Chapitre 9. Anneaux

I. Rappels I.1. Notations, exemples fondamentaux

Un **anneau non-unitaire** correspond à un la donnée de $A, +, \times, 0_A$ tels que $(A, +)$ groupe commutatif de neutre 0_A et $\times$ l.c.i. associative sur A et distributive a gauche et a droite par rapport a $+$.

Un **anneau = anneau unitaire** correspond à un la donnée de $A, +, \times, 0_A, 1_A$ tel que $(A, +, \times, 0_A)$ anneau et 1_A élément neutre pour la multiplication.

Un **anneau commutatif** est un anneau dans lequel $\times$ est commutatif

Un anneau est **nul** si $A = \{0_A\}$ autrement dit ssi $1_A = 0_A$. Dans un anneau non nul, $1_A \neq 0_A$.

Exemples : $(K, +, \times)$, $(K[X], +, \times)$, avec $K = Z, Q, R, C$, sont des anneaux commutatifs. $(M_n(K), +, \times)$ est un anneau non commutatif.

L'**anneau produit** d'un nombre fini d'anneaux est le produit cartésien des anneaux, muni des lois produit. L'anneau produit est un anneau.

L'ensemble des polynômes a coefficients dans un anneau commutatif, forme un anneau commutatif pour la somme et le produit de polynômes.

L'ensemble des fonctions d'un ensemble quelconque dans un anneau est aussi un anneau pour la somme et le produit de fonctions.

Un **sous-anneau** d'un anneau $(A, +, \times)$ est une partie non vide de A qui est encore un anneau pour les lois induites et qui contient le neutre multiplicatif de A. Autrement dit c'est une partie $B \subseteq A$ telle que $\forall x, y \in B\ x + y \in B, \forall x \in B - x \in B,\ \forall x, y \in B\ xy \in B,\ 1_A \in B$. (entraine automatiquement $B \neq \emptyset$)

L'ensemble des entiers de Gauss $Z[i]$ est un sous-anneau de $(C, +, \times)$.

Plus généralement si B est un sous-anneau d'un anneau $(A, +, \times)$, alors pour $x \in A \setminus B$ qui commute avec tous les éléments de B, on peut définir $B[x] = \left\{\sum_{i=0}^{k} b_i x^i : (b_i)_{0 \leq i \leq k}, k \in N\right\}$.

Alors $B[x]$ est un sous-anneau de $(A, +, \times)$ et B est un sous-anneau de $(B[x], +, \times)$.

Un élément d'un anneau est **inversible** s'il est symétrisable pour la loi $\times$. Dans ce cas l'**inverse d'un élément** inversible d'un anneau est le symétrique pour la loi $\times$.

On note $\boldsymbol{A^\times}$ l'ensemble des éléments inversibles d'un anneau. On note $\boldsymbol{A^*} = A \setminus \{0_A\}$

L'ensemble des éléments inversibles d'un anneau unitaire est un groupe pour $\times$ d'élément neutre 1_A.

Un **anneau à division** est un anneau unitaire dans lequel tout élément non nul est inversible $A^\times = A^*$.

Un **corps** est un anneau unitaire commutatif dans lequel tout élément non nul est inversible $A^\times = A^*$.

Un corps est donc un anneau à division commutatif.

Une **corps gauche** est un anneau à division non commutatif.

Un anneau non nul est **intègre** ssi $ab = 0 \Rightarrow a = 0$ ou $b = 0$

Un corps est un anneau intègre

Les anneaux Z, Q, R sont des anneaux intègres. Si K corps, $K[X]$ anneau intègre.

Si K est un corps, $K[X_1, \ldots, X_n]$ est un anneau intègre.

Les anneaux inclus dans des corps sont des anneaux intègres.

Les corps sont les anneaux intègres finis.

I.2. Idéaux

Un **idéal à droite (resp. à gauche) d'un anneau** $(A, +, \times)$ est une partie $I \subseteq A$ tel que $(I, +)$ sous-groupe de $(A, +)$ et $\forall x \in I\ \forall a \in A\ xa \in I$ (resp. $ax \in I$).

Un **idéal = idéal bilatère** d'un anneau est un idéal à droite et à gauche de cet anneau.

Les idéaux les plus simples sont les suivants :
Si $a \in A$ un anneau, alors $aA = \{ax : x \in A\}$ est un idéal à droite de A
Si $a \in A$ un anneau, alors $Aa = \{xa : x \in A\}$ est un idéal à gauche de A
Si $a \in A$ un anneau, alors $AaA = \{xay : x, y \in A\}$ est un idéal de A
Un idéal d'une de ces formes simples est un **idéal principal (gauche/droite/bilatère)**
Dans un anneau commutatif, il n'y a plus de distinction entre idéal à gauche, à droite, ou bilatère. On note alors $(\boldsymbol{a}) = aA = Aa = AaA$ les ideaux principaux de A.
Un anneau principal est un anneau commutatif intègre dont tous les idéaux sont principaux.
Z est un anneau principal. Si K est un corps, $K[X]$ est un anneau principal.

I.3. Morphismes d'anneaux

Un **morphisme d'anneaux (unitaires)** est une application $f : A \to B$ entre deux anneaux $(A, +, \times), (B, +, \times)$ telle que $\forall x, y \in A \;\; f(x + y) = f(x) + f(y),\;\; f(xy) = f(x)f(y),\;\; f(1_A) = 1_B$
L'image réciproque d'un idéal de l'anneau de d'arrivée par un morphisme d'anneaux est un idéal de l'anneau de départ.
Le noyau d'un morphisme d'anneaux est un idéal de son anneau de départ.
L'image d'un morphisme d'anneaux est un sous-anneau $f(A) \subseteq B$ de l'anneau d'arrivée.
L'image directe d'un idéal par un morphisme d'anneaux est un idéal du sous-anneau image $f(A)$.
L'image directe d'un idéal par un morphisme d'anneaux surjectif est un idéal de l'anneau d'arrivée.
Si un morphisme d'anneaux est bijectif, sa réciproque est aussi un morphisme d'anneaux, c'est donc un isomorphisme.

I.4. Anneaux quotients

Rappel : Si H est un sous-groupe distingue de $(G, +)$, alors $\frac{G}{H}$ existe et la l.c.i. $+$ est compatible avec la relation d'equivalence naturelle, ce qui permet de definir la loi quotient correspondante.
Si I est un ideal d'un <u>anneau commutatif</u> $(A, +, \times)$ alors $+$, et $\times$ sont compatibles avec la relation d'equivalence naturelle donc definissent des lois quotient sur $\frac{A}{I}$, de plus $\left(\frac{A}{I}, +, \times\right)$ est un anneau commutatif. On appelle cet anneau, l'**anneau quotient** de $(A, +, \times)$ par l'idéal $(I, +)$.
La projection canonique d'un anneau commutatif dans son quotient par un idéal, $p : A \to \frac{A}{I}$ est toujours un morphisme d'anneaux dont le noyau est l'idéal I.
Les nZ sont les ideaux (principaux) de Z, les $\left(\frac{Z}{nZ}, +, \times\right)$ sont les anneaux quotients de $(Z, +, \times)$.

I.5. Arithmétique

Dans un anneau commutatif, soit $a \in A^*$ et $b \in A$, on dit : $\boldsymbol{a}$ **divise** $\boldsymbol{b}$ **=** $\boldsymbol{a}$ **est un diviseur de** $\boldsymbol{b}$ ssi $\exists k \in A \; b = ak$ ssi $bA \subseteq aA$.
Dans un anneau intègre $\forall a, b \in A^* \; \forall c \in A, \; ab|ac \Leftrightarrow b|c$
Dans un anneau intègre $\forall a, b \in A^*, \; ab|a \Leftrightarrow b \in A^\times$
Dans un anneau intègre $\forall a, b \in A^*, \; a|b$ et $b|a \Leftrightarrow a, b$ associés

II. Ces êtres étranges qui vivent dans les anneaux

II.1. Eléments centraux

Un élément central d'un anneau est un élément qui commute avec tous les autres éléments de l'anneau pour la loi $\times$. Le **centre d'un anneau** est l'ensemble des éléments centraux $\boldsymbol{Z(A)}$
Le centre d'un anneau est un sous-anneau. Le centre d'un anneau est un idéal ssi l'anneau est

commutatif ssi le centre coïncide avec tout l'anneau.

II.2. Diviseurs de zéro

Dans un anneau, un élément non nul est un **diviseur de zéro à gauche (resp. à droite)**, s'il est possible de le multiplier à droite (resp. à gauche) par un élément non nul de sorte à obtenir 0_A. Dans un produit de deux éléments non nuls qui donne 0, celui à gauche est un diviseur de 0 à gauche, celui à droite est un diviseur de 0 à droite. Un **diviseur de zéro** tout court est un diviseur de zéro à gauche ou à droite.
Un diviseur de 0 à gauche et à droite, vérifie $ab = b'a = 0$ mais généralement rien n'oblige que $b = b'$.
L'endomorphisme de dérivation $D \in L(R[X])$ est un diviseur de zéro à gauche mais pas à droite dans l'anneau $(L(R[X]), +, \circ)$.
Dans l'anneau $(L(E), +, \circ)$ avec E Kev, une application lineaire est un diviseur de zero a gauche (resp. a droite) ssi elle n'est pas injective (resp. surjective).
Un élément inversible d'un anneau n'est jamais un diviseur de zéro et donc réciproquement.
Il existe dans beaucoup d'anneaux des éléments ni inversible, ni diviseur de zéro. Par ex : 2 dans Z.

II.3. Eléments réguliers

Dans un magma, un élément a est dit **simplifiable à gauche (resp droite)** (dans toute expression par la lci) si dans toute égalité de produits ou il est à gauche (resp. droite) dans les deux membres, on a toujours égalité si on l'enlève dans les deux membres à gauche (resp droite).
Dans un anneau, un élément est dit **régulier à gauche (resp droite)** ssi il est simplifiable à gauche (resp droite) pour la loi $\times$.
Dans un anneau, un élément est régulier à gauche (resp. droite) ssi il n'est pas nul et n'est pas un diviseur de zéro à gauche (resp. droite)
Dans un anneau, un élément est dit **régulier** ssi il est régulier à gauche et à droite.
Dans un anneau, un élément est régulier ssi il n'est pas nul et n'est pas un diviseur de zéro.
Un anneau est intègre ssi il n'a pas de diviseurs de zéro ssi tous ses éléments non nuls sont réguliers.

II.4. Eléments nilpotents

Un élément a d'un anneau est **nilpotent** si $\exists k \in N^* \; a^k = 0_A$
Un élément a d'un anneau est **unipotent** si $\exists k \in N^* \; (a - 1_A)^k = 0_A$
Sur l'anneau des applications linéaires d'un Kev de dimension finie, une application linéaire dont la matrice est triangulaire avec des 0 sur la diagonale est nilpotente.
Le **nilradical d'un anneau** A note $\boldsymbol{nil}(\boldsymbol{A})$ est l'ensemble des éléments nilpotents de l'anneau.
$\boldsymbol{uni}(\boldsymbol{A})$ est l'ensemble des éléments unipotents d'un anneau A.
Pour x nilpotent dans un anneau, alors $1 - x$ inversible. De plus $\prod_{k=0}^{n} \left(1 + x^{2^k}\right) = (1 - x)^{-1}\left(1 - x^{2^{n+1}}\right)$

II.5. Caractéristique d'un anneau

Un **élément de (Z)-torsion** d'un anneau A est un élément $a \in A$ tel que $\exists k \in Z^* \; ka = 0_A$, c'est un élément d'ordre fini dans le groupe $(A, +)$.
Dans $M_n(R)$ il n'y a pas d'éléments de torsion, dans $\frac{Z}{nZ}$, tout élément est de torsion.
Dans le corps $\frac{Z}{pZ}$ avec p premier, tout élément est de torsion, mais aucun n'est diviseur de 0, il faut donc faire attention a bien faire la distinction en général.
L'ensemble des éléments de torsion d'un anneau $Tor(A)$ est un ideal de l'anneau A.

$\psi: Z \to A: k \mapsto k1_A$ est un morphisme d'anneaux dont le noyau $\ker(\psi)$ est un ideal de Z donc de la forme nZ.
On appelle **caractéristique** d'un anneau $(A, +, \times)$ l'unique entier $n \in N$ tel que $\ker(\psi) = nZ$. On note $\boldsymbol{car(A)}$.
$car(Z) = 0,\ car\left(\frac{Z}{nZ}\right) = n.$
Dans un anneau de caractéristique non nulle, tout élément x est de torsion puisque $car(A)x = 0_A$.
La caractéristique d'un anneau intègre (et donc d'un corps) est soit 0, soit un nombre premier.

II.6. Eléments irréductibles

Deux éléments x, y d'un anneau A sont **associés** ssi $\exists \lambda \in A^\times\ y = \lambda x$ ssi $y \in A^\times x$ ssi x et y sont sur la même orbite relativement à l'action du groupe $(A^\times, \times)$ sur l'anneau.
Un élément a d'un anneau $(A, +, \times)$ est **irréductible** ssi a non inversible et $\forall x, y \in A \mid xy = a \Rightarrow x$ inversible ou y inversible ssi a non inversible et $\forall x, y \in A \mid xy = a \Rightarrow x$ ou y est associe à a. Autrement dit un élément non inversible est irréductible ssi il ne peut pas s'exprimer comme un produit d'éléments provenant d'autres orbites, c'est-à-dire que si on quotiente l'anneau par la relation être sur la même orbite, un élément non inversible est irréductible ssi ses seuls diviseurs sont lui-même et 1_A.
Dans $(Z, +, \times)$ les éléments irréductibles sont les nombres premiers.
Si K est un corps, tout polynome de degre ≥ 2 de $K[X]$ qui admet une racine n'est pas irréductible car on peut factoriser par $X - x$. Autres exemples vus plus tard.
Un élément peut être irréductible dans un sous-anneau sans l'être dans un anneau qui le contient.
Dans $A[X]$ avec A anneau commutatif non intègre, il peut exister des polynomes de degre 1 non irréductible par ex : $(6X + 4)(2X + 3) = 2X$ dans $\frac{Z}{12Z}[X]$.
Dans l'anneau de Gauss $Z[i]$ on peut definir une norme $N(x) = |x|^2 = a^2 + b^2$ et on a x inversible dans $Z[i]$ ssi $N(x) = 1$. De plus $N(x)$ premier implique x irréductible.

III. Etude des idéaux

Un idéal d'un anneau commutatif coïncide avec l'anneau entier ssi il contient un élément inversible ssi il contient 1_A ssi l'anneau quotient par l'idéal est nul.

III.1. Operations entre idéaux

Dans un anneau commutatif l'intersection quelconque d'idéaux est un idéal.
Dans un anneau commutatif on définit **l'idéal somme** comme l'ensemble somme $\boldsymbol{I_1 + \cdots + I_n} = \{i_1 + \cdots + i_n : i_1 \in I_1, \ldots, i_n \in I_n\}$. La somme finie d'ideaux est un ideal de l'anneau commutatif.
Dans un anneau commutatif on définit **l'idéal produit** :
$\boldsymbol{I_1 \ldots I_n} = \left\{\sum_{k=1}^{N} i_{1,k} \ldots i_{n,k} :\ N \in N^*, \left(i_{1,k}, \ldots, i_{n,k}\right)_{1 \leq k \leq N} \in (I_1 \times \ldots \times I_n)^N\right\}$
L'idéal produit fini est un idéal de l'anneau commutatif.
Attention l'ensemble produit d'idéaux n'est généralement pas un idéal car pas stable par addition.
L'idéal produit fini est inclus dans l'intersection finie des idéaux du produit. $IJ \subseteq I \cap J$
L'intersection d'un nombre fini d'idéaux est incluse dans l'idéal somme finie de ces idéaux. $I \cap J \subseteq I + J$
En fait l'idéal somme est le plus petit idéal contenant l'union des idéaux.
On peut écrire $I_1 \ldots I_n \subseteq I_1 \cap \ldots \cap I_n \subseteq I_1 + \cdots + I_n$
Dans un anneau commutatif on a toujours pour les idéaux principaux : $aA \times bA = (ab)A$
$aA + bA$ est un ideal comme somme, donc dans un anneau principal $\exists c \in A\ \ aA + bA = cA$

$aA \cap bA$ est un idéal comme intersection, donc dans un anneau principal $\exists c \in A \;\; aA \cap bA = cA$
Dans $(Z, +, \times)$ on a $aZ + bZ = (a \wedge b)Z$, et a $aZ \cap bZ = (a \vee b)Z$
La réunion de deux idéaux n'est en général pas un idéal.
La somme d'idéaux est associative et commutative, le produit d'idéaux est associatif et commutatif.
Le produit d'idéaux est distributif par rapport à l'addition : $(I + J)K = IK + JK$

III.2. Générateurs d'un idéal

Un générateur d'un idéal principal est un élément de l'anneau a tel que l'idéal $I = aA = \langle a \rangle$
Dans un anneau commutatif intègre deux éléments a, b sont associés ssi a divise b et b divise a ssi $aA = bA$. Dans un tel anneau, les idéaux principaux n'admettent donc qu'un unique générateur à association près.
On peut définir **l'idéal engendré par une partie $\boldsymbol{P} \subseteq \boldsymbol{A}$** d'un anneau commutatif comme le plus petit idéal de A contenant P. C'est l'ensemble $\langle \boldsymbol{P} \rangle = \left\{ \sum_{k=1}^{N} x_k p_k : N \in N^*, \; (x_k)_{1 \le k \le N} \in A^N, (p_k)_{1 \le k \le N} \in P^N \right\}$
Pour un ensemble fini de points on a $\langle a_1, \dots, a_n \rangle = \langle a_1 \rangle + \cdots + \langle a_n \rangle$
$\langle a_1, \dots, a_n \rangle \langle b_1, \dots, b_m \rangle = \langle \left(a_i b_j\right)_{i,j} \rangle$ TODO vérifier
Un idéal **monogène** = idéal principal.
Un idéal est **de type fini** ssi il est engendré par un nombre fini d'éléments ssi c'est une somme finie d'idéaux principaux.
$K[X_1, \dots, X_n]$ est un anneau dont tous les idéaux sont de type fini.
L'idéal $\langle X_1, \dots \rangle$ de l'anneau $K[X_1, \dots] = \cup_{k \in N} K[X_0, \dots, X_k]$ n'est pas de type fini
Dans un groupe fini, l'ensemble $\{e \in Z \mid \forall g \in G \; g^e = 1_G\}$ est un ideal de Z et **l'exposant $\boldsymbol{\omega(G)}$** de G est le generateur positif de cet ideal. Comme $\{e \in Z \mid \forall g \in G \; g^e = 1_G\} = \cap_{g \in G} \{e \in Z \mid g^e = 1_G\}$ il s'ensuit que $\omega(G) = ppcm(ord(g) : g \in G)$

III.3. Idéaux des anneaux euclidiens

Un anneau (commutatif) euclidien est un anneau commutatif intègre muni d'une application appelée **stathme euclidien** $\nu : A^* \to N$ telle que pour tous $a \in A^*, b \in A^*$:
Si b divise a alors $\nu(b) \le \nu(a)$, et si b ne divise pas a alors $\exists q \in A \; \exists r \in A \; a = bq + r$ et $\nu(r) < \nu(b)$
En prolongeant $\nu : A \to N$ par $\nu(0_A) = -\infty$ on peut alors affirmer sans condition dans un tel anneau que $\forall a \in A \; \forall b \in A^* \; \exists q \in A \; \exists r \in A \; a = bq + r$ et $\nu(r) < \nu(b)$
Il n'y a pas forcement unicité de (q, r). Il suffit que $\forall a, b \in A^* \;\; \nu(a - b) \le \max\left(\nu(a), \nu(b)\right)$, pour qu'il y ait unicité.
Dans un anneau euclidien, $x \in A^\times \Leftrightarrow \nu(x) = \min\{\nu(x) : x \in A^*\}$
$(Z, +, \times)$ est un anneau euclidien muni du stathme euclidien $n \mapsto n$.
$K[X]$ est un anneau euclidien muni du stathme euclidien $P \mapsto \deg(P)$
$Z[i]$ est un anneau euclidien muni du stathme euclidien $\nu : Z[i] \to N : x + iy \mapsto x^2 + y^2 = |x + iy|^2$
Les inversibles de $\mathbb{Z}[i]$ sont $1, -1, i, -i$.
Un anneau commutatif euclidien est un anneau principal.
$Z, K[X], Z[i]$ sont des anneaux euclidiens donc principaux.
$K[X, Y]$ n'est pas un anneau principal donc pas euclidien.
Si A est un anneau commutatif, $A[X]$ est un anneau principal ssi A est un corps. Donc $Z[X]$ non euclidien

$Z\left[\frac{1+i\sqrt{19}}{2}\right]$ est un anneau principal non euclidien.

III.4. Arithmétique des idéaux

III.4.1. Idéaux maximaux

Deux idéaux d'un anneau commutatif sont **comaximaux** ssi leur idéal somme est l'anneau $I + J = A$.

Cette propriété est analogue à la propriété « premier entre eux » dans Z.

Deux idéaux de Z sont comaximaux ssi leur générateur respectifs sont premiers entre eux.

Exemple 2 illisible TODO

Deux idéaux comaximaux d'un anneau commutatif vérifient $IJ = I \cap J$. Traduction dans Z : si 2 nombres sont premiers entre eux leur ppcm est leur produit.

Deux idéaux d'un anneau <u>principal</u> vérifiant $IJ = I \cap J$ sont comaximaux. Traduction dans Z : la réciproque est vraie càd : 2 nombres sont premiers entre eux ssi leur ppcm est leur produit.

Si l'anneau n'est pas principal cette réciproque est généralement fausse.

Dans un anneau commutatif, si un idéal I est comaximal avec $I_1, \dots, I_n$ alors il est comaximal avec leur ideal produit.

Dans un anneau commutatif, si $I_1, \dots, I_n$ famille d'idéaux 2 à 2 comaximaux alors $I_1 \dots I_n = I_1 \cap \dots \cap I_n$

III.4.2. Theoreme des restes chinois

Dans Z. Si $n_1, \dots, n_k$ sont 2 a 2 premiers entre eux et $n = n_1 \times \dots \times n_k$ alors l'application $\frac{Z}{nZ} \to \frac{Z}{n_1 Z} \times \dots \frac{Z}{n_k Z} : x \mapsto \left(\overline{x}^1, \dots, \overline{x}^k\right)$ est un isomorphisme d'anneaux.

Théorème. Soit $I_1, \dots, I_k$ des ideaux 2 a 2 comaximaux d'un anneau commutatif A, soit $I = I_1 \dots I_k = I_1 \cap \dots \cap I_k$, alors l'application $\varphi : \frac{A}{I} \to \frac{A}{I_1} \times \dots \times \frac{A}{I_k} : x + I \mapsto (x + I_1, \dots, x + I_k)$ est un isomorphisme d'anneaux.

III.4.4. Un exemple d'application Th des restes chinois : le polynôme d'interpolation de Lagrange

Soit $(a_1, \dots, a_n) \in K^n, (b_1, \dots, b_n) \in K^n$, si $a \neq a', \langle X - a \rangle$ et $\langle X - a' \rangle$ sont comaximaux. Donc $\frac{K[X]}{P}$ et $\frac{K[X]}{\langle X - a_1 \rangle} \times \dots \times \frac{K[X]}{\langle X - a_n \rangle}$ sont isomorphes avec $P = \prod_{i=1}^{n} (X - a_i)$ donc les $b_1, \dots, b_n$ ont un unique antécédent dans $\frac{K[X]}{P}$ qui a pour unique représentant de degré $< n$: $L = \sum_{r=1}^{n} b_r \prod_{i \neq r} \frac{X - a_i}{a_r - a_i}$

On verifie $\forall i \;\; L(a_i) = b_i$.

III.4.3. Système fondamental d'idempotents

Un **élément idempotent d'un anneau** est un élément $x \in A$ tel que $x^2 = x$.

Dans un anneau intègre, les seuls éléments idempotents sont 0_A et 1_A

Un **système fondamental d'idempotents orthogonaux d'un anneau commutatif** est une partie finie $\{e_1, \dots, e_n\}$ d'éléments <u>non nuls</u> de l'anneau tels que $\forall i \neq j \; e_i e_j = 0$ et $e_1 + \dots + e_n = 1_A$.

Dans ce cas cela implique automatiquement que tous les e_i sont idempotents.

Dans un anneau produit $A_1 \times \dots \times A_n$ les $e_i = \left(0_{A_1}, \dots, 1_{A_i}, \dots, 0_{A_n}\right)$ forme un système fondamental d'idempotents orthogonaux, et $\langle e_i \rangle = \left\{0_{A_1}\right\} \times \dots \times A_i \times \dots \times \left\{0_{A_n}\right\}$

Dans un anneau commutatif $\{1_A\}$ est un système fondamental d'idempotents

Si x est idempotent non nul dans un anneau commutatif A, alors $\{x, 1_A, -x\}$ est un système fondamental d'idempotents orthogonaux.

Si A est un anneau commutatif admettant un système fondamental d'idempotents orthogonaux a n

éléments, alors il existe n anneaux tels que $A \approx A_1 \times \ldots \times A_n$.
Précisément si A est un anneau commutatif de système fondamental d'idempotents orthogonaux $\{e_1, \ldots, e_n\}$ alors $A \approx \frac{A}{\langle 1_A - e_1 \rangle} \times \ldots \times \frac{A}{\langle 1_A - e_n \rangle}$

III.5. Radical d'un ideal

Le **radical d'un idéal I d'un anneau** $(A, +, \times)$ est l'ensemble $\sqrt{I} = \{a \in A \mid \exists n \in N \; a^n \in I\}$
Un ideal est dit **radical** ssi il coïncide avec son radical $\sqrt{I} = I$.
Soit $n \in Z$ de decomposition en facteurs premiers $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ alors $\sqrt{nZ} = (p_1 \ldots p_k)Z$
Dans Z les ideaux radicaux sont les nombres premiers, ou produits de facteurs premiers de valuation 1.
Dans un anneau commutatif, le radical d'un idéal est un idéal.
Dans un anneau commutatif, l'ensemble des éléments nilpotents $nil(A)$ est un ideal car $nil(A) = \sqrt{\langle 0_A \rangle}$
Pour cette raison on appelle aussi $nil(A)$ **le nilradical de A**.
Un anneau est dit **réduit** ssi il n'a pas d'éléments nilpotents non nuls ssi $nil(A) = \{0_A\}$
Un anneau intègre est toujours réduit, mais reciproque fausse $Z/6Z$.
Dans un anneau commutatif, un idéal est radical ssi l'anneau quotient par l'idéal est un anneau réduit.

III.6. Idéaux maximaux

Un **idéal maximal** d'un anneau commutatif est un idéal propre qui n'est contenu dans aucun autre idéal propre que lui-même.
Krull. Dans un anneau tout idéal propre est inclus dans un idéal maximal. (Par lemme de Zorn)
Dans un anneau commutatif, un idéal propre est maximal ssi l'anneau quotient par l'idéal $\frac{A}{I}$ est un corps.
Les idéaux maximaux de Z sont les pZ avec p premier.
Un élément a d'un anneau <u>principal</u> est irréductible ssi l'idéal qu'il engendre $\langle a \rangle$ est un idéal maximal, ssi $\frac{A}{\langle a \rangle}$ est un corps.

III.7. Idéaux premiers

Un idéal premier d'un anneau commutatif est un idéal <u>propre</u> de l'anneau tel que $\forall a, b \in A \;\; ab \in I \Rightarrow a \in I$ ou $b \in I$
Un anneau commutatif est intègre ssi son idéal $\langle 0_A \rangle$ est un idéal premier.
Un entier naturel est premier ssi son idéal dans Z est un idéal premier.
Dans $F(R, R)$, l'ensemble des fonctions qui s'annulent en 0 est un idéal premier.
Un morphisme d'anneau vers un anneau intègre a pour noyau un idéal premier de l'anneau de départ.
Dans un anneau commutatif, un idéal propre est un idéal premier ssi l'anneau quotient par l'idéal est un anneau intègre.
Dans un anneau commutatif, un idéal maximal est toujours premier.
Un **élément premier** d'un anneau commutatif A est un élément $a \in A$ dont l'idéal $\langle a \rangle$ est premier, autrement dit a est non inversible et $\forall x, y \in A$ si a divise xy alors a divise x ou a divise y.
Dans $F(R, R)$, l'idéal des fonctions qui s'annulent en 0 n'est pas principal.

III.8. Idéaux de A I

Soit deux idéaux $I \subseteq J \subseteq A$, alors on peut definir **l'idéal quotient par un autre idéal** $\frac{J}{I} = \pi(J) = \{j + I : j \in J\}$

Th. factorisation. Un morphisme d'anneaux $f: A \to B$, se factorise sur un idéal I ssi $f(I) = \{0_B\}$ ssi

$I \subseteq \ker(f)$ ssi $\exists \overline{f}: \frac{A}{I} \to B$ tel que $f = \overline{f} \circ \pi$.

Dans ce cas $\overline{f}$ est unique, $\overline{f}$ est un morphisme d'anneaux et on a $\forall a + I \in \frac{A}{I}\ \ \overline{f}(a + I) = f(a)$,

$im(\overline{f}) = im(f), \ker(\overline{f}) = \frac{\ker(f)}{I}$

De plus $\overline{f}$ est surjective ssi f l'est et $\overline{f}$ est injective ssi $\ker(f) = I$.

Th. isomorphisme 1. Un morphisme d'anneaux $f: A \to B$, se factorise toujours sur son noyau en une application $\overline{f}: \frac{A}{\ker(f)} \to B$ injective telle que $f = \overline{f} \circ \pi$. Donc $\frac{A}{\ker(f)} \approx im(f)$

Th. isomorphisme 3. Soit deux idéaux $I \subseteq J \subseteq A$ alors $\frac{\frac{A}{I}}{\frac{J}{I}} \approx \frac{A}{J}$ en factorisant $\pi: A \to A/J$ sur I.

L'ensemble somme d'un sous-anneau B avec un ideal I du meme anneau A, est un sous-anneau de A.

Th. isomorphisme 2. Pour un sous-anneau B et un idéal I d'un anneau A on a toujours $\frac{B+I}{I} \approx \frac{B}{B \cap I}$

IV. Corps des fractions

Soit A un anneau commutatif intègre, on peut construire un corps de fractions sur K, en posant une relation d'équivalence R sur $A \times A^*$ en posant $(a, b)R(c, d) \Leftrightarrow ad = bc$

On pose $\boldsymbol{Frac(A)} = \frac{A \times A^*}{R}$ et on note $\frac{a}{b}$ une classe de représentant (a, b). On a bien $\frac{a}{b} = \frac{c}{d}$ ssi $ad = bc$.

On définit ensuite $+$ et $\times$ naturellement $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ et $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$

$(Frac(A), +, \times)$ est un corps appele **corps des fractions de l'anneau intègre** A

Dans un corps K, $Frac(K) \to K: \frac{a}{b} \mapsto ab^{-1}$ est un isomorphisme de corps (donc inutile de faire ça).

Un plongement d'un anneau L dans un anneau M correspond a un morphisme injectif de $L \to M$ autrement dit cela correspond à un isomorphisme de L vers un sous anneau de M autrement dit cela correspond à un sous-anneau de M isomorphe a L.

Un anneau commutatif intègre se plonge naturellement dans son corps de fractions par injection.

Si un anneau commutatif intègre est plongé dans un corps, on peut aussi plonger le corps de fractions de l'anneau dans le corps de manière conservative, c'est à dire de sorte que l'anneau reste plongé naturellement dans son corps de fractions par injection. Autrement dit, si $\exists \phi: A \to K$ injectif alors $\exists f: Frac(A) \to K$ injectif tel que $\phi = f \circ i$ avec $i: A \to Frac(A): x \mapsto \frac{x}{1}$

V. Localisation

Une partie multiplicative d'un anneau commutatif $\boldsymbol{A}$ est un $M \subseteq A$ stable par multiplication qui contient 1_A

Un anneau quotient par un idéal est une partie multiplicative ssi l'idéal est premier.

Un **ensemble de valide dénominateurs** d'un anneau commutatif A est une partie multiplicative qui ne contient pas 0_A, c'est une partie stable par multiplication qui contient 1_A mais pas 0_A.

Le **localisé d'un anneau abélien A** par rapport à un ensemble de dénominateurs D est note $\boldsymbol{D^{-1}A}$ (risque confusion si A/D) et correspond à l'ensemble $\frac{A \times D}{R}$ avec la relation d'équivalence R définie par $(a, d)R(b, e) \Leftrightarrow \exists \delta \in D\ \delta(ae - bd) = 0_A$. On note les classes $\frac{a}{d} = (a, d)$

Le localisé d'un anneau est un anneau.

L'intuition du localisé est qu'il permet de rendre inversibles certains éléments dénominateurs de l'anneau, par exemple $\mathbb{D} = D^{-1}Z$ avec $D = \{10^n : n \in N\}$.

Le localisé est plus flexible car l'anneau n'est pas supposé intègre, au prix d'un facteur δ dans la def. Si

l'anneau est intègre, $\delta \neq 0$ ne joue pas de role, sinon il est nécessaire : $\frac{x}{1_A} = \frac{0_A}{1_A} \Leftrightarrow \exists \delta \in D\ \delta x = 0_A$

Le corps des fractions d'un anneau intègre est le localisé de A par A^*.

Dans un anneau commutatif, l'ensemble des éléments réguliers est un ensemble valide de dénominateurs, son localisé s'appelle **l'anneau total des fractions** de A.

Un anneau commutatif, quotienté par un idéal premier, forme un ensemble valide de dénominateurs, on note $\boldsymbol{A_P} = \left(\frac{A}{P}\right)^{-1} A$ son localisé. Si A est un intègre, $\langle 0_A \rangle$ est premier et $A_{\langle 0_A \rangle} = Frac(A)$.

Dans un anneau commutatif, pour un ensemble <u>non nilpotent</u> x, l'ensemble $D = \{x^n : n \in N\}$ est un ensemble valide de dénominateurs et on note $\boldsymbol{A_x}$ son localisé. Par exemple $\mathbb{D} = Z_{10}$

Attention si x est un élément premier, alors $A_{\langle x \rangle}$ est bien defini mais en general $A_{\langle x \rangle} \neq A_x$

Les dénominateurs sont les éléments qui ne sont pas des multiples de x dans $A_{\langle x \rangle}$ alors que ce sont les puissances de x dans A_x.

Tout anneau commutatif se plonge naturellement dans n'importe lequel de ses localisés comme sous-anneau par l'injection canonique $A \to D^{-1}A : a \mapsto \frac{a}{1_A}$ car elle est injective.

Dans $C^0(R, R)$ les fonctions ne s'annulant pas en 0 forment un ensemble valide de denominateurs donc on peut definir le localisé correspondant. Deux fonctions ont même image dans le localisé ssi elles coïncident localement en 0. L'anneau localisé ne distingue donc que les comportements locaux au voisinage de 0, d'où l'appellation de « localisé ».

Un anneau commutatif est dit **local** ssi il n'a qu'un seul idéal maximal.

Un anneau commutatif A est local ssi son quotient par le groupe des inversibles $\frac{A}{A^\times}$ est un ideal.

Attention : En général le localisé d'un anneau n'est pas forcément un anneau local.

Un localisé de la forme $A_P = \left(\frac{A}{P}\right)^{-1} A$ avec P idéal premier, est un anneau local.

Dans un anneau commutatif intègre A on peut identifier A et son image par injection et considerer $A \subseteq Frac(A)$, alors si $D^{-1}A$ est un localisé de A on peut aussi considérer que $A \subseteq D^{-1}A \subseteq Frac(A)$ avec $D^{-1}A = \left\{\frac{a}{d} :\ a \in A, d \in D\right\}$

Si M est un ideal maximal alors il est premier, on peut considérer $A \subseteq A_M \subseteq Frac(A)$ et donc $A_M = \left\{\frac{a}{d} : a \in A, d \notin M\right\}$

Un anneau commutatif intègre A est l'intersection de ses localisés en ses idéaux maximaux $A = \bigcap_{M \text{ ideal maximal} \subset A} A_M$

VI. Anneaux noethériens

VI.1. Définitions équivalentes

Un anneau commutatif noethérien est un anneau commutatif dans lequel tout idéal est de type fini.

Un anneau commutatif est noethérien ssi toute suite <u>croissante</u> d'idéaux est stationnaire, c'est-à-dire constante à partir d'un certain rang.

VI.2. Fabrication d'anneaux noethériens

Un anneau commutatif noethérien quotienté par un de ses idéaux est encore un anneau noethérien.

Tout localisé d'un anneau commutatif noethérien est un anneau noethérien.

Les anneaux $Z, \frac{Z}{nZ}, K[X], K[X_1, \dots, X_n]$ avec K corps sont des anneaux noethériens.

Th. de la base de Hilbert. Les polynômes à coefficients dans un anneau commutatif noethérien A,

forment un anneau commutatif noethérien $A[X]$

Autres exemples (illisible) TODO

VI.3. Anneaux artiniens

Un anneau commutatif est dit **artinien** ssi toute suite décroissante d'idéaux est stationnaire

Bien qu'il y ait beaucoup d'anneau noethériens il n'y a pas beaucoup d'anneaux artiniens.

Z n'est pas un anneau artinien : $\langle 2\rangle \supset \langle 4\rangle \supset \cdots \supset \langle 2^n\rangle \supset \cdots$ n'est pas stationnaire.

Dans un anneau noethérien, les éléments n'ont qu'un nombre fini de diviseurs.

Dans un anneau artinien, les éléments n'ont qu'un nombre fini de multiples.

Un anneau commutatif fini est toujours évidemment noethérien et artinien.

Les idéaux d'une K-algèbre sont des sous-espaces vectoriels. Si $I \subset J, I \neq J$ alors $\dim(I) < \dim(J)$

Une K-algebre de dimension finie est toujours un anneau artinien.

Un anneau commutatif artinien est soit fini, soit une K-algebre de dimension finie.

VII.1. Irréductibles ou premiers ?

Dans un anneau intègre on a: $ab|ac \Leftrightarrow b|c$; $ab|a \Leftrightarrow b \in A^\times$; $a|b$ et $b|a \Leftrightarrow a, b$ associés

Dans un anneau commutatif intègre, $a \in A^*$ est premier ⇒ a est irréductible.

Réciproque fausse en général : dans $Z\left[i\sqrt{5}\right]$, 2 est irréductible, mais n'est pas premier.

Dans un anneau principal $a \in A^*$ est irréductible ⇒ a est premier.

VII.2. Pgcd-Ppcm. Dans un anneau commutatif intègre A. Soit $a_1, \dots, a_n \in A^*$. Soit $d \in A^*, m \in A^*$

d est un pgcd de $a_1, \dots, a_n$ ssi c'est un diviseur commun et tout diviseur commun le divise.

ssi c'est un maximum pour la relation « diviser » de l'ensemble des diviseurs communs. (pas unique car « divise » pas un ordre)

ssi $\forall i \in [\![1, n]\!]\ d|a_i$ et $\forall c \in A^*\ (\forall i \in [\![1, n]\!]\ c|a_i \Rightarrow c|d)$

ssi $\langle a_1, \dots, a_n\rangle \subseteq \langle d\rangle$ et $\forall c \in A^*\ \langle a_1, \dots, a_n\rangle \subseteq \langle c\rangle \Rightarrow \langle d\rangle \subseteq \langle c\rangle$.

ssi l'ensemble des idéaux principaux contenant $\langle a_1, \dots, a_n\rangle$ admet $\langle d\rangle$ pour minimum. (unique car $\subseteq$ est un ordre)

m est un ppcm de $a_1, \dots, a_n$ ssi c'est un multiple commun et il divise tout multiple commun.

ssi c'est un minimum pour la relation « diviser » de l'ensemble des multiples communs. (pas unique)

ssi $\forall i \in [\![1, n]\!]\ a_i|m$ et $\forall c \in A^*\ (\forall i \in [\![1, n]\!]\ a_i|c \Rightarrow m|c)$

ssi $\langle m\rangle \subseteq \langle a_1\rangle \cap \dots \cap \langle a_n\rangle$ et $\forall c \in A^*\ \langle c\rangle \subseteq \langle a_1\rangle \cap \dots \cap \langle a_n\rangle \Rightarrow \langle c\rangle \subseteq \langle m\rangle$.

(ssi $\langle m\rangle \subseteq \langle a_1\rangle \cap \dots \cap \langle a_n\rangle$ et $\forall c \in A^*\ c \in \langle a_1\rangle \cap \dots \cap \langle a_n\rangle \Rightarrow c \in \langle m\rangle$.)

ssi $\langle m\rangle = \langle a_1\rangle \cap \dots \cap \langle a_n\rangle$

Si d est un pgcd (resp. ppcm) de n éléments alors l'ensemble des associés de d, est l'ensemble des pgcd (resp. ppcm) de ces mêmes éléments.

Dans Z, ou $K[X]$ on prend un représentant unitaire pour rendre le rendre unique. En général, on a pas un moyen simple de le rendre unique.

Pour un pgcd inversible, on choisit l'unité 1_A comme représentant.

Dans un anneau commutatif intègre, $ppcm(a, b)$ existe ⇒ $pgcd(a, b)$ existe.

Dans ce cas $pgcd(a, b) \times ppcm(a, b)$ est associé a ab : $pgcd(a, b)ppcm(a, b) \sim ab$

Réciproque fausse : Dans $\mathbb{Z}\left[i\sqrt{5}\right]$, $1 - i\sqrt{5}$ et 2 ont 1 pour pgcd, mais pas de ppcm.

Dans un anneau commutatif intègre, $pgcd(ac, bc)$ existe ⇒ $pgcd(a, b)$ existe.

Dans ce cas $pgcd(ac, bc) \sim c\ pgcd(a, b)$

Cette propriété permet d'exprimer tout élément de $Frac(A)$ sous forme irréductible unique.
Réciproque fausse : Dans $\mathbb{Z}[i\sqrt{5}]$, $1 - i\sqrt{5}$ et 2 ont 1 pour pgcd mais 6 et $2(1 + i\sqrt{5})$ n'en ont pas.
Dans un anneau commutatif intègre, $ppcm(ac, bc)$ existe $\Leftrightarrow ppcm(a, b)$ existe.
Dans ce cas $ppcm(ac, bc) \sim c\ ppcm(a, b)$
Un anneau commutatif intègre est un **anneau à pgcd** :
ssi tout couple d'éléments non nuls a un pgcd.
ssi tout couple d'éléments non nuls a un ppcm.
ssi tout idéal de type fini est contenu dans un idéal principal minimum.
ssi toute intersection finie d'idéaux est un idéal principal.
Les anneaux à pgcd permettent de généraliser le lemme de Gauss et d'Euclide
Deux éléments non nuls $a, b \in A^*$ d'un anneau intègre sont **premiers entre eux** et on note $\boldsymbol{a \wedge b \sim 1}$
ssi tout diviseur commun à a et à b est inversible ssi 1_A est pgcd de a et b ssi ab est $ppcm$ de a et b.
Ex : Deux polynômes de $C[X]$ sont premiers entre eux ssi ils n'ont pas de racine commune.
Un inversible d'un anneau intègre est premier avec tout autre élément de l'anneau.
Caractérisation du pgcd. Dans un anneau à pgcd, $a \wedge b \sim d \Leftrightarrow \exists a', b' \in A^* \begin{cases} a = da' \\ b = db' \\ a' \wedge b' \sim 1 \end{cases}$
Corollaire. Dans un anneau à pgcd, $ac \wedge bc \sim c(a \wedge b)$
Lemme de Gauss. Dans un anneau à pgcd pour $a, b \in A^*$, $a \wedge b \sim 1 \Leftrightarrow (\forall c \in A^*\ \ a|bc \Rightarrow a|c)$
Dans un anneau intègre, a inversible ou irréductible $\Rightarrow a$ premier avec tout élément qu'il ne divise pas (càd $\forall b \in A \setminus \langle a \rangle\ \ a \wedge b \sim 1$).
Dans un anneau à pgcd, a inversible ou irréductible $\Leftrightarrow a$ premier avec tout élément qu'il ne divise pas.
Lemme d'Euclide. Dans un anneau à pgcd avec p irréductible on a $\forall x, y \in A\ p|xy \Rightarrow p|x$ ou $p|y$
Dans un anneau à pgcd un élément est irréductible ssi il est premier.

VII.5. Anneaux de Bézout

Un anneau commutatif intègre est un **anneau de Bézout** ssi la somme de deux idéaux principaux est toujours un idéal principal, autrement dit ssi tous les idéaux de types finis sont principaux.
Tout anneau principal est un anneau de Bézout.
Un anneau de Bézout est un anneau à pgcd.
Ex : $K[X, Y]$ n'est pas de Bézout donc pas principal.
Ex : L'anneau $H(C)$ des applications holomorphes complexes est un anneau de Bézout non principal.
Ex : L'anneau $\{P \in Q[X] \mid P(0) \in Z\}$ est un anneau de Bézout. TODO vérifier illisible.
Th. de Bézout. Dans un anneau de Bézout, $a \wedge b = 1$ ssi $\exists u, v \in A\ au + bv = 1_A$.
Attention dans la terminologie classique l'intégrité n'est pas requise pour les anneaux de Bézout et les anneaux à pgcd.

VII.6. Anneaux factoriels

Rappel : Dans un anneau commutatif intègre, tout élément premier est irréductible.
Un **anneau factoriel** est un anneau commutatif intègre vérifiant l'existence et l'unicité de la décomposition en facteurs irréductibles.
$(\boldsymbol{E})$ Tout $x \in A^*$ non inversible s'écrit $a = p_1 \dots p_r$ avec $r \geq 0$ et les p_i sont des éléments irréductibles de A non nécessairement distincts.
$(\boldsymbol{U})$ La décomposition précédente est unique au sens suivant : si on a 2 décompositions $a = p_1 \dots p_r =$

$q_1 \dots q_s$ avec p_i, q_j irréductibles, alors $r = s$ et $\exists \sigma \in S_r$ tel que $\forall i$ p_i et q_{σ_i} sont associés. Autrement dit unique à ordre et facteur inversible près.
ssi :
$(\boldsymbol{E'})$ Tout $x \in A^*$ non inversible s'écrit $a = \lambda p_1^{k_1} \dots p_r^{k_r}$ avec $\geq 0, k_1, \dots, k_r \geq 1$, $\lambda \in A^\times$ et les p_i sont des éléments irréductibles de A non associés 2 à 2.
$(\boldsymbol{U'})$ Tout élément irréductible est premier. (Donc irréductible ⇔ premier)
ssi :
(E'') Toute suite croissante d'idéaux principaux est stationnaire (faible que noethérien)
(U')

VII.6.1. Caractérisation et exemples

Si A est un anneau factoriel, $A[X]$ est un anneau factoriel.
$K[X_1, \dots, X_n]$ est un anneau factoriel si K factoriel.
Dans un anneau noethérien intègre, tout élément admet une décomposition en produit fini de facteurs irréductibles, mais cette décomposition n'est généralement pas unique.
Un anneau à la fois noethérien et à pgcd est un anneau factoriel.
Un anneau principal est factoriel. $K[X_1, \dots, X_n]$ est un anneau factoriel.

VII.6.2. Valuation

La **valuation** d'un élément non nul $x \in A^*$ en un facteur $p \in A$, d'un anneau factoriel est la plus grande puissance entière de p qui divise x : $\boldsymbol{v_p(x)} = \max\{n \in N \mid p^n | x\}$, autrement dit c'est la puissance associée a p dans la decomposition de x en facteurs irréductibles, ou 0 s'il n'intervient pas.
La valuation d'un même élément non nul, en 2 facteurs associes est identique. $p \sim p' \Rightarrow v_p(x) = v_{p'}(x)$
La valuation d'un élément non nul x ne depend donc que de la classe d'association de p de $A/\sim$.
Grace à l'axiome du choix on peut extraire un ensemble de représentants irréductibles P.
Dans Z on choisit traditionnellement les nombres premiers positifs, dans $K[X]$ on choisit traditionnellement les polynômes unitaires. Donc pour tout irréductible il admet un représentant dans P, et deux éléments de P associés ne peuvent être que le même élément représentant sa classe.
Dans un anneau factoriel on peut donc écrire $\forall x \in A^*$ $x = u \prod_{p \in P} p^{v_p(x)}$ avec $u \in A^\times$, cette écriture est unique a ordre près.
Dans un anneau factoriel pour tout p irréductible et tous éléments $x, y \in A^*$
on a $v_p(xy) = v_p(x) + v_p(y)$
Dans un anneau factoriel pour $x, y \in A^*$ on a $x|y \Leftrightarrow \forall p \in P\ v_p(x) \leq v_p(y)$
Dans un anneau factoriel, si $a = \prod_{p \in P} p^{\alpha_p}$, $b = \prod_{p \in P} p^{\beta_p}$ alors $pgcd(a,b) \sim \prod_{p \in P} p^{\min(\alpha_p, \beta_p)}$, $ppcm(a,b) \sim \prod_{p \in P} p^{\max(\alpha_p, \beta_p)}$. Ainsi tout anneau factoriel, est un anneau à pgcd.
Un anneau de Bézout est à PGCD.
Un anneau factoriel est à PGCD.
Un anneau de Bézout n'est pas forcément factoriel.
Un anneau factoriel n'est pas forcément de Bézout.
Un anneau est principal ssi il est factoriel et de Bézout.

VIII. Quelques conséquences amusantes

VIII.1. L'équation $x^2 + y^2 = z^2$ TODO

VIII.2. L'équation $x^4 + y^4 = z^4$ TODO

VIII.3. Les sommes des deux carrés TODO

Un entier n est somme de deux carrés ssi les nombres premiers qui apparaissent avec une puissance impaire dans la décomposition de n en facteurs premiers, sont 2 ou congrus a 1 mod 4.

VIII.4. L'anneau $Z[i\sqrt{d}]$ TODO

L'anneau $Z[i\sqrt{d}]$ est principal ssi $d = 1$ ou $d = 2$.

Anneau intégralement clos. Un anneau commutatif intègre A est **intégralement clos** ssi $\forall p \in A\ \forall q \in A^*\ \forall P \in A[X]$ tel que P unitaire, $P\left(\frac{p}{q}\right) = 0 \Rightarrow \frac{p}{q} \in A$.

Tout anneau à PGCD est intégralement clos.

Complément. Les nombres premiers

1. A quoi servent les nombres premiers

RSA : on choisit p, q premiers tres grands, on calcule $n = pq$, et $m = (p-1)(q-1) = \varphi(n)$, on choisit e puis on calcule d tel que $ed = 1\ mod\ m$ c'est-à-dire $d = e^{-1}$ dans $\left(\frac{Z}{mZ}\right)^{\times}$.

Un message x se crypte en un message $y = x^e\ mod\ n$, le message y se décrypte en $x = y^d\ mod\ n$.

La clé publique (pour crypter) est donc (e, n). La clé privée (pour décrypter) est donc d (n est publique).

Ça marche car $y^d\ mod\ n = x^{ed}\ mod\ n = x^{1+mk}\ mod\ n = x\ mod\ n$. n n'est pas facile à factoriser.

2. Comment trouver un grand nombre premier

On peut utiliser les nombres de **Mersenne** c'est-à-dire de la forme $M(n) = 2^n - 1$. On ne sait pas fabriquer de grands nombres premiers facilement. On note $\pi(n)$ le nombre de premiers $\leq n$.

Th. des nombres premiers. $\pi(n) \sim_{n\to\infty} n/\ln(n)$

3. Test de pseudo-primalité

Un nombre $n \geq 2$ est **probablement premier de base $b \geq 2$** ssi $b^n = b\ mod\ n$.

Si de plus n non premier, on dit que n est **pseudo-premier** de base b.

Test : 1) on choisit un certain nombre d'entiers $b_1, \dots, b_k$

2) on calcule pour tout i, $b_i^n\ mod\ n$ pour determiner si n est probablement premier de base b_i.

3) si pour au moins un i le test echoue, on conclut que n n'est pas premier.

4) sinon on conclut que n est premier

Si le test marche on veut estimer la marge d'erreur. (faux positifs).

4. Les nombres de Carmichael

Un entier de Carmichael, est un entier non premier, qui est probablement premier pour toute base de N. Autrement dit c'est un faux positif dans le test de pseudo-primalite.

Rappel : Dans un groupe fini, l'ensemble $\{e \in Z \mid \forall g \in G\ g^e = 1_G\}$ est un ideal de Z et l'exposant $\omega(G)$ de G est le generateur positif de cet idéal. Comme $\{e \in Z \mid \forall g \in G\ g^e = 1_G\} = \bigcap_{g\in G}\{e \in Z \mid g^e = 1_G\}$ il s'ensuit que $\omega(G) = ppcm(ord(g) : g \in G)$

On définit **l'indicatrice de Carmichael** $\omega: N \to N$ par $\omega(0) = \omega(1) = 1$ et $\omega(n \geq 2) = \omega\left(\left(\frac{Z}{nZ}\right)^{\times}\right)$

Elle ressemble à l'indicatrice d'Euler, mais est différente, $\forall n\ \omega(n) | \phi(n)$.

Si n nombre de Carmichael alors $n - 1$ multiple de $\omega(n)$

Si un nombre $n \in N^*$ admet un facteur premier p tel que $p^2 | n$, n n'est pas un nombre de Carmichael.

Autrement dit les valuations d'un nombre de Carmichael sont soit 1 soit 0. Cela restreint les possibilités.
Si $n = p_1 \dots p_k$ avec p_i premiers distincts, alors n nombre de Carmichael ssi $\forall i\ p_i - 1 | n - 1$
Si $n = p_1 \dots p_k$ avec p_i premiers distincts <u>impairs</u>, est un nombre de Carmichael, alors $\forall i\ p_i - 1 | \frac{n}{p_i} - 1$
Si les nombres $6k+1, 12k+1, 18k+1$ sont tous premiers alors $n = (6k+1)(12k+1)(18k+1)$ est un nombre de Carmichael.
Pour n suffisamment grand il existe au moins $n^{\frac{2}{7}}$ nombres de Carmichael entre 1 et n.

Exemples et contre-exemples.

Anneau non nul intègre

Les anneaux Z, Q, R sont des anneaux intègres.
Si A intègre, $A[X]$ intègre.
Si A intègre, $A[X_1, \dots, X_n]$ intègre.

Anneau principal

Z est un anneau principal.
Si K est un corps, $K[X]$ est un anneau principal.
$Z[i\sqrt{d}]$ est principal ssi $d = 1$ ou $d = 2$
Si A est un anneau commutatif, alors ($A[X]$ est un anneau principal ssi A est un corps)

Anneau euclidien

$(Z, +, \times)$ est un anneau euclidien muni du stathme euclidien $n \mapsto n$.
$K[X]$ est un anneau euclidien muni du stathme euclidien $P \mapsto \deg(P)$
$Z[i]$ est un anneau euclidien muni du stathme euclidien $v: Z[i] \to N: x + iy \mapsto x^2 + y^2 = |x + iy|^2$
$Z, K[X], Z[i]$ sont des anneaux euclidiens donc principaux.
$K[X, Y]$ n'est pas un anneau principal donc pas euclidien.
$Z[X]$ est un anneau non euclidien.
$Z\left[\frac{1+i\sqrt{19}}{2}\right]$ est un anneau principal non euclidien.

Anneau réduit ($nil(A) = \{0_A\}$)

Anneau noethérien

Les anneaux $Z, \frac{Z}{nZ}, K[X], K[X_1, \dots, X_n]$ avec K corps sont des anneaux noethériens.
Si A anneau noethérien, alors $A[X_1, \dots, X_n]$ noethérien.
$A[(X_n)_{n\in\mathbb{N}}]$ n'est pas noethérien.

Anneau artinien

Z n'est pas un anneau artinien.

Anneau à pgcd (somme de deux idéaux principaux est contenue dans un idéal principal minimal)

Si A anneau à pgcd, alors $A[X]$ à pgcd.
Il existe des anneaux intègres à PGCD qui ne sont pas factoriels (prendre un anneau de Bézout non factoriel comme l'anneau des entiers algébriques)
Il existe des anneaux intègres à PGCD qui ne sont pas de Bézout (par exemple un anneau factoriel noethérien non principal : $\mathbb{Q}$[X,Y] ou $\mathbb{Z}$[X]).
Il existe des anneaux intègres à PGCD qui ne sont ni factoriels ni de Bézout (par ex : $A[X]$ où A est un anneau à PGCD non factoriel, comme l'anneau des entiers algébriques)

Anneau de Bézout (somme de deux idéaux principaux est un idéal principal)
L'anneau $H(C)$ des applications holomorphes complexes est un anneau de Bézout non principal, donc non factoriel.
L'anneau $\{P \in Q[X] \mid P(0) \in Z\}$ est un anneau de Bézout. TODO vérifier
Anneau factoriel (existence et unicité de la décomposition en facteurs irréductibles)
Si A est un anneau factoriel, $A[X]$ est un anneau factoriel.
Si A est un anneau factoriel, $A[X_1, \dots, X_n]$ est un anneau factoriel.
Si A est un anneau factoriel, $A[(X_n)_{n\in\mathbb{N}}]$ est un anneau factoriel.
$\frac{Z[T]}{T^2+5}$ est un anneau intègre, noethérien mais pas factoriel.

Propriétés de hiérarchie des structures
Corps algébriquement clos => corps => anneau euclidien => anneau principal => anneau factoriel => anneau à PGCD => anneau intégralement clos => anneau intègre => anneau commutatif => anneau.
Un anneau commutatif est intègre ssi $\langle 0_A \rangle$ est un idéal premier.
Un anneau intègre est réduit.
Dans un anneau commutatif, un idéal propre est un idéal premier ssi $\frac{A}{I}$ est un anneau intègre.
Un corps est un anneau intègre.
Les corps finis sont les anneaux intègres finis.
Les anneaux inclus dans des corps sont des anneaux intègres.
Dans un anneau commutatif, un idéal propre est maximal ssi $\frac{A}{I}$ est un corps.
Dans un anneau <u>principal</u>, a irréductible ssi $\langle a \rangle$ idéal maximal, ssi $\frac{A}{\langle a \rangle}$ est un corps.
Dans un anneau commutatif, un idéal est radical ssi $\frac{A}{I}$ est un anneau réduit.
Un anneau principal est commutatif intègre. (par définition)
Un anneau principal est un anneau de Bézout, donc est un anneau à pgcd.
Un anneau principal est factoriel.
Un anneau euclidien est commutatif intègre. (par définition)
Un anneau euclidien est principal.
Un anneau commutatif fini est noethérien et artinien.
Si A anneau commutatif noethérien et I idéal de A, alors $\frac{A}{I}$ anneau noethérien.
Un localisé d'un anneau commutatif noethérien est un anneau noethérien.
Une K-algebre de dimension finie est un anneau artinien.
Un anneau commutatif artinien est soit fini, soit une K-algebre de dimension finie.
Un anneau à pgcd est commutatif intègre. Attention dans la terminologie classique pas intègre.
Un anneau noethérien et à pgcd est un anneau factoriel.
Plus précis : Un anneau intègre est factoriel ssi c'est un anneau à pgcd principalement noethérien.
Un anneau de Bézout est commutatif intègre. Attention dans la terminologie classique pas intègre.
Un anneau de Bézout est un anneau à pgcd.
Un anneau factoriel est commutatif intègre. (par définition)
Un anneau factoriel, est un anneau à pgcd.

Les anneaux factoriels de Bézout, sont les anneaux principaux.
Dans un anneau commutatif, un idéal maximal est toujours premier.
Dans un anneau commutatif intègre, tout élément premier est irréductible.
Un anneau intègre est factoriel ssi toute suite croissante d'idéaux principaux est stationnaire et tout élément irréductible est un élément premier.