Leçon 122 - Anneaux principaux. Exemples et applications.

Extrait du rapport de jury

Cette leçon ne doit pas se cantonner aux aspects théoriques. L'arithmétique des anneaux principaux doit être décrite et les démonstrations doivent être maîtrisées (lemme d'Euclide, théorème de Gauss, décomposition en irréductibles, PGCD et PPCM, équations du type $ax + by = d$, etc.). On doit présenter des exemples d'utilisation effective du lemme chinois. Les anneaux euclidiens représentent une classe importante d'anneaux principaux et l'algorithme d'Euclide a toute sa place dans cette leçon pour effectuer des calculs. Les applications en algèbre linéaire ne manquent pas et doivent être mentionnées (par exemple, le lemme des noyaux ou la notion de polynôme minimal pour un endomorphisme, pour un endomorphisme relativement à un vecteur ou pour un nombre algébrique). Si les anneaux classiques $\mathbb{Z}$ et $\mathbb{K}[X]$ doivent impérativement figurer, il est possible d'en évoquer d'autres (décimaux, entiers de Gauss $\mathbb{Z}[i]$ ou d'Eisenstein $\mathbb{Z}[j]$) accompagnés d'une description de leurs inversibles, de leurs irréductibles, en lien avec la résolution de problèmes arithmétiques (équations diophantiennes).
Les candidates et candidats peuvent aller plus loin en s'intéressant à l'étude des réseaux, à des exemples d'anneaux non principaux, mais aussi à des exemples d'équations diophantiennes résolues à l'aide d'anneaux principaux. À ce sujet, il sera fondamental de savoir déterminer les unités d'un anneau, et leur rôle au moment de la décomposition en facteurs premiers. De même, la résolution des systèmes linéaires sur $\mathbb{Z}$ ou le calcul effectif des facteurs invariants de matrices à coefficients dans un anneau principal peuvent être présentés en lien avec ce sujet

Présentation de la leçon

Je vais vous présenter la leçon 122 intitulée : "Anneaux principaux. Exemples et applications". Euler est le premier en 1770 à étendre la notion de divisibilité aux entiers de corps quadratiques, mais Lagrange montre peu après que ces anneaux ne sont pas tous principaux. La généralisation de l'arithmétique sur $\mathbb{Z}$ est alors sans trop d'espoirs, mais Kummer puis Dedekind et Kronecker éclairent la théorie des nombres d'un jour nouveau en introduisant la notion d'idéaux, et dégageant l'excellente structure arithmétique des anneaux principaux qui va permettre de généraliser les propriétés des anneaux classiques, et notamment de $\mathbb{Z}$ avec son arithmétique !
On s'intéresse dans la première partie aux généralités sur les anneaux principaux ainsi que les liens existants entre ces anneaux et d'autres types d'anneaux. On introduit tout d'abord la définition d'idéal qui est indispensable pour définir les structures d'idéal principal ainsi que d'anneau principal. On donne également la définition d'idéal maximal et premier. Ainsi, grâce à cette définition, on voit que l'anneau $\mathbb{Z}$ et tous les corps sont principaux, ce qui rejoint bien ce que nous disions en préambule de cette leçon. De plus, il est possible de dégager une classe importante d'anneaux principaux qui sont les anneaux euclidiens. Ces anneaux continuent de jouir des propriétés issues de la principalité mais possèdent en plus une division euclidienne ! On peut par exemple citer $\mathbb{Z}$ ou $\mathbb{K}[X]$. On justifie ensuite de ces anneaux sont bien principaux et que cet ensemble d'anneaux est strictement contenu dans les anneaux principaux. On termine enfin en montrant que $A[X]$ est principal si, et seulement si, A est un corps grâce à l'euclidianité. Pour conclure cette partie, nous allons voir qu'il est possible de plonger les anneaux principaux dans un type d'anneau plus général : les anneaux factoriels. Tout d'abord, on commence par définir la notion d'élément irréductible (qui coïncide avec les nombres premiers dans le cas de $\mathbb{Z}$ (c'est fait pour !)) ce qui nous permet de définir dans la foulée les anneaux factoriels. On remarquera que l'unicité de la décomposition en produit d'irréductibles est essentielle d'après la remarque 23. On termine cette sous-partie en montrant que tout anneau principal est bien factoriel ainsi que le théorème du transfert. Celui-ci nous permet au passage de justifier que la classe des anneaux principaux est strictement incluse dans celle des anneaux factoriels.
Dans le deuxième partie, on s'intéresse à l'arithmétique qui peut être associée aux anneaux principaux (car c'est surtout ce qui nous intéresse avec cette notion !). Puisque les anneaux principaux sont des anneaux factoriels, on peut d'abord commencer à s'intéresser à l'arithmétique dans cette structure anneau. Il est possible d'y définir une divisibilité qui conduit naturellement à la notion d'éléments associés et de nombres premiers entre eux. Le but de tout cela étant de définir la notion de PGCD et de PPCM comme dans le cadre de $\mathbb{Z}$. Maintenant que les principaux outils sont définis, nous allons voir quelles propriétés supplémentaires ceux-ci possèdent dans un anneau principal. Tout d'abord, il est possible de caractériser les PGCD et les PPCM au moyen des idéaux ainsi qu'une relation de Bézout entre deux éléments premiers entre eux. Ces deux notions conduisent finalement aux lemmes d'Euclide et de Gauss concernant la divisibilité qui sont très utiles en arithmétique. On termine cette partie en énonçant

l'algorithme d'Euclide ainsi qu'un exemple en application.
On conclut enfin cette leçon par une dernière partie où l'on donne des applications à la notion de principalité. Tout d'abord, dans le cadre de l'algèbre linéaire, la principalité joue un rôle crucial pour définir le polynôme minimal d'un endomorphisme. Cette notion de polynôme minimal ainsi que le lemme de noyaux (qui repose entièrement sur la relation de Bézout !) permettent d'établir la décomposition de Dunford et de donner une caractérisation très importante de la diagonalisabilité. On continue ensuite en étudiant l'anneau des entiers de Gauss $\mathbb{Z}[i]$, en montrant qu'il est euclidien, en donnant notamment ses inversibles ainsi que ses irréductibles. On y démontre également le théorème des deux carrés et on donne dans la proposition 54 la description de l'anneau des entiers d'Eisenstein $\mathbb{Z}[j]$. On termine enfin cette leçon avec le théorème des restes chinois ainsi qu'une application à la résolution des équations diophantiennes.
On trouvera également en annexe un schéma bilan des liens entre les différents types d'anneaux étudiés dans cette leçon.

Plan général

Cours détaillé

Dans toute cette leçon, on considère $(A, +, \cdot)$ un anneau commutatif, unitaire, intègre et non nul et $\mathbb{K}$ un corps.

I Généralités

I.1 Idéaux principaux et anneaux principaux

Définition 1 : Idéal [Rombaldi, p.215] :
On dit que $I \subseteq A$ est un **idéal** de A lorsque :
$*$ $(I, +)$ est un sous-groupe de $(A, +)$.
$*$ Pour tout $a \in A$ et tout $x \in I$, on a $ax \in I$.

Définition 2 : Idéal maximal [Perrin, p.43] :
Un idéal I de A est un **idéal maximal** lorsque $I \neq A$ et pour tout idéal J de A tel que $I \subseteq J$ et $J \neq A$ on ait $I = J$.

Proposition 3 : [Perrin, p.43]
Soit I un idéal de A.
I est un idéal maximal de A si, et seulement si, A/I est un corps.

Définition 4 : Idéal premier [Perrin, p.43] :
Un idéal I de A est un **idéal premier** lorsque $I \neq A$ et :

$$\forall a, b \in A,\ (ab \in I) \implies (a \in I \text{ ou } b \in I)$$

Proposition 5 : [Perrin, p.43]
Soit I un idéal de A.
I est un idéal premier de A si, et seulement si, A/I est un anneau intègre.

Corollaire 6 : [Perrin, p.43]
Tout idéal maximal de A est un idéal premier.

Proposition 7 : [Perrin, p.43]
Les idéaux premiers et maximaux de $\mathbb{Z}$ sont les $p\mathbb{Z}$ avec p un nombre premier au sens usuel.

Définition 8 : Idéal principal [Perrin, p.42] :
Un idéal I de A est un **idéal principal** lorsqu'il existe $a \in A$ tel que I est l'idéal engendré par a (on note alors $I = (a)$).

Définition 9 : Anneau principal [Perrin, p.49] :
Un anneau est un **anneau principal** lorsque celui-ci est intègre et que tous ses idéaux sont principaux.

Exemple 10 : [Rombaldi, p.237]
L'anneau $\mathbb{Z}$ ainsi que tout les corps $\mathbb{K}$ sont principaux.

Proposition 11 : [Rombaldi, p.241]
Soit $a \in A$ non nul.
Si A est un anneau principal, alors on a les équivalences suivantes :

$(a \text{ est premier}) \iff ((a) \text{ premier}) \iff ((a) \text{ maximal}) \iff (a \text{ est irréductible})$

I.2 Un cas particulier d'anneaux principaux : les anneaux euclidiens

Définition 12 : Anneau euclidien [Perrin, p.50] :
L'anneau A est un **anneau euclidien** lorsque A est intègre et que A est muni d'une division euclidienne (parfois appelée stathme) $v : A\backslash\{0_A\} \longrightarrow \mathbb{N}$ telle que pour $a, b \in A\backslash\{0_A\}$, il existe $q, r \in A$ où $a = bq + r$ et $(r = 0$ ou $v(r) < v(b))$.

Lemme 13 : [Perrin, p.50]
Soit $P \in A[X]$ non nul et de coefficient dominant inversible.
Pour tout $F \in A[X]$, il existe deux polynômes $Q, R \in A[X]$ tels que $F = PQ + R$ et $(\deg(R) < \deg(P)$ ou $R = 0)$.

Proposition 14 : [Perrin, p.50]
L'anneau $\mathbb{K}[X]$ est un anneau euclidien avec comme stathme le degré des polynômes.

Exemple 15 : [Perrin, p.50]
* L'anneau $\mathbb{Z}$ muni de la valeur absolue est un anneau euclidien.
* L'anneau $\mathbb{K}[X]$ avec comme stathme le degré des polynômes est euclidien.
* L'anneau $\mathbb{D}$ des nombres décimaux (sous-anneau de $\mathbb{Q}$ engendré par $\mathbb{Z}$ et $\frac{1}{10}$) est euclidien.
* L'anneau $\mathbb{K}[[X]]$ des séries formelles est un anneau euclidien.

Proposition 16 : [Perrin, p.50]
Tout anneau euclidien est principal

Attention, la réciproque de la proposition précédente est fausse comme le montre l'exemple suivant :

Exemple 17 : [Perrin, p.53]
Les anneaux $\mathbb{Z}\left[\frac{1}{2}(1 + i\sqrt{19})\right]$ et $\mathbb{R}[X, Y]/(X^2+Y^2+1)$ sont des anneaux principaux mais non euclidiens.

Proposition 18 : [Perrin, p.51]
L'anneau $A[X]$ est principal si, et seulement si, A est un corps.

I.3 Une généralisation des anneaux principaux : les anneaux factoriels

Définition 19 : Élément irréductible [Perrin, p.46] :
On considère $p \in A$.
On dit que p est un **élément irréductible de** A lorsque p est non inversible et $(p = ab) \implies (a \in A^\times$ ou $b \in A^\times)$.

Exemple 20 : [Perrin, p.47]
Les éléments irréductibles de $\mathbb{Z}$ sont les nombres premiers (au sens usuel) ainsi que leurs opposés.

Définition 21 : Anneau factoriel [Perrin, p.47] :
L'anneau A est un **anneau factoriel** lorsque :
* A est intègre.
* Tout élément a de A non nul s'écrit sous la forme $a = u\prod_{i=1}^{r} p_i$, avec r un entier naturel, $u \in A^\times$ et $p_1, ..., p_r$ sont des éléments irréductibles.
* La décomposition précédente est unique à permutation près et à inversibles près.

Remarque 22 : [Perrin, p.47]
Soit $\mathcal{P}$ est un système de représentants des irréductibles de A.
L'anneau A est factoriel lorsque :
* A est intègre.
* Tout élément a de A non nul s'écrit sous la forme $a = u\prod_{p\in\mathcal{P}} p^{v_p(a)}$, avec $u \in A^*$ et $v_p(a) \in \mathbb{N}$ nuls sauf en un nombre fini de p.
* La décomposition précédente est unique.

Remarque 23 : [Perrin, p.48]
L'unicité de l'écriture de la définition précédente est essentielle. En effet, dans l'anneau $A = \mathbb{Z}\left[i\sqrt{5}\right] = \{a + ib\sqrt{5},\ a, b \in \mathbb{Z}\}$ on a :

$$9 = 3 \times 3 = (2 + i\sqrt{5})(2 - i\sqrt{5})$$

où 3, $2 + i\sqrt{5}$ et $2 - i\sqrt{5}$ sont des éléments irréductibles...

Théorème 24 : [Perrin, p.49]
Tout anneau principal est factoriel.

Théorème 25 : Théorème du transfert [Perrin, p.51] :
Si A est un anneau factoriel, alors $A[X]$ est un anneau factoriel.

La réciproque du théorème 24 est cependant fausse comme le montre l'exemple suivant :

Exemple 26 : [Perrin, p.53]
∗ $\mathbb{Z}[X]$ est un anneau factoriel (car $\mathbb{Z}$ l'est) mais pas principal.
∗ L'anneau $\mathbb{K}[X,Y]$ n'est pas principal bien que factoriel (par le théorème du transfert).

II Arithmétique dans les anneaux principaux

II.1 Divisibilité et éléments premiers entre eux

Dans toute cette sous-partie, on considère A un anneau factoriel, deux éléments a et b de A et $p \in A\backslash\{0_A\}$.

Définition 27 : Divisibilité [Perrin, p.46] :
On dit que a **divise** b lorsqu'il existe $c \in A$ tel que $b = ac$ (et on note $a|b$).

Proposition 28 : [Perrin, p.46]
b divise a si, et seulement si, $(a) \subseteq (b)$.

Définition 29 : Éléments associés [Perrin, p.46] :
On dit que a et b sont des **éléments associés** lorsqu'il existe $u \in A^\times$ tel que $a = bu$.

Définition 30 : Éléments premiers entre eux [Perrin, p.46] :
On dit que a et b sont **premiers entre eux** (ou encore étrangers) lorsque :

$$\forall d \in A,\ (d|a \text{ et } d|b) \implies (d \in A^\times)$$

Définition 31 : PGCD et PPCM :
On considère $\mathcal{P}$ un système de représentants des irréductibles de A et deux éléments $a = u\prod_{p\in\mathcal{P}} p^{v_p(a)}$ et $b = v\prod_{p\in\mathcal{P}} p^{v_p(b)}$ de A.
On dit que $\prod_{p\in\mathcal{P}} p^{\max(v_p(a),v_p(b))}$ est **un PPCM de a et b** et que $\prod_{p\in\mathcal{P}} p^{\min(v_p(a),v_p(b))}$ est **un PGCD de a et b**.

Remarque 32 :
∗ Les PPCM et PGCD ainsi définis sont uniques à association près.
∗ Ces PGCD et PPCM satisfont les propriétés usuelles concernant la division et la multiplication.

II.2 PGCD et PPCM

Dans toute cette partie, on considère A un anneau principal et deux éléments $a, b \in A$.

Proposition 33 : [Perrin, p.49]
Soient $p, m \in A$.
p est un PGCD (respectivement m est un PPCM) de a et b si, et seulement si, c'est un générateur de l'idéal $(a)+(b)$ (respectivement $(a)\cap(b)$).

Théorème 34 : Théorème de Bézout [Perrin, p.49] :
a et b sont premiers entre eux si, et seulement si, il existe $u, v \in A$ tels que $au + bv = 1$.

Remarque 35 : [Perrin, p.49]
La proposition précédente est mise en défaut dans un anneau factoriel non principal. En effet, l'anneau $\mathbb{K}[X,Y]$ est factoriel, X et Y sont premiers entre eux, mais on a $(X)+(Y) = (X,Y) \neq (1)$.

Lemme 36 : Lemme d'Euclide [Perrin, p.48] :
Si p est irréductible et p divise ab, alors (p divise a ou p divise b).

Lemme 37 : Lemme de Gauss [Perrin, p.48] :
Soit $c \in A\backslash\{0_A\}$.
Si a divise bc et que a est premier avec b, alors a divise c.

II.3 Algorithme d'Euclide

Dans toute cette partie, on suppose que A est un anneau euclidien avec un stathme noté φ.

Théorème 38 : Algorithme d'Euclide :
Soient $a, b \in A$ non nuls avec $\varphi(b) \leq \varphi(a)$.
Si r est le reste de la division euclidienne de a par b, alors le PGCD de a et b est le même que celui de b et r.

Exemple 39 :
∗ Un PGCD de 255 et 141 est 3.
∗ Un PGCD de $X^3 - X^2 - X + 1$ par $X^2 - 3X + 2$ est $X - 1$.

III Applications

III.1 Algèbre linéaire

Dans toute cette sous-partie, on considère E un $\mathbb{K}$-espace vectoriel de dimension finie et $u \in \mathcal{L}(E)$.

Proposition 40 : [Berhuy, p.942]
L'application :

$$\mathrm{ev}_u : \left| \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathcal{L}(E) \\ P & \longmapsto & P(u) \end{array} \right.$$

est un morphisme de $\mathbb{K}$-algèbres associatives unitaires et $\mathbb{K}[u]$ est une sous-algèbre commutative de $\mathcal{L}(E)$.

Définition 41 : Polynôme minimal [Deschamps, p.97] :
On appelle **polynôme minimal de** u le générateur unitaire du noyau de ev_u et on le note π_u.

Lemme 42 : [Rombaldi, p.608]
Soient r un entier naturel supérieur ou égal à 2, $P_1, ..., P_r$ des polynômes non nuls de $\mathbb{K}[X]$ et $Q_1, ..., Q_r$ les polynômes définis par $Q_k = \prod_{j=1, j\neq k}^{r} P_j$.
Si les polynômes P_k sont deux à deux premiers entre eux dans $\mathbb{K}[X]$, alors les polynômes Q_k sont premiers entre eux dans leur ensemble et pour tout $k \in [\![1; p]\!]$, P_k et Q_k sont premiers entre eux.

Lemme 43 : Lemme des noyaux [Rombaldi, p.609] :
Soient r un entier naturel supérieur ou égal à 2, $P_1, ..., P_r$ des polynômes non nuls de $\mathbb{K}[X]$ deux à deux premiers entre eux et $P = \prod_{i=1}^{r} P_k$.
On a alors la décomposition $\mathrm{Ker}(P(u)) = \bigoplus_{i=1}^{r} \mathrm{Ker}(P_i(u))$ et les différents projecteurs $\pi_k : \mathrm{Ker}(P(u)) \longrightarrow \mathrm{Ker}(P_k(u))$ sont des éléments de $\mathbb{K}[u]$.

Théorème 44 : Décomposition de Dunford [Rombaldi, p.613]
Si le polynôme caractéristique de u est scindé sur $\mathbb{K}$, alors il existe un unique couple (d, n) d'endomorphismes de E tel que d est diagonalisable, n est nilpotent, d et n commutent et $u = d + n$.
De plus, d et n sont des polynômes en u.

Proposition 45 : [Deschamps, p.88 + 102]
Les assertions suivantes sont équivalentes :
∗ u est diagonalisable.
∗ u possède un polynôme annulateur scindé à racines simples.
∗ π_u est scindé à racines simples.

III.2 L'anneau des entiers de Gauss

Dans toute cette sous-partie, on pose $\Sigma = \{n \in \mathbb{N} \text{ tq } n = a^2 + b^2,\ a, b \in \mathbb{N}\}$, $\mathcal{P}$ l'ensemble des nombres premiers (au sens usuel) et une application (qui est multiplicative) $N : a + ib \longmapsto a^2 + b^2$ définie de $\mathbb{Z}[i]$ dans $\mathbb{N}$.

Définition 46 : L'anneau $\mathbb{Z}[i]$ [Perrin, p.56] :
On appelle **anneau** $\mathbb{Z}[i]$ l'anneau $\mathbb{Z}[i] = \{a + ib,\ (a, b) \in \mathbb{Z}^2\}$ muni de l'addition et de la multiplication usuelles.

Remarque 47 :
$\mathbb{Z}[i]$ reste un anneau intègre car inclus dans $\mathbb{C}$, cependant les nombres premiers (au sens usuel) qui sont somme de deux carrés ne sont plus irréductibles dans $\mathbb{Z}[i]$ (par exemple $5 = (2 + i)(2 - i)$).

Proposition 48 : [Perrin, p.56]
$\mathbb{Z}[i]^\times = \{-1; 1; -i; i\}$.

Proposition 49 : [Perrin, p.56]
L'ensemble Σ est stable par multiplication.

Proposition 50 : [Perrin, p.57]
L'anneau $\mathbb{Z}[i]$ est euclidien pour le stathme N.

Développement 1 : [cf. PERRIN]

Lemme 51 : [Perrin, p.57]
Soit $p \in \mathcal{P}$.
Les assertions suivantes sont équivalentes :
∗ $p \in \Sigma$. ∗ L'élément p n'est pas irréductible dans $\mathbb{Z}[i]$.
∗ On a $p = 2$ ou $p \equiv 1$ [4]

Théorème 52 : Théorème des deux carrés [Perrin, p.58] :
Soit $n = \prod_{p \in \mathcal{P}} p^{v_p(n)} \in \mathbb{N}$.
$n \in \Sigma$ si, et seulement si, pour tout $p \in \mathcal{P}$ vérifiant $p \equiv 3$ [4], l'entier $v_p(n)$ est pair.

Proposition 53 : [Perrin, p.58]
Les irréductibles de $\mathbb{Z}[i]$ sont, aux éléments inversibles près :
∗ Les entiers premiers $p \in \mathbb{N}$ tels que $p \equiv 3$ [4].
∗ Les entiers de Gauss $a + ib$ dont la norme est un nombre premier.

Proposition 54 : [Berhuy, p.530]
L'anneau $\mathbb{Z}[j] = \{a + bj,\ (a,b) \in \mathbb{Z}^2\}$ est un anneau euclidien qui possède 6 éléments inversibles.

III.3 Le théorème des restes chinois

Dans toute cette sous-partie, on suppose que l'anneau A est principal.

Développement 2 : [cf. ROMBALDI]

Lemme 55 : [Rombaldi, p.249]
Soient $a_1, ..., a_r$ des éléments deux à deux premiers entre eux de A.
Si l'on pose pour tout $j \in [\![1; r]\!]$, $b_j = \prod_{\substack{i=1 \\ i \neq j}}^{r} a_j$, alors les b_j sont premiers entre eux dans leur ensemble.

Théorème 56 : Théorème des restes chinois [Rombaldi, p.249] :
Soient $a_1, ..., a_r$ des éléments de A deux à deux premiers entre eux.
L'application :

$$\varphi : \left| \begin{array}{ccc} A & \longrightarrow & \prod_{i=1}^{r} A/(a_i) \\ x & \longmapsto & (\pi_1(x), ..., \pi_r(x)) \end{array} \right.$$

est un morphisme d'anneaux surjectif de noyau $\left(\prod_{i=1}^{r} a_i\right)$.

On a donc en particulier :

$$A\Big/\left(\prod_{i=1}^{r} a_i\right) = \prod_{i=1}^{r} A/(a_i)$$

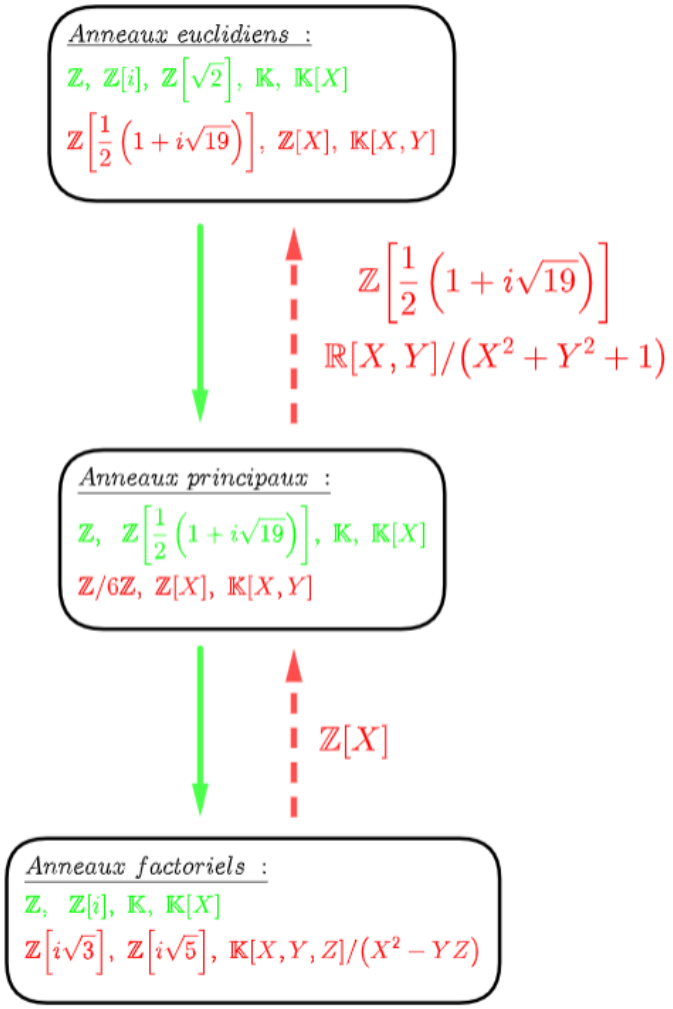
Exemple 57 : [Rombaldi, p.291]
Le système d'équations diophantiennes :

$$(S) \begin{cases} k \equiv 2 & [4] \\ k \equiv 3 & [5] \\ k \equiv 1 & [9] \end{cases}$$

possède pour solution particulière $k_0 = 118$ et l'ensemble des solutions à ce système d'équations diophantiennes est $\{118 + 180n,\ n \in \mathbb{Z}\}$.

IV Annexe

IV.1 Schéma bilan des liens entre les différents types d'anneaux étudiés



Remarques sur la leçon

— Il faut bien faire attention à la manipulation des objets : les PGCD et PPCM peuvent être définis dans le cadre d'anneaux principaux et factoriels mais la définition n'est pas la même !

— Il faut également bien comprendre ce que chaque catégorie d'anneau étudiée ici apporte par rapport aux autres.

— On peut également parler d'endomorphismes cycliques, semi-simples et donner la décomposition de Dunford à partir du lemme des noyaux.

Liste des développements possibles

— Théorème des deux carrés.

— Théorème des restes chinois + application.

Bibliographie

— Jean-Étienne Rombaldi, *Mathématiques pour l'agrégation, Algèbre et géométrie*.

— Daniel Perrin, *Cours d'algèbre*.

— Grégory Berhuy, *Algèbre : Le grand combat*.

— Claude Deschamps, *Tout-en-un MP/MP**.