$\mathrm{Irr}(p,n) = \left\{ \begin{array}{l} \text{polynômes irréductibles} \\ \text{unitaires de degré } n \\ \text{à coefficients dans } \mathbb{F}_p \end{array} \right\}$

(Théorème 13 du chapitre 4)

p premier $n \geq 1$ entier $X^{p^n} - X$

$n = 1$ $$X^p - X = \prod_{r \mid n} \prod_{P \in \mathrm{Irr}(p,r)} P$$

$$= \prod_{P \in \mathrm{Irr}(p,1)} P \qquad \mathrm{Irr}(p,1) = \{X - \alpha\}_{\alpha \in \mathbb{F}_p}$$

$$= \prod_{\alpha \in \mathbb{F}_p} X - \alpha \qquad = \{X - [k]_p\}_{0 \leq k \leq p-1}$$

$Q = X^p - X$ $\qquad \forall \alpha \in \mathbb{F}_p, \ \alpha^p = \alpha$

donc Q a p racines $\underset{\text{2 à 2 distinctes}}{\wedge}$ dans $\mathbb{F}_p$ et $\deg(Q) = p$

($\mathbb{K}$ corps $Q \in \mathbb{K}[X]$ unitaire avec $\deg(Q) \geq 1$ et Q possède $\deg(Q)$ racines 2 à 2 distinctes dans $\mathbb{K}$, notées $\alpha_1, \ldots, \alpha_{\deg(Q)}$

alors $Q = \prod_{i=1}^{\deg(Q)} (X - \alpha_i)$)

$\mathbb{K}$ corps $P \in \mathbb{K}[X]$

$\varphi_P : \begin{array}{l} \mathbb{K} \longrightarrow \mathbb{K} \\ \alpha \longmapsto P(\alpha) \end{array}$

<u>Remarque</u> : $Q = X^p - X \in \mathbb{F}_p[X]$ $\quad Q \neq 0$

fonction polynômiale associée $\varphi_Q : \begin{array}{l} \mathbb{F}_p \longrightarrow \mathbb{F}_p \\ \alpha \longmapsto Q(\alpha) \end{array}$

φ_Q est la fonction nulle !

$p = 2$ $n = 2$ $$X^{2^2} - X = \prod_{P \in \mathrm{Irr}(2,1)} P \times \prod_{P \in \mathrm{Irr}(2,2)} P$$

$$= X(X - [1]_2) \times \prod_{P \in \mathrm{Irr}(2,2)} P$$

$$\shortparallel$$

$$X^4 - X = X(X^3 - [1]_2) = X(X - [1]_2)(X^2 + X + [1]_2)$$

$$\mathrm{Irr}(2,2) = \{X^2 + X + [1]_2\}$$

LOCALISATION

anneau quotient : on force certains éléments à être nul

anneau localisé : on force certains éléments à être inversibles
⚠ parfois, cela force aussi certains éléments à être nuls

strict minimum : corps des fractions d'un anneau intègre
ambitieux : le localisé d'un anneau par rapport à un idéal premier est un anneau local

① Corps des fractions d'un anneau intègre

$\mathbb{Z} \subset \mathbb{Q}$

$\mathbb{Z}^\times = \{1, -1\}$ $\quad \mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$

"le plus petit corps contenant l'anneau intègre en question"

Construction / Description A anneau intègre
et on connaît un surcorps de A : $A \underset{\text{sous-anneau}}{\subset} \underset{\text{corps}}{\mathbb{K}}$

Exemple $A = \mathbb{Z}[i]$ $\quad \mathbb{K} = \mathbb{C}$

$A = \mathbb{Z}[\sqrt{5}]$ $\quad \mathbb{K} = \mathbb{C}$ $\quad \mathbb{K} = \mathbb{R}$

$\sqrt{5} \notin \mathbb{Q}$

p premier $\quad A = \mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \right\}_{\substack{a \in \mathbb{Z} \\ b \in \mathbb{Z} \setminus p\mathbb{Z}}}$ $\quad \mathbb{K} = \mathbb{C} \quad \mathbb{K} = \mathbb{R} \quad \mathbb{K} = \mathbb{Q}$

$\mathrm{Frac}(A) = \mathbb{Q}$

$$\mathrm{Frac}(A) = \left\{ \frac{a}{b} \right\}_{\substack{a \in A \\ b \in A \setminus \{0\}}} \underset{\text{sous-anneau}}{\subset} \mathbb{K}$$

$b \in A \setminus \{0\}$ donc $b \in \mathbb{K} \setminus \{0\}$ donc $b \in \mathbb{K}^\times$

$\mathrm{Frac}(A)$ est un corps : soit $x \in \mathrm{Frac}(A) \setminus \{0\}$. On écrit $x = \frac{a}{b}$ avec $\substack{a \in A \\ b \in A \setminus \{0\}}$

Comme $x \neq 0$, on a $a \neq 0$. Donc $\frac{b}{a}$ existe et c'est un élément de $\mathrm{Frac}(A)$

donc $\frac{a}{b} \in \mathrm{Frac}(A)^\times$

$$\mathrm{Frac}(A) = \left\{ \frac{a}{b} \right\}_{\substack{a\in A \\ b \in A\setminus\{0\}}} \overset{\text{sous-anneau}}{\subset} \mathbb{K}$$

$b \in A\setminus\{0\}$ donc $b \in \mathbb{K}\setminus\{0\}$ donc $b \in \mathbb{K}^\times$

$\mathrm{Frac}(A)$ est un corps : soit $x \in \mathrm{Frac}(A)\setminus\{0\}$ On écrit $x = \frac{a}{b}$ avec $a\in A$, $b \in A\setminus\{0\}$

Comme $x \neq 0$, on a $a \neq 0$. Donc $\frac{b}{a}$ existe et c'est un élément de $\mathrm{Frac}(A)$

donc $\frac{a}{b} \in \mathrm{Frac}(A)^\times$

On montre : $\mathrm{Frac}(A)$ est le plus petit corps contenant A

c'est-à-dire : Si $\mathbb{L}$ est un surcorps de A, alors $\mathbb{L}$ contient $\mathrm{Frac}(A)$.

On montre : $\mathrm{Frac}(\mathbb{Z}[i]) = \{a + ib\}_{a,b\in\mathbb{Q}}$

$\mathrm{Frac}(\mathbb{Z}[\sqrt{5}]) = \{a + \sqrt{5}.b\}_{a,b\in\mathbb{Q}}$

p premier $\quad \mathrm{Frac}(\mathbb{Z}_{(p)}) = \mathbb{Q} \qquad \mathrm{Frac}(\mathbb{Z}_{(p)}) = \left\{ \frac{a}{b} \right\}_{\substack{a\in \mathbb{Z}_{(p)} \\ b \in \mathbb{Z}_{(p)}\setminus\{0\}}} \subset \mathbb{Q}$

Il suffit de montrer : $\mathbb{Q} \subset \mathrm{Frac}(\mathbb{Z}_{(p)})$

Soit $x \in \mathbb{Q}$, on écrit $x = \frac{a}{b}$ avec $a \in \mathbb{Z}$, $b \in \mathbb{Z}\setminus\{0\}$ en particulier $a \in \mathbb{Z}_{(p)}$ et $b \in \mathbb{Z}_{(p)}\setminus\{0\}$

donc $\frac{a}{b} \in \mathrm{Frac}(\mathbb{Z}_{(p)})$

(cet argument montre la chose suivante : soit A un anneau intègre qui est un sous-anneau de $\mathbb{Q}$ (et qui contient $\mathbb{Z}$ comme sous-anneau) alors $\mathrm{Frac}(A) = \mathbb{Q}$)

<u>Cas où on ne connaît pas de surcorps de A</u> $\quad A = \mathbb{Q}[X]$

($\mathbb{R}[X]$ n'est pas un corps)

On considère V l'ensemble des symboles « $\frac{a}{b}$ » avec $a \in A$ $b \in A\setminus\{0\}$

On met une structure d'anneau sur cet ensemble

$a,b,c,d \in A$, $b,d \in A\setminus\{0\}$ $\quad \frac{a}{b} + \frac{c}{d} \text{ « = » } \frac{ad+bc}{bd}$, $bd \in A\setminus\{0\}$ car A intègre $\qquad \frac{a}{b} \times \frac{c}{d} \text{ « = » } \frac{a\times c}{b\times d} \qquad a \text{ « = » } \frac{a}{1}$

$$\frac{a}{b} = \frac{c}{d} \iff ad = bc$$

$$\mathrm{Frac}(\mathbb{Q}[X]) = \left\{ \frac{P}{Q} \right\}_{\substack{P\in \mathbb{Q}[X] \\ Q \in \mathbb{Q}[X]\setminus\{0\}}}$$

Cas où on ne connaît pas de surcorps de A $A = \mathbb{Q}[X]$

($\mathbb{R}[X]$ n'est pas un corps)

On considère l'ensemble des symboles "$\frac{a}{b}$" avec $a \in A$, $b \in A \setminus \{0\}$

On met une structure d'anneau sur cet ensemble

$a,b,c,d \in A$, $b,d \in A\setminus\{0\}$: $\frac{a}{b} + \frac{c}{d} \text{ "=" } \frac{ad+bc}{bd}$, $bd \in A\setminus\{0\}$ car A intègre

$\frac{a}{b} \times \frac{c}{d} \text{ "=" } \frac{a\times c}{b \times d}$ $a \text{ "=" } \frac{a}{1}$

$\frac{a}{b} = \frac{c}{d} \iff ad = bc$

$\mathrm{Frac}(\mathbb{Q}[X]) = \left\{ \frac{P}{Q} \right\}_{P \in \mathbb{Q}[X],\ Q \in \mathbb{Q}[X]\setminus\{0\}}$

$$\frac{1+X}{1+X^2} + \frac{2+X}{X} = \frac{(1+X)X + (2+X)(1+X^2)}{X(1+X^2)}$$

__Notation__ Si $\mathbb{K}$ est un corps, $\mathrm{Frac}(\mathbb{K}[X])$ est noté $\mathbb{K}(X)$ et s'appelle le corps des fractions rationnelles en une indéterminée à coefficients dans $\mathbb{K}$

Le cas où on inverse certains éléments non nuls d'un anneau intègre (mais pas tous)

p nombre premier

$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \right\}_{a \in \mathbb{Z},\ b \in \mathbb{Z}\setminus p\mathbb{Z}}$ « par rapport à $\mathbb{Z}$, on a rendu inversibles tous les éléments qui ne sont pas multiples de p »

$\mathbb{Z} \subset \mathbb{Z}_{(p)}$ $\mathbb{Z}_{(p)}^\times \cap \mathbb{Z} = \mathbb{Z} \setminus p\mathbb{Z} \supset \mathbb{Z}^\times = \{1,-1\}$

__Formalisme général__ On suppose que $A \subset \mathbb{K}$ (A anneau intègre, $\mathbb{K}$ corps)

et on veut « rendre inversibles » les éléments d'une partie S de A tel que $0_A \notin S$

On considère $S^{-1}A = \left\{ \frac{a}{s} \right\}_{a \in A,\ s \in S} \subset \mathbb{K}$ Sous-anneau de $\mathbb{K}$?

$a, b \in A$, $s, t \in S$ $\frac{a}{s} \times \frac{b}{t} = \frac{ab}{st}$, $ab \in A$, $st \in S$?

On rajoute la condition que S est une partie multiplicative, c'est-à-dire $\forall s \in S\ \forall t \in S,\ st \in S$

On montre que $S^{-1}A$ est un sous-anneau de $\mathbb{K}$, qui contient A, dans lequel tout élément de S est inversible et c'est « le plus petit anneau contenant A vérifiant cette propriété »

Formalisme général On suppose que $\underset{\text{anneau intègre}}{A} \subset \underset{\text{corps}}{\mathbb{K}}$ $A \subset \underset{\substack{\cup \\ S^{-1}A}}{\mathrm{Frac}}(A)$, $\subset$

et on veut « rendre inversibles » les éléments d'une partie S de A tel que $0_A \notin S$

On considère $S^{-1}A = \left\{ \frac{a}{s} \right\}_{\substack{a \in A \\ s \in S}} \subset \mathbb{K}$ Sous-anneau de $\mathbb{K}$?

(1) ?

$a, b \in A$
$s, t \in S$

$\frac{a}{s} \times \frac{b}{t} = \frac{ab}{st}$ $ab \in A$, $st \in S$?

On rajoute la condition que S est une partie multiplicative, c'est-à-dire $\forall s \in S \ \forall t \in S, \ st \in S$

On montre que $S^{-1}A$ est un sous-anneau de $\mathbb{K}$, qui contient A, dans lequel tout élément de S est inversible et c'est « le plus petit anneau contenant A vérifiant cette propriété »

c'est-à-dire : si B est un anneau intègre qui contient A et dans lequel tous les éléments de S sont inversibles, alors B contient $S^{-1}A$. (par exemple $B = \mathrm{Frac}(A)$)

Exemple $S = \mathbb{Z} \setminus p\mathbb{Z} \subset \underset{A}{\underset{\shortparallel}{\mathbb{Z}}}$ est une partie multiplicative
(p premier) (lemme d'Euclide)

$S^{-1}\mathbb{Z} = \mathbb{Z}_{(p)}$

$$\mathbb{Z} \subsetneq \mathbb{Z}_{(p)} \subsetneq \mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$$

Exemple $A = \mathbb{Q}[X]$ $S = \{ P \in \mathbb{Q}[X], \ P(0) \neq 0 \}$
$= \{ P \in \mathbb{Q}[X], \ X \text{ ne divise pas } P \}$
$= \mathbb{Q}[X] \setminus X \cdot \mathbb{Q}[X]$

$S^{-1}A \subset \mathbb{Q}(X) = \mathrm{Frac}(\mathbb{Q}[X])$
$= \left\{ \frac{P}{Q}, \ P \in \mathbb{Q}[X], \ Q \in \mathbb{Q}[X], \ Q(0) \neq 0 \right\}$

Question Exhiber un autre anneau intègre qui contient $S^{-1}A$?
(c'est-à-dire un anneau intègre qui contient $\mathbb{Q}[X]$ et dans lequel tout élément de $\mathbb{Q}[X] \setminus X\,\mathbb{Q}[X]$ est inversible)

Réponse $\mathbb{Q}[[X]]$
$\cup$
$\mathbb{Q}[X]$

$\frac{1}{X} \in \mathrm{Frac}(\mathbb{Q}[X])$ $\frac{1}{X} \notin S^{-1}A$

Soit $P, Q \in \mathbb{Q}[X]$, $Q \neq 0$ $\frac{1}{X} = \frac{P}{Q}$

$S^{-1}A \subset \mathbb{Q}(X) = \mathrm{Frac}(\mathbb{Q}[X])$

$= \left\{ \frac{P}{Q},\ P \in \mathbb{Q}[X],\ Q \in \mathbb{Q}[X],\ Q(0) \neq 0 \right\}$

Question Exhiber un autre anneau intègre qui contient $S^{-1}A$?
(c'est-à-dire un anneau intègre qui contient $\mathbb{Q}[X]$ et dans lequel tout élément de $\mathbb{Q}[X] \setminus X\,\mathbb{Q}[X]$ est inversible)

Réponse $\mathbb{Q}[[X]]$
$\cup$
$\mathbb{Q}[X]$

$\frac{1}{X} \in \mathrm{Frac}(\mathbb{Q}[X])$ $\quad \frac{1}{X} \notin S^{-1}A$

Soit $P, Q \in \mathbb{Q}[X]$, $Q \neq 0$ tq $\frac{1}{X} = \frac{P}{Q}$

donc $Q = PX$ donc $Q(0) = 0$

$\mathbb{Q}[[X]]^\times = \left\{ \sum_{i=0}^{\infty} a_i X^i,\ \text{avec } a_0 \neq 0 \right\}$

en particulier, si $P \in \mathbb{Q}[X]$ tel que $P(0) \neq 0$
alors $P \in \mathbb{Q}[[X]]^\times$

donc $\mathbb{Q}[X] \subset S^{-1}A \subset \mathbb{Q}[[X]]$

Remarque les deux exemples ci-dessus sont des cas particuliers de la situation générale suivante :
on prend A un anneau (intègre)
I un idéal premier de A
et $S = A \setminus I$