prop $I \subsetneq R$: ideal が素ideal $\iff {}^{\forall}a \in R\ {}^{\forall}b \in R,\ ab \in I \Rightarrow a \in I$ or $b \in I$

Remark $a, b \in \mathbb{Z}_{\geq 1}$, p: 素数 のとき $p \mid ab \Rightarrow p \mid a$ or $p \mid b$

(!) ($\Leftarrow$) 対偶を示す。R/I が整域でなければ、$\exists a \in R\ \exists b \in R$ s.t. $[a]_I \neq 0_{R/I}$ かつ $[b]_I \neq 0_{R/I}$ かつ $[ab]_I = 0_{R/I}$

つまり、$a \notin I$, $b \notin I$, $ab \in I$

($\Rightarrow$) 対偶を示す。上の議論を逆にたどる。//

Def R: 可換環, $\mathrm{Spec}(R) := \{\mathfrak{p} \subsetneq R \mid \mathfrak{p}$ は素ideal$\}$

EX $\mathrm{Spec}(\mathbb{Z}) = \{(0), (p) \mid p$ は素数$\}$, $\mathrm{Spec}(\text{体}) = \{(0)\}$

(n)

$n = ab$

$a, b \geq 2$

prop A, B : 可換環, $f : A \to B$: 環準同型写像について,

${}^{\forall}\mathfrak{q} \in \mathrm{Spec}(B)$, $f^{-1}(\mathfrak{q}) \in \mathrm{Spec}(A)$

(!) $A \xrightarrow{f} B \xrightarrow{\text{自然}} B/\mathfrak{q}$ という合成を h とすると, $\ker h = f^{-1}(\mathfrak{q})$ である。

自然 ↘ $A/f^{-1}(\mathfrak{q})$

よって準同型定理より $A/f^{-1}(\mathfrak{q})$ は $B/\mathfrak{q}$ の部分環と同型

$B/\mathfrak{q}$ は整域なので、$A/f^{-1}(\mathfrak{q})$ も整域である。//

Remark $I \subseteq R$: ideal について $V(I) := \{\mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{p} \supseteq I\}$ とすると,

$\mathrm{Spec}(R)$ は $\{V(I) \mid I \subseteq R$: ideal$\}$ を閉集合系とする位相空間になることが check できる。この位相を Zariski 位相という。

$A \xrightarrow{f} B$: 環準同型について, $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ が well-defined

$\mathfrak{q} \longmapsto f^{-1}(\mathfrak{q})$

だったが、これは Zariski 位相について連続であることも示せる。

Remark $\mathbb{Z} \overset{\iota}{\hookrightarrow} \mathbb{Q}$: 包含環準同型について, $\iota^{-1}((0)) = (0)$ は $\mathbb{Z}$ の素idealだが極大idealではない。

Def R : 整域, $a \neq 0$ in R が素元 $\overset{\text{def}}{\Leftrightarrow}$ $(a) \in \mathrm{Spec}(R)$

Ex $R = \mathbb{Z}$ のとき a が素元 $\Leftrightarrow$ $a = \pm p$ (p は素数)

Ex $\mathbb{Z}[X]$ で $a = 2, X$ はともに素元だが,
$\mathbb{Q}[X]$ で $a = 2$ は $(2) = (1) = \mathbb{Q}[X]$ より素元ではない ($a = X$ は素元)

Ex $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ (Gauss整数環) において,
2は素元ではない。実際, $2 = (1+i)(1-i)$ だが, $1 \pm i \notin (2)$ が分かる。

次回は"素因数分解の一意性"について議論する。

一意分解整域（UFD）

前回主に扱ったこと　中国剰余定理（CRT）
極大idealと素ideal

Def 群とは以下の3つの公理をみたす3つ組$(G,\cdot,e)$のことである。

ここでG：集合，$\cdot: G\times G\to G$：写像（2項演算），$e\in G$：元である。

① $\forall a\in G\ \forall b\in G\ \forall c\in G,\ (a\cdot b)\cdot c = a\cdot(b\cdot c)$　結合

② $\forall a\in G,\ e\cdot a = a = a\cdot e$　単位

③ $\forall a\in G\ \exists b\in G,\ ab = e = ba$　逆元

Remark ・$e'\in G$が$\forall a\in G,\ e'\cdot a = a = a\cdot e'$ならば$e = e'$（環のときと同様）

・③のbも一意的で、a^{-1}と書く。　常識

Remark さらに④をみたすとき，アーベル群，可換群，加群などと呼ぶ。
（このとき，$\cdot$を$+$で、eを0又は0_Gと採用することが多い）

④ $\forall a\in G\ \forall b\in G,\ ab = ba$

Def R：可換環

$R^\times := \{a\in R \mid \exists b\in R\ \ ab = 1_R = ba\}$について$(R^\times, 1_R, \cdot)$は可換群になる

Ex $\mathbb{Z}^\times = \{\pm 1\}$, $\mathbb{Q}^\times = \mathbb{Q}\setminus\{0\}$

$\{0\}^\times = \{0\}$, $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$

$(\mathbb{Z}/12\mathbb{Z})^\times = \{[1]_{12\mathbb{Z}}, [5]_{12\mathbb{Z}}, [7]_{12\mathbb{Z}}, [11]_{12\mathbb{Z}}\}$

記法 R：可換環，$a,b\in R$

$a\mid b \overset{\text{def}}{\Leftrightarrow} \exists c\in R \text{ s.t. } b=ac \left(\Leftrightarrow (b)\subseteq(a)\right)$

Def R：可換環，$a,b\in R$

aとbは同伴である（今回だけ$a\approx b$と書く）$\Leftrightarrow \exists c\in R^\times \text{ s.t. } b=ac$ $\left(\times\frac{1}{c}=a\right)$

Prop ① $\approx$は同値関係である

② R：~~可換環~~ 整域（訂正です），$a,b\in R$ TFAE (A) $a\approx b$

(B) $a\mid b$ かつ $b\mid a$

(C) $(a)=(b)$

以下は全て同値

☺ 容易

Recall R：整域，$a\neq 0_R$が素元 $\overset{\text{def}}{\Leftrightarrow} (a)\in \mathrm{Spec}(R)$ （このとき$a\in R^\times$が従う）

Def R：整域，$a\in R$が既約元 $\overset{\text{def}}{\Leftrightarrow}$ ① $a\neq 0_R$，$a\notin R^\times$

② $\forall b\in R\ \forall c\in R$, $a=bc \Rightarrow b\in R^\times$ or $c\in R^\times$

Prop R：整域，$a\in R$ aが素元 $\Rightarrow$ aが既約元 訂正

☺ ①はOK。②を示すため $a=bc$とする。$bc\in(a)$ より $b\in(a)$ or $c\in(a)$

$b\in(a)$ なら $\exists r\in R$, $b=ar$。つまり $a=arc$ となって $1=rc$ $\therefore c\in R^\times$

$c\in(a)$も同様 //

Ex $\mathbb{Z}[\sqrt{-5}]\left(=\{a+b\sqrt{-5}\mid a,b\in\mathbb{Z}\}\overset{\text{部分環}}{\subseteq}\mathbb{C}\right)$ において 整域

$6=2\cdot 3=(1+\sqrt{-5})(1-\sqrt{-5})$ で，$2,3,1\pm\sqrt{-5}$ のどれも

既約元だが素元でないことがcheckできる。

Def R：整域が一意分解整域（UFD）

$\overset{\text{def}}{\Leftrightarrow} \forall a \in R \quad a \neq 0_R,\ a \notin R^\times \Rightarrow \exists r \geq 1\ \exists p_1, \cdots \exists p_r \in R$：素元 s.t.
$a = p_1 \cdots p_r$

Thm R：UFD, $a \in R$, $a \neq 0_R$, $a \notin R^\times$ が
$a = p_1 \cdots p_r = q_1 \cdots q_s$ のとき $r = s$ で $q_1 \sim q_s$ は適当に並びかえて
$\forall i \leq r$, $p_i \approx q_i$ とできる。（ここで $r, s \geq 1$ で $p_1 \sim p_r$, $q_1 \sim q_s$ は素元）

☺ $r \leq s$ としてよく，r についての帰納法

$r = 1$：$p_1 = q_1 \cdots q_s$ だが、$\exists i$, $p_1 \mid q_i$。並びかえて $i = 1$ としてよい。
$\exists c \in R^\times$, $q_1 = p_1 c$ だが q_1 は既約元でもあるので $c \in R^\times$。よって $p_1 \approx q_1$。
今 $1 = c^{-1} q_2 \cdots q_s$ となるので $s = 1$ でなければならない。

$r \geq 2$：$p_1 \cdots p_r = q_1 \cdots q_s$ で上と同様に $\exists d \in R^\times$, $q_1 = p_1 d$ とできる。
$p_2 p_3 \cdots p_r = d q_2 \cdots q_s$ なので帰納法の仮定から
$r - 1 = s - 1$ かつ $q_2 \sim q_s$ を並びかえて $q_2 \approx d p_2 \approx p_2$
$q_i \approx p_i$ $(i \geq 3)$ //

prop R：PID, $a \in R$ a が素元 $\Leftrightarrow$ a が既約元

☺ ($\Leftarrow$) a を既約元とする。$(0_R) = \{0\} \subsetneq (a) \subsetneq R = (1_R)$ である。
$(a) \subseteq (b)$ $(\text{i.e. } \exists c \in R,\ a = bc)$ とする。
$b \in R^\times$ なら $(b) = R$ で、$c \in R^\times$ なら $(a) = (b)$ となるので
(a) は極大 ideal（特に $(a) \in \operatorname{Spec} R$） //

Lemma R: PID において ideal の昇鎖律 (ACC) が成り立つ。つまり
$I_1 \subseteq I_2 \subseteq \cdots$ が R の ideal ならば $\exists N \geq 1$ s.t. $I_N = I_{N+1} = \cdots$

(:) $J := \bigcup_{i \geq 1} I_i$ が R の ideal であることは簡単に check できる。

$J = (a)$ とできるが、N を $I_N \ni a$ ととると、$J = I_N = I_{N+1} = \cdots$ が分かる。
(実際 $I_N \supseteq J$ である。) //

Remark 上の議論と全く同様に、ネーター環においても ACC が成り立つ。
(普通はこれをネーター環の定義にする)

prop R: PID $\forall a \in R, a \neq 0_R, a \notin R^\times$ $\exists b \in R$: 既約元 s.t. $b \mid a$

(:) a が既約元なら OK ($b = a$ とする)。そうでないとき $a = a'a''$, $a', a'' \notin R^\times$
とできるが、どちらかが既約元なら OK。そうでなければ $a' = a'''a''''$, $a''', a'''' \notin R^\times$
とくり返す。この過程で既約元があらわれなければ
$(a) \subsetneq (a') \subsetneq \cdots$ となるので Lemma に矛盾する //

Thm PID は UFD

(:) R: PID とし $\forall a \in R, a \neq 0_R, a \notin R^\times$ が既約元の積 $a = a_1 \cdots a_r$ になることを示せばよい。prop より $\exists a_1 \in R$: 既約元 s.t. $a_1 \mid a$ ($a = a_1 c$ とする)
$c \notin R^\times$ なら $\exists a_2 \in R$: 既約元 s.t. $a_2 \mid c$ とくり返す ($c = a_2 d$ とする)
この操作が終わらないと $(a) \subsetneq (c) \subsetneq (d) \subsetneq \cdots$ となって Lemma に矛盾。
よって $\exists a_1 \sim \exists a_r$: 既約元 $\exists u \in R^\times$ s.t. $a = a_1 \cdots a_r u$ となる //

Remark $\mathrm{Spec}(\mathbb{Z}) = \{(0), (p) \mid p: \text{素数}\}$ と $\mathbb{Z}^\times = \{\pm 1\}$ より
整数における通常の"素因数分解の一意性"が示された。

Thm R: UFD $\Rightarrow R[X] = \{R\text{係数}1\text{変数多項式}\}$ もUFD

これが言えれば $\mathbb{Z}[X_1, \cdots, X_n]$ でも素因子分解の一意性が
$\mathbb{Q}[X_1, \cdots, X_n]$ 分かる。