

結合法則より、カッコは要らない。

5　$ab = ac \implies b = c$ [1-p.22 2.1.8(1)]

両辺に左から a^{-1} をかける。

6　$ab = c \implies b = a^{-1}c,\ a = cb^{-1}$ [1-p.22 2.1.8(2)]

両辺に左から a^{-1} や b^{-1} をかける。

7　$(ab)^{-1} = b^{-1}a^{-1}$ [1-p.23 2.1.10(3)]

$(ab)(b^{-1}a^{-1}) = e = (b^{-1}a^{-1})(ab)$

部分代数系

1　部分代数系の定義 [1-p.29 2.3.1, 2.3.2]

「部分集合・演算の制限写像・単位元」であって、もとの構造を保っているもの。

制限写像であるから、演算が閉じていることを確認すればよい（すなわち、積・和・inv について閉じているか)。

2　部分代数系の例

2.1　環

$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{C}[x]$

2.2　可換群 [1-p.56 2.8.2]

$gH = Hg$ を満たすため、必ず正規部分群である。

3　部分代数系 $H \subseteq G$ でも逆元は同じ [1-p.29 2.3.2(3)]

$\forall x \in H, \exists y \in H, yx = e_H = xy$。演算は制限写像であったから、$yx = e_G = xy$ でもある。

準同型・同型

1　群準同型写像の定義 [1-p.40 2.5.1(1)]

写像 $\varphi\colon G_1 \to G_2$ であって、以下の条件を満たすもの。

1. $\varphi(gg') = \varphi(g)\varphi(g')$

2　群準同型写像は以下を満たす

2.1　$\varphi(e_1) = e_2$ [1-p.41 2.5.3(1)]

$\varphi(e_1) = \varphi(e_1 e_1) = \varphi(e_1)\varphi(e_1)$

2.2　$\varphi(g^{-1}) = \varphi(g)^{-1}$ [1-p.41 2.5.3(2)]

$\varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(e_1) = e_2$

3　モノイド準同型写像の定義

写像 $\varphi\colon S \to T$ であって、以下の条件を満たすもの。

1. $\varphi(xy) = \varphi(x)\varphi(y)$
2. $\varphi(1_S) = 1_T$

3.1　条件 2 は必要

$\varphi\colon \mathbb{Z} \to \mathbb{Z}, x \mapsto 0$ は条件 1 を満たすが、2 を満たさない。

4　恒等写像は準同型 [1-p.41 2.5.4]

- $\mathrm{id}(xy) = xy = \mathrm{id}(x)\mathrm{id}(y)$
- $\mathrm{id}(e) = e$

5　準同型写像の合成は準同型 [1-p.43 2.5.11(1)]

- $g \circ f(xy) = g(f(x) \cdot f(y)) = g \circ f(x) \cdot g \circ f(y)$
- $g \circ f(e_R) = g(e_S) = e_T$

6　同型写像の定義 [1-p.40 2.5.1(2)]

準同型写像 $\varphi\colon G_1 \to G_2$ であって、以下の条件を満たすもの。

$\exists \varphi'\colon G_2 \to G_1, \varphi' \circ \varphi = \mathrm{id}_{G_1}$かつ$\varphi \circ \varphi' = \mathrm{id}_{G_2}$

7　準同型写像が全単射なら同型 [1-p.41 2.5.2]

写像 $f\colon R \to S$ が全射かつ単射であるとき、逆写像をもつ。なぜなら、

- 全射より、$\forall x \in S, f^{-1}(\{x\}) \neq \emptyset$
- 単射より、$\forall x \in S, |f^{-1}(\{x\})| \leq 1$

であるため、$x \in S$ と $f^{-1}(x) \in T$ との間に 1 対 1 対応があるからである。

逆写像 $g := f^{-1}$ が準同型写像であることを示す。

$$
\begin{aligned}
g(xy) &= g(f \circ g(x) \cdot f \circ g(y)) \\
&= g(f(g(x) \cdot g(y))) \\
&= g \circ f(g(x) \cdot g(y)) \\
&= g(x) \cdot g(y) \\
g(e) &= e
\end{aligned}
$$

8　同型は「同値関係」

- 「反射律」: id は準同型であり、$\mathrm{id} \circ \mathrm{id} = \mathrm{id}$ より、$R \simeq R$
- 「対称律」:

$$
\begin{aligned}
& R \simeq S \\
\Longrightarrow\ & \exists \varphi\colon R \to S, \exists \varphi'\colon S \to R \\
& \varphi' \circ \varphi = \mathrm{id}_R \text{かつ} \varphi \circ \varphi' = \mathrm{id}_S \\
\Longrightarrow\ & S \simeq R \quad (\varphi' \text{を主体にみる})
\end{aligned}
$$

- 「推移律」:

$$
\begin{aligned}
& R \simeq S \text{ かつ } S \simeq T \\
\Longrightarrow\ & \exists \varphi\colon R \to S, \exists \varphi'\colon S \to R \\
& \exists \psi\colon S \to T, \exists \psi'\colon T \to S \\
& \varphi' \circ \varphi = \mathrm{id}_R \text{かつ} \varphi \circ \varphi' = \mathrm{id}_S \\
& \psi' \circ \psi = \mathrm{id}_S \text{かつ} \psi \circ \psi' = \mathrm{id}_T \\
\Longrightarrow\ & \exists \psi \circ \varphi\colon R \to T, \exists \varphi' \circ \psi'\colon T \to R \\
& (\varphi' \circ \psi') \circ (\psi \circ \varphi) = \mathrm{id}_R \text{かつ} \\
& (\psi \circ \varphi) \circ (\varphi' \circ \psi') = \mathrm{id}_T \\
\Longrightarrow\ & R \simeq T
\end{aligned}
$$

9　自己同型写像は合成に関して群をなす（自己同型群 Aut$G$）[1-p.45 2.5.16]

- 閉じている：自己同型写像 $\varphi, \psi\colon G \to G$ に対し、$\psi \circ \varphi$ は逆写像として $\varphi^{-1} \circ \psi^{-1}$ をもつ。これは準同型。
- 結合法則：写像の結合法則による
- 単位元：id_G
- 逆元：同型写像の定義より、φ が同型なら φ^{-1} も同型。

核 Ker・像 Im

1 可換環の準同型写像 $f\colon R \to R'$

1.1 $\mathrm{Im}\, f$ は R' の部分環 [2-p.14 1.3.10 の後]

加法が部分可換群

- $f(x) + f(y) = f(x+y) \in \mathrm{Im}\, f$

乗法が部分モノイド

- $f(x) \cdot f(y) = f(x \cdot y) \in \mathrm{Im}\, f$
- $1_{R'} = f(1) \in \mathrm{Im}\, f$

1.2 $\mathrm{Ker}\, f$ は R のイデアル [2-p.18 1.3.24]

- $f(0_R) = 0_S$ より、$\mathrm{Ker}\, f \neq \emptyset$
- $f(x+y) = f(x)+f(y) = 0+0 = 0$ より、$x+y \in \mathrm{Ker}\, f$
- $f(ax) = f(a) \cdot f(x) = f(a) \cdot 0 = 0$ より、$ax \in \mathrm{Ker}\, f$

2 群の準同型写像 $f\colon G \to G'$

2.1 $\mathrm{Im}\, f$ は G' の部分群 [1-p.41 2.5.3(3)]

- $f(x) \cdot f(y) = f(x \cdot y) \in \mathrm{Im}\, f$

2.2 $\mathrm{Ker}\, f$ は G の正規部分群 [1-p.56 2.8.3]

$h \in \mathrm{Ker}\, f$ として、

$g' \in g(\mathrm{Ker}\, f) \iff \exists h, g' = gh \iff \exists h, f(g') = f(g)f(h) \iff \exists h, f(g') = f(h)f(g) \iff \cdots \iff g' \in (\mathrm{Ker}\, f)g$

3 R 加群の R 準同型写像 $f\colon V \to W$

3.1 $\mathrm{Im}\, f$ は W の R 部分加群 [2-p.150 演習 2.4.2]

2.1 より、加法に関して部分群である。

また、f の準同型性より $rf(x) = f(rx)$ であり、作用に関して閉じている。

3.2 $\mathrm{Ker}\, f$ は V の R 部分加群 [2-p.150 演習 2.4.2]

2.2 より、加法に関して部分群である。

また、f の準同型性より $f(x) = 0 \implies f(rx) = rf(x) = 0$ であり、作用に関して閉じている。

4 $f\colon G_1 \to G_2$ が準同型のとき、f が単射 $\iff \mathrm{Ker}\, f = \{e_1\}$ [1-p.44 2.5.13]

4.1 $\implies$

準同型なので、$f(e_1) = e_2$。単射性より、$\mathrm{Ker}\, f = \{e_1\}$。

4.2 $\impliedby$

対偶を示す。

$$\begin{aligned}
&g \neq g' \text{かつ } f(g) = f(g') \\
\implies &g \neq g' \text{かつ } f(g)f(g^{-1}) = f(g')f(g^{-1}) \\
\implies &g \neq g' \text{かつ } e_2 = f(g'g^{-1}) \\
\implies &\mathrm{Ker}\, f \neq e_1
\end{aligned}$$

商

1 同値類の性質

1.1 $y \in [x] \implies [y] = [x]$ [1-p.48 2.6.8(2)]

$z \in [y] \iff z \sim y, \quad z \in [x] \iff z \sim x$ である。ここで、

$$\begin{aligned}
z \sim y &\implies z \sim y \text{ かつ } y \sim x \quad (\because y \in [x]) \\
&\implies z \sim x \\
z \sim x &\implies z \sim x \text{ かつ } x \sim y \quad (\because y \in [x]) \\
&\implies z \sim y
\end{aligned}$$

より、$z \sim y \iff z \sim x$ であり、$[y] = [x]$ である。

1.2 $[x] \cap [y] \neq \emptyset \implies [x] = [y]$ [1-p.48 2.6.8(3)]

$$\begin{aligned}
[x] \cap [y] \neq \emptyset &\implies \exists z, z \in [x] \text{ かつ } z \in [y] \\
&\implies \exists z, [x] = [z] \text{ かつ } [y] = [z] \\
&\implies [x] = [y]
\end{aligned}$$

2 部分群 $H \subseteq G$ に対し $g \sim g' \overset{\text{def}}{\iff} g^{-1}g' \in H$ は同値関係 [1-p.48 2.6.6]

2.1 例

- 可換環 R、(両側)イデアル I に対し、$-r' + r \in I$
- 可換群 G、正規部分群 N に対し、$g^{-1}g' \in N$
- R 加群 V、R 部分加群 W に対し、$-v' + v \in W$

2.2 証明

- 反射律:$x^{-1}x = e \in H$ より、$x \sim x$
- 対称律:

$$\begin{aligned}
x \sim y &\implies x^{-1}y \in H \implies (x^{-1}y)^{-1} \in H \\
&\implies y^{-1}x \in H \implies y \sim x
\end{aligned}$$

- 推移律:

$$\begin{aligned}
x \sim y \text{ かつ } y \sim z &\implies x^{-1}y \in H \text{ かつ } y^{-1}z \in H \\
&\implies (x^{-1}y)(y^{-1}z) \in H \\
&\implies x^{-1}z \in H \implies x \sim z
\end{aligned}$$

3 群の同値類は C_g は、gH [1-p.52 2.6.17]

3.1 証明

$$\begin{aligned}
g' \in C_g &\iff g \sim g' \iff g' \sim g \iff g'^{-1}g \in H \\
&\iff \exists h \in H, g'^{-1}g = h \\
&\iff \exists h \in H, g' = gh^{-1} \\
&\iff \exists \tilde{h} \in H, g' = g\tilde{h} \quad (\tilde{h} = h^{-1}, h = \tilde{h}^{-1}) \\
&\iff g' \in gH
\end{aligned}$$

3.2 系

- 可換環 $r \pmod{I} = r + I$
- 可換群 $C_g = gN = Ng$
- R 加群 $v \pmod{I} = v + W$

4　商集合 $X/\sim$ の普遍性

任意の集合 Z と任意の写像 $f\colon X \to Z$ について,

$$\forall x_1, x_2 \in X, x_1 \sim x_2 \implies f(x_1) = f(x_2)$$

ならば, $f = \overline{f} \circ p$ となるただ 1 つの写像 $\overline{f}\colon X/\sim \to Z$ が存在する。

$$\begin{tikzcd} X \arrow[r, two heads, "p"] \arrow[dr, "f"'] & X/\sim \arrow[d, dotted, "\exists!\,\overline{f}"] \\ & Z \end{tikzcd}$$

4.1　証明

図式が可換になるようにするには、$\forall x \in X, \overline{f}([x]) = f(x)$ でなければならないから、存在すればただ一つ。

$[x] = [x'] \implies x \sim x' \implies f(x) = f(x')$ より、これは well-defined。

4.2　系

4.2.1　商環の普遍性（イデアル I による同値関係） [2-p.27 1.4.6]

任意の可換環 Z と任意の環準同型写像 $f\colon R \to Z$ について,

$$\forall r_1, r_2 \in R, r_1 \equiv r_2 \pmod{I} \implies f(r_1) = f(r_2)$$

ならば, $f = \overline{f} \circ p$ となるただ 1 つの環準同型写像 $\overline{f}\colon R/I \to Z$ が存在する。

4.2.2　商群の普遍性（正規部分群 N による同値関係） [1-p.66 2.10.5]

任意の群 Z と任意の群準同型写像 $\varphi\colon G \to Z$ について,

$$\forall g_1, g_2 \in G, g_1 \sim g_2 \implies \varphi(g_1) = \varphi(g_2)$$

ならば, $\varphi = \overline{\varphi} \circ \pi$ となるただ 1 つの群準同型写像 $\overline{\varphi}\colon G/N \to Z$ が存在する。

4.2.3　商 R 加群の普遍性（R 部分加群 W による同値関係）

任意の R 加群 Z と任意の R 準同型写像 $f\colon V \to Z$ について,

$$\forall v_1, v_2 \in V, v_1 \equiv v_2 \pmod{W} \implies f(v_1) = f(v_2)$$

ならば, $f = \overline{f} \circ p$ となるただ 1 つの R 準同型写像 $\overline{f}\colon V/W \to Z$ が存在する。

5　商集合の準同型定理

集合 A, B と写像 $h\colon A \to B$ について,

$$a_1 \sim_h a_2 \overset{\text{def}}{\iff} h(a_1) = h(a_2)$$

と定める。このとき、$h = \overline{h} \circ p$ なる $\overline{h}$ は単射である。ゆえに、$\overline{h}\colon A/\sim \to \operatorname{Im} h$ は全単射。

$$\begin{tikzcd} A \arrow[r, two heads, "p"] \arrow[dr, "h"'] & A/\sim \arrow[d, hook, "\exists!\,\overline{h}"] \\ & \operatorname{Im} h \subseteq B \end{tikzcd}$$

5.1　証明

普遍性より、$\overline{h}([a]) = h(a)$。

$\overline{h}([a]) = \overline{h}([a']) \implies h(a) = h(a') \implies a \sim_h a' \implies [a] = [a']$ より、単射である（well-defined のときの議論を逆に辿れる）。

5.2　系（「準同型写像が全単射 $\implies$ 同型」が有用）

5.2.1　可換環の準同型定理 [2-p.25 1.4.3]

$\overline{f}\colon R/\operatorname{Ker} f \to R'$ は単射であり、$R/\operatorname{Ker} f \simeq \operatorname{Im} f$

（$\operatorname{Ker} f$ は R のイデアルであった）

5.2.2　群の準同型定理 [1-p.63 2.10.1]

$\overline{f}\colon G/\operatorname{Ker} f \to G'$ は単射であり、$G/\operatorname{Ker} f \simeq \operatorname{Im} f$

（$\operatorname{Ker} f$ は G の正規部分群であった）

5.2.3　R 加群の準同型定理 [2-p.101 2.4.19(1)]

$\overline{f}\colon V/\operatorname{Ker} f \to W$ は単射であり、$V/\operatorname{Ker} f \simeq \operatorname{Im} f$

（$\operatorname{Ker} f$ は V の R 部分加群であった）

6　商集合の演算は well-defined （例：商環）

$[x] = [x'] \iff x \equiv x' \pmod{I}$ より、$a \equiv b \pmod{I}$、$c \equiv d \pmod{I}$ なる (a, b, c, d) を考える。

6.1　加法 $+\colon R/I \times R/I \to R/I,\ ([x], [y]) \mapsto [x + y]$

$a + c \equiv b + d \pmod{I}$ を示す。

$a - b, c - d \in I$ かつイデアルは加法に関して閉じているので、$(a + c) - (b + d) = (a - b) + (c - d) \in I$ である。

6.2　乗法 $\times\colon R/I \times R/I \to R/I,\ ([x], [y]) \mapsto [x \cdot y]$

$a \cdot c \equiv b \cdot d \pmod{I}$ を示す。

$a - b, c - d \in I$ かつイデアルは加法・定数倍に関して閉じているので、$(a \times c) - (b \times d) = (a - b) \times c + b \times (c - d) \in I$ である。

7　商集合は代数系をなす

先ほどの well-defined な演算に基づき、公理を確認

8　商集合への自然な射影 π は準同型

- $\pi(xy) = [xy] = [x][y] = \pi(x)\pi(y)$
- $\pi(e) = [e]$

直積

1　直積集合は代数系をなす

公理を確認すればよい。

2　直積集合 $X \times Y$ の普遍性

任意の集合 Z と任意の写像 $\alpha\colon Z \to X, \beta\colon Z \to Y$ について，$\alpha = \mathrm{pr}_X \circ f$ かつ $\beta = \mathrm{pr}_Y \circ f$ となるただ 1 つの写像 $f\colon Z \to X \times Y$ が存在する。

$$\begin{tikzcd} & Z \arrow[ddl, "\alpha"'] \arrow[d, dotted, "\exists! f"] \arrow[ddr, "\beta"] & \\ & X \times Y \arrow[dl, "\mathrm{pr}_X"] \arrow[dr, "\mathrm{pr}_Y"'] & \\ X & & Y \end{tikzcd}$$

2.1　証明

図式が可換になるようにするには、$\forall z \in Z, f(z) = (\alpha(z), \beta(z))$ でなければならないから、存在すればただ一つ。これは確かに存在する。

2.2　系

2.2.1　直積環の普遍性 [2-p.102 2.4.24]

任意の可換環 Z と任意の環準同型写像 $\alpha\colon Z \to X, \beta\colon Z \to Y$ について，$\alpha = \mathrm{pr}_X \circ f$ かつ $\beta = \mathrm{pr}_Y \circ f$ となるただ 1 つの環準同型写像 $f\colon Z \to X \times Y$ が存在する。

2.2.2　中国剰余定理 $(n = 2)$ [2-p.32 1.6.2]

$\pi_I\colon R \to R/I, \pi_J\colon R \to R/J$ はともに環準同型だから、普遍性より、$f\colon R \to R/I \times R/J$ は環準同型。

$$\begin{tikzcd} & R \arrow[ddl, "\pi_I"'] \arrow[d, dotted, "\exists! f"] \arrow[ddr, "\pi_J"] & \\ & R/I \times R/J \arrow[dl, "pr_I"] \arrow[dr, "pr_J"'] & \\ R/I & & R/J \end{tikzcd}$$

$I \cap J = \mathrm{Ker}\, f$ である。加えて、I, J が互いに素であることより $R/I \times R/J = \mathrm{Im}\, f$ である。

よって、準同型定理より $\overline{f}\colon R/(I \cap J) \to R/I \times R/J$ は全単射な環準同型写像であり、$R/(I \cap J) \simeq R/I \times R/J$ である。

$$\begin{tikzcd} R \arrow[r, two heads, "p"] \arrow[dr, two heads, "f"'] & R/(I \cap J) = R/\mathrm{Ker}\, f \arrow[d, dotted, "\exists! \overline{f}"] \\ & R/I \times R/J = \mathrm{Im}\, f \end{tikzcd}$$

$I \cap J = IJ$ なので、$R/IJ \simeq R/I \times R/J$（中国剰余定理）である。