中国剰余定理

前回主に扱ったこと　商環の普遍性
　　　　　　　　　　準同型定理

recall　R：可換環，$I, J \subseteq R$：ideals について
　　$\exists$（自然な単射環準同型）$R/I\cap J \hookrightarrow (R/I)\times(R/J)$

イデアルの演算　R：可換環，$I, J \subseteq R$：ideals について，以下は ideal である。
（容易に check できる）

左
① $I+J := \{i+j \mid i\in I, j\in J\}$
② $I\cap J$　右
　　（①②：有限個の場合も同様）
③ $IJ := \sum\{ij \mid i\in I, j\in J\}$ $=\{ij$ の有限和$\}$ ← 訂正です
④ $(I:J) := \{r\in R \mid rJ\subseteq I\}$　（ここで $rJ := \{rj \mid j\in J\}$）　商
⑤ $\sqrt{I} := \{r\in R \mid \exists m\geq 1, r^m\in I\}$　ラディカル（根基）

Remark　R の ideal の族 $\{I_\lambda\}_{\lambda\in\Lambda}$ について　$\bigcap_{\lambda\in\Lambda} I_\lambda$ の他に

$$\sum_{\lambda\in\Lambda} I_\lambda := \left\{ \sum_{\lambda\in\Lambda} v_\lambda \;\middle|\; \forall\lambda\in\Lambda, v_\lambda\in I_\lambda \text{ かつ } \#\{\lambda\in\Lambda \mid v_\lambda\neq 0\}<\infty \right\}$$

も R の ideal である。

高々有限コが $v_\lambda\neq 0$

Ex.　$R=\mathbb{Z}$，$a, b\geq 1$ について $I=(a)\ (=a\mathbb{Z})$，$J=(b)$ のとき
① $(a)+(b) = (\gcd(a,b))$
② $(a)\cap(b) = (\mathrm{lcm}(a,b))$
③ $(a)(b) = (ab)$

$\gcd(a,b)\,\mathrm{lcm}(a,b) = ab$

Def R：可換環，$I, J \subseteq R$：ideals が互いに素 $\overset{\text{def}}{\Leftrightarrow} I+J=R$

Remark $K \subseteq R$：ideal について，$K=R \Leftrightarrow 1_R \in K$（前にやった）

より、$I+J=R \Leftrightarrow \exists i \in I\ \exists j \in J$ s.t. $i+j=1_R$

Thm（中国剰余定理）R：可換環，$I, J \subseteq R$：ideals s.t. IとJは互いに素

① $IJ=I \cap J$

② $R/IJ \longrightarrow (R/I) \times (R/J)$ は環同型写像
$[r]_{IJ} \mapsto ([r]_I, [r]_J)$

(:) ① $IJ \subseteq I \cap J$ は明らか。

$IJ \supseteq I \cap J$ を示す：仮定より $\exists i_0 \in I\ \exists j_0 \in J$ s.t. $i_0+j_0=1_R$

$x \in I \cap J$ について，$x = xi_0 + xj_0 \in IJ$

② ①と recall より、$\to$ が全射であることを言えばよい。

$([a]_I, [b]_J) \in (R/I) \times (R/J)$ について，$y = bi_0 + aj_0$ とすると $[y]_I = [a]_I$ $[y]_J = [b]_J$ //

Thm（中国剰余定理）R：可換環，$I_1, \cdots, I_n \subseteq R$：ideals
($\leq \forall i \neq \forall j \leq n$ について I_i と I_j が互いに素 ならば

① $I_1 \cdots I_n = I_1 \cap \cdots \cap I_n$

② $R/I_1 \cdots I_n \longrightarrow (R/I_1) \times \cdots \times (R/I_n)$ は環同型写像
$[r]_{I_1 \cdots I_n} \longmapsto ([r]_{I_1}, \cdots, [r]_{I_n})$

十二 十日

(!) nについての帰納法。$n=1$は明らか。$n=2$はすで前にやった。

① $x_1+y_1=1_R$ $(\exists x_1\in I_1, \exists y_1\in I_n)$ をとる。

$\vdots$

$x_{n-1}+y_{n-1}=1_R$ $(\exists x_{n-1}\in I_{n-1}, \exists y_{n-1}\in I_n)$

$1_R - x_1\cdots x_{n-1} = (x_1+y_1)\cdots(x_{n-1}+y_{n-1}) - x_1\cdots x_{n-1} \in I_n$ なので

$J:=I_1\cdots I_{n-1}$ とすると JとI_nは互いに素。よって $JI_n = J\cap I_n$ //

② $R/JI_n \xrightarrow{\sim} (R/J)\times(R/I_n)$ から従う。 //

Ex. $R=\mathbb{Z}$, $I_1=3\mathbb{Z}$, $I_2=5\mathbb{Z}$, $I_3=7\mathbb{Z}$ とすると

$$\mathbb{Z}/105\mathbb{Z} \xrightarrow{\sim} (\mathbb{Z}/3\mathbb{Z})\times(\mathbb{Z}/5\mathbb{Z})\times(\mathbb{Z}/7\mathbb{Z})$$
$$[r]_{105\mathbb{Z}} \longmapsto ([r]_{3\mathbb{Z}}, [r]_{5\mathbb{Z}}, [r]_{7\mathbb{Z}})$$

これは整数nの3,5,7で割った余りを知ることと，nの$105=3\cdot5\cdot7$の余りを知ることが同じであることを意味する。("百五減算")

Remark $R=\mathbb{Z}[X]$, $I:=(2)$, $J:=(X)$ とすると $I+J=(2,X)\subsetneq\mathbb{Z}[X]$ なので(実際 $f(X),g(X)\in\mathbb{Z}[X]$ をうまく選んで $1=2f(X)+Xg(X)$ とは出来ない)、IとJは互いに素ではない($\mathbb{Z}[X]$のidealとしては)

Remark $A=(a_{ij})_{1\le i,j\le n}\in M_n(\mathbb{Z})$ について，$|\det A| \le \prod_{j=1}^{n}\sqrt{a_{1j}^2+\cdots+a_{nj}^2}$

なので，十分たくさんの素数pについて、$\mathbb{Z}/p\mathbb{Z}$で$\det A$を計算すると，CRTから $\det A\in\mathbb{Z}$ を求めることができる。$\mathbb{Z}/p\mathbb{Z}$は体なので(今からやる)Gauss消法を用いることができる。

極大idealと素ideal

Def R：可換環，$I \subsetneq R$：ideal

① Iが素ideal $\overset{\text{def}}{\Leftrightarrow}$ R/Iが整域

② Iが極大ideal $\overset{\text{def}}{\Leftrightarrow}$ R/Iが体

（あたり前だが，極大idealは素ideal）

Remark R：整域 or 体において，定義より $1_R \neq 0_R$ だったので，

Iが素ideal or 極大ideal $\Rightarrow I \subsetneq R$

prop $I \subsetneq R$：idealが極大ideal $\Leftrightarrow$ $J \subseteq R$が $I \subsetneq J \subseteq R$ なるideal ならば $J = R$

☺($\Leftarrow$) $R/I \ni [r]_I \neq 0_{R/I}$ について，

$J := (r) + I$ はRのidealで，$r \notin I$ より $J = R$。

よって $\exists x \in R, \exists i_0 \in I$ s.t. $rx + i_0 = 1_R$ つまり $[r]_I \cdot [x]_I = 1_{R/I}$

($\Rightarrow$) 対偶を示す。$I \subsetneq J \subsetneq R$ なるidealについて $r \in J \setminus I$ をとる。

$[r]_I \neq 0$ in R/I だが，$\forall x \in R$, $rx \in J$ より，$rx \equiv 1_R \bmod J$

となることはない（そうなら $1_R \in J$ となり，$J = R$ となる）

よって $[r]_I \neq 0$ はR/Iで逆元をもたない。 //

Remark 選択公理を仮定すると，零環でない可換環Rには少なくともひとつ極大idealが存在することを示せる。（Rがネーターなら不要）

Ex $\mathbb{Z}$のidealは (a) に限るのだった $(a \geq 0)$

$(0) = \{0\}$, $(1) = \mathbb{Z}$, $a, b \geq 2$ なら $(a) \subsetneq (b) \Leftrightarrow b < a$ かつ $b \mid a$

なので $\mathbb{Z}$の極大idealは，ぴったり(p)である（pは素数）。