現代数学への流れ　第11回

復習　R：環 可換環

部分集合 $I \subset R$ が イデアルであるとは、以下をみたすことを いう。

- $I \subset R$ は 和に関して Rの部分群
- 任意の $r \in R$ と $a \in I$ について　$r \cdot a \in I$ が いえる。

$I, J \subset R$: イデアル

に対して、

$$I + J = \{ a + b \mid a \in I,\ b \in J \}$$

$I \cap J$

$$I \cdot J = \{ a_1 b_1 + \cdots + a_r b_r \mid r \geq 0 \quad a_i \in I \quad b_i \in J \}$$

は イデアル となる。

(:) ・ $I+J$ が イデアル.

$0 = 0+0 \in I+J$

$a+b$, $a'+b' \in I+J$ $\Rightarrow$ $a+b+a'+b' = (a+a')+(b+b') \in I+J$

$a+b \in I+J$ $\Rightarrow$ $-(a+b) = (-a)+(-b) \in I+J$

すり. $I+J$ は 和に関して R の部分群

次に $r \in R$, $a+b \in I+J$ について

$r\cdot(a+b) = ra + rb \in I+J$

$\therefore$ $I+J$ は R の イデアル.

・ $I \cap J$ が イデアル.

$0 \in I$, $0 \in J$ より $0 \in I \cap J$.

$a, b \in I \cap J$ について $a+b \in I$ より $a+b \in J$ なので $a+b \in I \cap J$

$a \in I \cap J$ について $-a \in I$ より $-a \in J$ なので $-a \in I \cap J$.

∴ $I \cap J$ は R の部分群

さらに $r \in R$, $a \in I \cap J$ について $ra \in I$ かつ $ra \in J$ より $ra \in I \cap J$

∴ $I \cap J$ は イデアル.

$I \cdot J$ が イデアル.

$0 \in I \cdot J$

$a_1b_1 + \cdots + a_rb_r$, $a_1'b_1' + \cdots + a_s'b_s'$ を任意の $I \cdot J$ について

$$a_1b_1 + \cdots + a_rb_r + a_1'b_1' + \cdots + a_s'b_s' \in I \cdot J$$

$a_1b_1 + \cdots + a_rb_r \in I \cdot J$ について

$$-(a_1b_1 + \cdots + a_rb_r) = (-a_1)b_1 + \cdots + (-a_r) \cdot b_r \in I \cdot J$$

∴ $I \cdot J$ は R の部分群

さらに $r \in R$ $a_1b_1 + \cdots + a_rb_r \in I \cdot J$ について

$$r \cdot (a_1b_1 + \cdots + a_rb_r) = (ra_1)b_1 + \cdots + (ra_r) \cdot b_r \in I \cdot J$$

$I-J$ も イデアル. //

同様に $I_1, \cdots, I_n \subset R$: イデアルに対して

$$I_1 + \cdots + I_n = \{ a_1 + \cdots + a_n \mid a_i \in I_i \}$$

$$I_1 \cap \cdots \cap I_n$$

$$I_1 \cdot \cdots \cdot I_n = \{ a_{1,1} \cdots a_{n,1} + \cdots + a_{1,r} \cdots a_{n,r} \mid r \geq 0 \quad a_{i,j} \in I_i \}$$

は イデアルになる.

(:) 省略 //

剰余環

R : 可換環 $I \subset R$: イデアル.

Rに以下で同値関係を導入する.

$$x \sim y \iff x - y \in I.$$

このとき, 商集合 $R/\sim$ を R/I と記し,

このときの剰余類は $C(x) = x + I$ であらわした.

そこで R/I 上に以下のような演算を考える.

$$(x+I) + (y+I) = x+y+I$$

$$(x+I) \cdot (y+I) = xy + I$$

このとき, この演算は well-defined.

☺ $x \sim x'$, $y \sim y'$ を取る. このとき,

$$x+y - (x'+y') = (x-x') + (y-y') \in I+I = I$$

$$xy - x'y' = (x-x')y + x'(y-y') \in I+I = I \quad //$$

上記の演算により R/I は可換環になる。

(:) 略 //

$x+I$ を $\bar{x}$ などと表す。

定理1 (準同型定理)

$\phi: R \to S$: 可換環の準同型

このとき、

$$\begin{array}{ccc} \bar{\phi}: & R/\ker(\phi) & \xrightarrow{\cong} \quad \mathrm{Im}(\phi) \\ & \downarrow & \downarrow \\ & \bar{x} & \mapsto \quad \phi(x) \end{array}$$

は well-defined で 同型になる。

(:) . well-defined.

$x \sim x'$ とは $x - x' \in \ker(\phi)$

$\therefore \quad \phi(x - x') = \phi(x) - \phi(x')$

$\phi(x - x') = 0$

$\therefore \quad \phi(x) = \phi(x')$

. $\bar{\phi}$ が同型

$\bar{\phi}$ が全射になることは明らか. 単射でもある.

$\bar{\phi}(\bar{x}) = \bar{\phi}(\bar{x}')$

$\Rightarrow \quad \phi(x) = \phi(x')$

$\Rightarrow \quad \phi(x - x') = 0 \quad \Rightarrow \quad x - x' \in \ker(\phi) \quad \Rightarrow \quad \bar{x} = \bar{x}'$ //

例4

$$\phi : \mathbb{Q}[x,y] \to \mathbb{Q}[t]$$

$$f(x,y) \mapsto f(t^2, t^3)$$

$$\text{im}(\phi) = \mathbb{Q}[t^2, t^3] = \{ f(t^2, t^3) \mid f(x,y) \in \mathbb{Q}[x,y] \}$$

$$\ker(\phi) = (x^3 - y^2)$$

(∵) $f(x,y) \in \ker(\phi)$ について

$$f(x,y) = g(x)(x^3 - y^2) + r_1(x)y + r_0(x)$$

とできる. このとき.

$$0 = f(t^2, t^3) = r_1(t^2)t^3 + r_0(t^2)$$

が偶で $r_1(t^2)t^3$ は t^{2k+1} の項しか含まず $r_0(t^2)$ は t^{2k} の項しか持たないが,

$r_1(t^2)=0 \quad r_0(t^2)=0$

が成立する. $\therefore \quad r_1(x)=0 \quad r_0(x)=0$ が成立.

$f(x,y) = g(x)(x^3-y^2)$

が成立. 以上より $\ker(\phi) \subset (x^3-y^2)$ が成立.

$(x^3-y^2) \subset \ker(\phi)$ は明らか.

$\therefore \quad \ker(\phi) = (x^3-y^2)$ //

よって定理1より

$$\mathbb{C}[x,y]/(x^3-y^2) \cong \mathbb{C}[t^2,t^3]$$

$$\frac{\psi}{f(x,y)} \quad \mapsto \quad f(t^2,t^3)$$

環の直積

$R_1, \cdots, R_n$: 環 可換環

$R = R_1 \times \cdots \times R_n = \{ (r_1, \cdots, r_n) \mid r_i \in R_i \}$

Rに 以下で 演算を定義する.

$(r_1, \cdots, r_n) + (r_1', \cdots, r_n') = (r_1 + r_1', \cdots, r_n + r_n')$

$(r_1, \cdots, r_n) \cdot (r_1', \cdots, r_n') = (r_1 r_1', \cdots, r_n \cdot r_n')$

これにより、 Rは 可換環になる (☺ 略)

単位元は $(1, \cdots, 1)$

中国式剰余定理

定理2 (中国式剰余定理)

R: 可換環　$I, J \subset R$: 行列

I, J が互いに素つまり、$I+J=R$ のとき、

$$R/_{I\cap J} \cong R/_I \times R/_J$$

$$\bar{x} \mapsto (x+I,\ x+J)$$

は well-defined で同型になる。

$$\phi: R \to R/_I \times R/_J$$

$$x \mapsto (x+I,\ x+J)$$

が準同型になることを ok.

ここで、 $\ker(\phi) = I \cap J$ ≠ 明らか.

そこで $\mathrm{im}(\phi) = R/I \times R/J$ を示す.

$I+J = R$ より、 $a \in I$, $b \in J$ が存在して $a+b=1$ とできる.

このとき、 $x(a+by) + I = 1y + I = ay + by + I = y + I$

$x(a+by) + J = xa + J = ax + bx + J = x + J$

となるので、 $\phi(x(a+by)) = (y+I,\ x+J)$ となる.

$\therefore \mathrm{im}(\phi) = R/I \times R/J$

よって 定理 第1 より、 $R/I \cap J \cong R/I \times R/J$.

例 $n, m \in \mathbb{Z}$ について $\gcd(n,m)=1$ ならば.

コールリッドの互除法より. $(n)+(m)=\mathbb{Z}$ が言える.

∴ 定理2より.

$$\mathbb{Z}/(n)\cap(m) \cong \mathbb{Z}/(n) \times \mathbb{Z}/(m)$$

が言え, さらに $\gcd(n,m)=1$ より. $(n)\cdot(m)=(nm)$ となることに

以上より,

$$\mathbb{Z}/(nm) \cong \mathbb{Z}/(n) \times \mathbb{Z}/(m)$$

$$\cup \qquad\qquad \cup$$

$$\bar{x} \quad \mapsto \quad (\bar{a}, \bar{b})$$

となる.

$$\mathbb{Z}/(nm) \cong \mathbb{Z}/(n) \times \mathbb{Z}/(m)$$

$$\downarrow \qquad\qquad \downarrow$$

$$? \longmapsto (x \bmod n,\ y \bmod n)$$

? どうやって求めるか？

ユークリッドの互除法を使って $an + bm = 1$ となる $a, b \in \mathbb{Z}$ を見つける。

ここで $Man + Nbm = z$ とおけば

$$z \bmod n = Nbm \bmod n = Nan + Nbm \bmod n = x \bmod n$$

$$z \bmod m = Man \bmod m = Man + Mbm \bmod m = y \bmod m$$

となる。 ∴ $\mathbb{Z}/(nm) \cong \mathbb{Z}/(n) \times \mathbb{Z}/(m)$

$$\downarrow \qquad\qquad \downarrow$$

$$z \bmod nm \longmapsto (x \bmod n,\ y \bmod m)$$

Q. $n = 11 \quad m = 6$

$$\mathbb{Z}/(66) \cong \mathbb{Z}/(\text{11}) \times \mathbb{Z}/(\text{6})$$

$$7 \longmapsto (3, 4)$$