A commutatif et intègre $\quad \mathbb{Z}, \mathbb{K}[x], \mathbb{Z}[i]$.

4 catégories :
1. 0 (tout le monde divise 0 : $0 = 0 \times x$)
2. les inversibles (divisent tout le monde : $x = u(u^{-1}x)$)
3. les autres : les irréductibles.
4. les décomposables : $x = a \times b$ a, b non inv, non nul

Fait : si x est irr., ses div. sont les inv. et les associés à x.
$\mathrm{Div}(x) = A^* \cup A^* x$.

$\mathbb{Z}$:
1. 0
2. ± 1
3. $\pm p$, p premier.
4. $6 = 2 \times 3$

$\mathbb{C}[x]$:
1. 0 $(\deg = -\infty)$
2. $\deg = 0$
3. $\deg = 1$ ($\mathbb{C}$ est alg. clos)
4. $\deg \geq 2$

$\mathbb{K}[x]$ $\quad P$ est déc. $\iff \exists Q, R \quad P = Q.R \quad d^\circ Q \geq 1, d^\circ R \geq 1$

Définition 5.3.2 *Soit A un anneau commutatif intègre. On dit que A est (un anneau) factoriel s'il vérifie les deux conditions suivantes : existence (E) et unicité (U) de la décomposition en facteurs irréductibles.*

(E) Tout $a \in A \setminus \{0\}$, non inversible, s'écrit

$$a = p_1 \cdots p_r,$$

où $r \geq 1$ et les p_i sont des éléments irréductibles de A ;

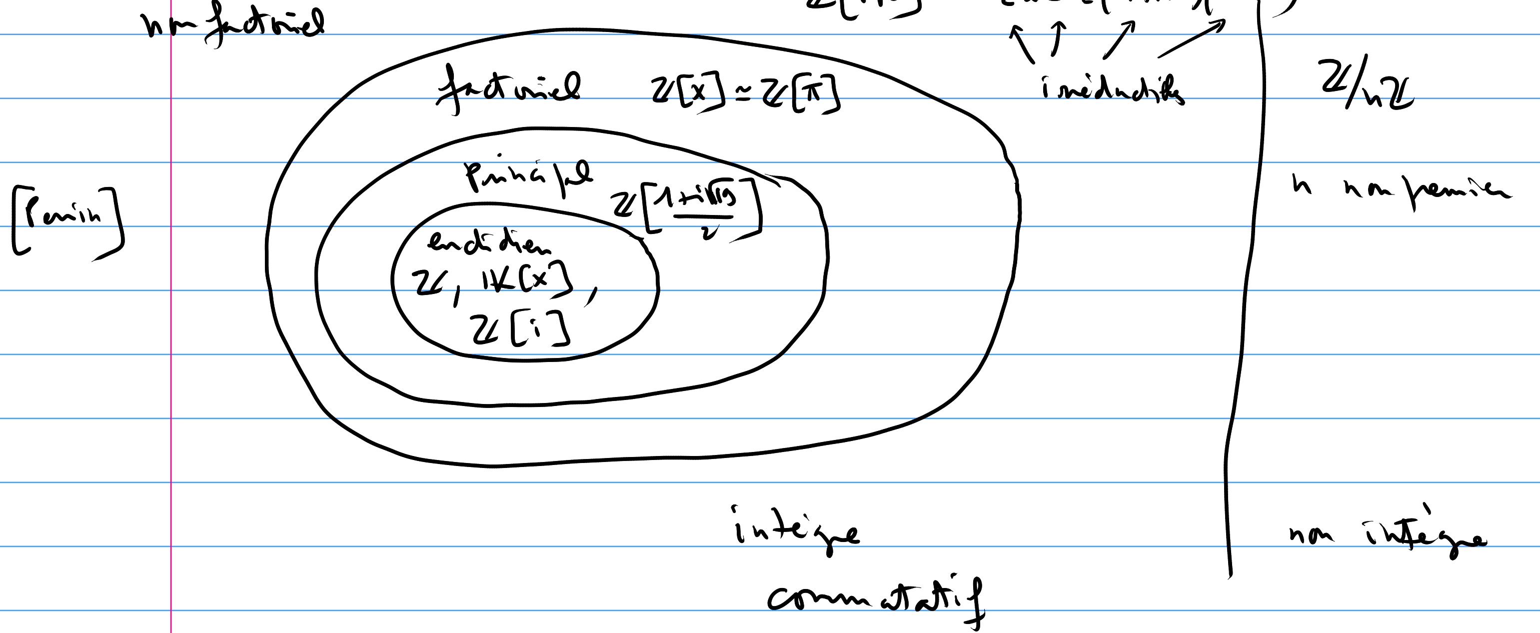
(U) La décomposition précédente est unique, au sens suivant : si l'on a deux décompositions

$$a = p_1 \cdots p_r = q_1 \cdots q_s,$$

où les p_i et les q_j sont irréductibles, alors $s = r$ et il existe une permutation $\sigma \in S_r$ telle que p_i et $q_{\sigma(i)}$ soient associés, pour tout $i = 1, \ldots, r$. C.-à-d., de façon plus concise, la décomposition est unique à l'ordre des termes et aux inversibles près.

dans $\mathbb{Z}$ $\quad -6 = (-2)\times 3 = (-3)\times 2$

$\mathbb{Z}[i\sqrt{5}]$ $\quad 2\times 3 = (1+i\sqrt{5})(1-i\sqrt{5})$



$\mathbb{Z} \subset \mathbb{Z}[i]$

2 irr. $\quad 2 = (1-i)(1+i)$ déc.

non inv.

$\mathbb{Z} \subset \mathbb{Z}\left[\frac{1}{2}\right] = \left\{ a_0 + \dots + a_n \cdot \frac{1}{2^n},\ n\in\mathbb{N},\ a_0 \dots a_n \in \mathbb{Z} \right\}$

2 irr. $\quad$ 2 inv

$= \left\{ \frac{m}{2^n},\ n\in\mathbb{Z},\ m\in\mathbb{Z} \right\}$

$\mathbb{Z} \subset \mathbb{Z}[i] \subset \mathbb{Z}\left[\frac{1}{2}, i\right]$

2 irr. $\quad$ 2 déc $\quad$ 2 inv.

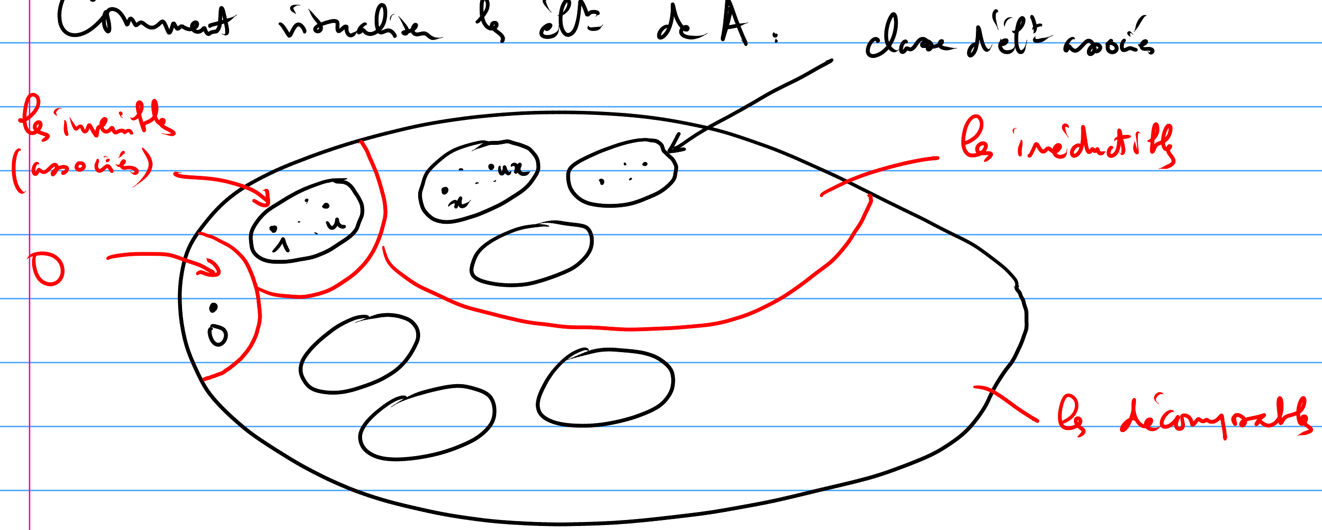
$\mathbb{Z} \subset \mathbb{Z}\left[\frac{1}{2}\right] \subset \mathbb{Z}\left[\frac{1}{6}\right]$

$6 = 2\times 3$ déc $\quad$ 6 irr. (ass. à 3) $\quad$ 6 inv.

$\mathbb{Z} \subset \mathbb{Z}\left[\frac{1}{3}\right] \subset \mathbb{Z}\left[\frac{1}{3}, i\right]$

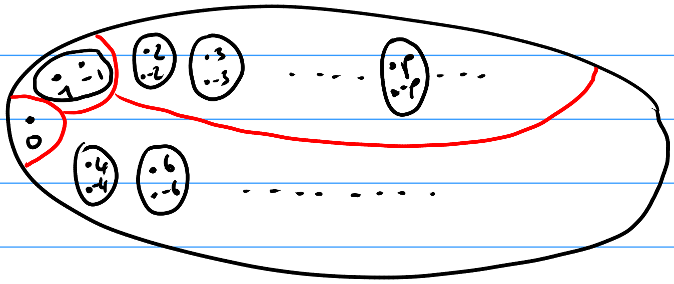
$6 = 2\times 3$ déc $\quad$ 6 irr. (ass. à 2) $\quad$ $6 = 3.(1-i)(1+i)$ déc

Comment visualiser les élts de A :



Ex :

$\mathbb{Z}$



La relation | est un ordre partiel sur les classes d'élts associés.
On peut organiser cet ordre sur un "treillis" :