Leçon 142 - PGCD et PPCM, algorithmes de calcul. Applications.

Extrait du rapport de jury

Le candidat doit prendre soin de différencier le cadre théorique des anneaux factoriels ou principaux dans lequel sont définis les PGCD et PPCM et dans lequel s'appliquent les énoncés des théorèmes proposés et le cadre euclidien fournissant les algorithmes. Le champ d'étude de cette leçon ne peut se limiter au cas de $\mathbb{Z}$, mais la leçon peut opportunément s'illustrer d'exemples élémentaires d'anneaux euclidiens, comme $\mathbb{Z}$ et $\mathbb{K}[X]$.
Une part substantielle de la leçon doit être consacrée à la présentation d'algorithmes : algorithme d'Euclide, algorithme binaire, algorithme d'Euclide étendu. Il est possible d'en évaluer le nombre d'étapes dans les pires cas et faire le lien avec les suites de Fibonacci.
Des applications élémentaires sont particulièrement bienvenues : calcul de relations de Bézout, résolutions d'équations diophantiennes linéaires, inversion modulo un entier ou un polynôme, calculs d'inverses dans les corps de ruptures, les corps finis. On peut aussi évoquer le théorème chinois effectif,la résolution d'un système de congruences et faire le lien avec l'interpolation de Lagrange.
Pour aller plus loin, on peut évoquer le rôle de algorithme d'Euclide étendu dans de nombreux algorithmes classiques en arithmétique (factorisation d'entiers, de polynômes, etc). Décrire l'approche matricielle de l'algorithme d'Euclide et l'action de $\mathrm{SL}_2(\mathbb{Z})$ sur $\mathbb{Z}^2$ est tout à fait pertinent. On peut aussi établir l'existence d'un supplémentaire d'une droite dans $\mathbb{Z}^2$ ou d'un hyperplan de $\mathbb{Z}^n$, la possibilité de compléter un vecteur de $\mathbb{Z}^n$ en une base. On peut aussi étudier les matrices à coefficients dans un anneau principal ou euclidien, et, de manière plus avancée, la forme normale d'Hermite et son application à la résolution d'un système d'équations diophantiennes linéaires. De même, aborder la forme normale de Smith, et son application au théorème de la base adaptée, permet de faire le lien avec la réduction des endomorphismes via le théorème des invariants de similitude.
La leçon invite aussi, pour des candidates et candidats maîtrisant ces notions, à décrire le calcul de PGCD dans $\mathbb{Z}[X]$ et $\mathbb{K}[X,Y]$, avec des applications à l'élimination de variables. On peut rappeler les relations entre PGCD et résultant et montrer comment obtenir le PGCD en échelonnant la matrice de Sylvester. Sur l'approximation diophantienne, on peut enfin envisager le développement d'un rationnel en fraction continue et l'obtention d'une approximation de Padé-Hermite à l'aide de l'algorithme d'Euclide, la recherche d'une relation de récurrence linéaire dans une suite ou le décodage des codes `BCH`.

Présentation de la leçon

Je vais vous présenter la leçon 142 intitulée : "PGCD et PPCM, algorithmes de calcul. Applications.". L'objectif de cette leçon sera de généraliser les notions de PGCD et de PPCM connue dans $\mathbb{Z}$ à d'autres types anneaux afin de pouvoir en tirer de bonnes propriétés arithmétiques.
Dans une première partie on s'intéresse aux notions de PGCD et de PPCM mais dans divers contextes : on commence par le cas le plus général avec un anneau factoriel. On commence par définir un élément irréductible puis un anneau factoriel et on remarque que l'unicité de la décomposition en produit d'irréductibles n'est pas superflue d'après la remarque 5 et on parle ensuite de divisibilité et d'éléments premiers entre eux puis enfin on définit le PGCD et le PPCM dans le cas factoriel à association près et on termine ce premier point en énonçant les lemmes d'Euclide et de Gauss. On s'intéresse brièvement au cas du contenu d'un polynôme avec le lemme de Gauss et le théorème 16 qui nous donnent par exemple le théorème du transfert. Enfin on termine cette première partie avec le cas des anneaux principaux où les notions de PPCM et de PGCD peuvent se traduire en termes d'idéaux et où l'on voit apparaître le théorème de Bézout.
On a remarqué dans la partie précédente que l'obtention d'un PGCD est quelque chose d'important et que la relation de Bézout peut être un outil pratique (par exemple pour trouver un inverse dans $\mathbb{Z}/n\mathbb{Z}$). Il nous faut donc savoir les déterminer et c'est l'objet de notre deuxième partie. On commence tout d'abord par l'obtention du PGCD dans le cadre d'un anneau euclidien avec l'algorithme d'Euclide qui donne le PGCD en tant que dernier reste non nul de la division euclidienne. Cet algorithme à l'avantage de ne pas fonctionner dans $\mathbb{Z}$ uniquement mais dans $\mathbb{K}[X]$ par exemple ! Dans une deuxième sous-partie on s'intéresse à la recherche de la relation de Bézout : on sait déjà que l'algorithme d'Euclide donne le PGCD entre deux éléments a et b et alors en remontant l'algorithme on peut obtenir la relation de Bézout en remplaçant successivement.
Enfin dans une dernière partie on s'intéresse à quelques applications en commençant par le cas de l'algèbre linéaire : on donne le lemme des noyaux (qui repose entièrement sur la relation de Bézout !) qui permet d'établir la décomposition de Dunford d'un endomorphisme. On continue avec une deuxième application avec la résolution d'équations diophantiennes. Pour cela, on démontre le théorème des restes chinois dans le cas général d'un anneau A principal avant de donner l'exemple d'un système de congruences dans $\mathbb{Z}/n\mathbb{Z}$ qui est l'une des utilisations les plus fréquentes de ce théorème.
On passe ensuite à la théorie des groupes avec tout d'abord le cas de l'exposant où l'on commence par en donner la définition ainsi que quelques propriétés et qui permet de montrer que les sous-groupes finis de $\mathbb{K}^\times$ sont cycliques et en particulier les sous-groupes finis de $\mathbb{F}_q^\times$. Puis on conclut avec le cas des groupes abéliens finis avec l'important théorème de structure qui permet de classifier ces groupes grâce aux facteurs invariants (qui peuvent être obtenus grâce à l'algorithme de Smith) comme on peut le voir avec le corollaire 49 et l'exemple 50.

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 commutatif quelconque.

I Notion de PGCD et PPCM

I.1 Définition et cas des anneaux factoriels

Définition 1 : 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 $(p = ab) \implies (a \in A^\times \text{ ou } b \in A^\times)$.

Exemple 2 : [Perrin, p.47]
Les éléments irréductibles de $\mathbb{Z}$ sont les nombres premiers (au sens usuel) ainsi que leurs opposés.

Définition 3 : 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 4 : [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 5 : [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...

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

Définition 6 : 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 7 : [Perrin, p.46]
b divise a si, et seulement si, $(a) \subseteq (b)$.

Définition 8 : 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 9 : 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 10 : 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 11 :
∗ 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.

Lemme 12 : Lemme d'Euclide [Perrin, p.48] :
Si p est irréductible et p divise ab, alors (p divise a ou p divise b).

Lemme 13 : Lemme de Gauss (1) [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.

I.2 Contenu d'un polynôme

Dans toute cette sous-partie, on suppose que A est un anneau factoriel.

Définition 14 : Contenu d'un polynôme [Perrin, p.51] :
On considère un polynôme $P \in A[X]$.
On appelle **contenu de** P (et on note $c(P)$) le PGCD (défini modulo $A^\times$) des coefficients de P. De plus, P est dit **primitif** lorsque $c(P) = 1$.

Lemme 15 : Lemme de Gauss (2) [Perrin, p.51] :
∗ Pour tous polynômes P, Q de $A[X]$ non nuls, on a $c(PQ) = c(P)c(Q)$.
∗ Le produit de deux polynômes primitifs est primitif.

Théorème 16 : [Perrin, p.51] :
Les polynômes $P \in A[X]$ irréductibles dans $A[X]$ sont exactement :
∗ Les constantes $p \in A$ irréductibles dans A.
∗ Les polynômes P de degré supérieur ou égal à 1, primitifs et irréductibles dans $\mathrm{Frac}(A)[X]$.

Exemple 17 :
Les polynômes $P \in \mathbb{Z}[X]$ irréductibles dans $\mathbb{Z}[X]$ sont exactement :
∗ Les nombres premiers (au sens usuel) ainsi que leurs opposés.
∗ Le polynômes P de degré supérieur ou égal à 1, primitifs et irréductibles dans $\mathbb{Q}[X]$.

Théorème 18 : Théorème de transfert [Perrin, p.51] :
Si A est factoriel, alors $A[X]$ est factoriel.

I.3 Cas des anneaux principaux

Définition 19 : Anneau principal [Perrin, p.49] :
Un anneau est un **anneau principal** lorsque celui-ci est intègre et que tous ses idéaux sont principaux.

Exemple 20 : [Rombaldi, p.237]
L'anneau $\mathbb{Z}$ ainsi que tout les corps $\mathbb{K}$ sont principaux.

Dans toute la suite de cette sous-partie, on suppose que A est un anneau principal et on considère deux éléments $a, b \in A$.

Proposition 21 : [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 22 : 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 23 : [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 $(X) + (Y) = (X, Y) \neq (1)$.

II Algorithme de calcul dans un anneau euclidien

II.1 Obtention du PGCD

Définition 24 : 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 $v(r) < v(b))$.

Exemple 25 : [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 26 : [Perrin, p.50]
Tout anneau euclidien est principal

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

Exemple 27 : [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 28 : [Perrin, p.51]
L'anneau $A[X]$ est principal si, et seulement si, A est un corps.

Dans toute la suite de cette sous-partie, on suppose que A est un anneau euclidien avec un stathme noté φ.

Théorème 29 : 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 30 :
∗ Un PGCD de 255 et 141 est 3.
∗ Un PGCD de $X^3 - X^2 - X + 1$ par $X^2 - 3X + 2$ est $X - 1$.

II.2 Recherche d'une relation de Bézout

Remarque 31 :
On obtient une relation de Bézout en "remontant" l'algorithme de Gauss.

Exemple 32 :
Une relation de Bézout entre 255 et 124 est : $255 \times (-53) + 124 \times 109 = 1$. En effet, en effectuant les divisions euclidiennes successives et en remontant l'algorithme d'Euclide, on obtient alors de manière explicite notre relation de Bézout.

III Applications

III.1 Algèbre linéaire

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

Lemme 33 : [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 $Q_k = \prod_{\substack{j=1 \\ j\neq k}}^{r} P_j$.

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 34 : 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 35 : 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.

III.2 Résolution d'équations diophantiennes

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

Développement 1 : [cf. ROMBALDI]

Lemme 36 : [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 37 : 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 :

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

Exemple 38 : [Rombaldi, p.291]
Le système d'équations diophantiennes :

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

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

III.3 Applications en théorie des groupes

Dans toute cette sous-partie, on considère un groupe $(G, *)$.

Définition 39 : Groupe d'exposant fini [Berhuy, p.344] :
On dit que G est **d'exposant fini** lorsqu'il existe un entier $n \in \mathbb{N}^*$ tel que pour tout $x \in G$, $x^n = e_G$.
Dans ce cas, on appelle **exposant de** G le plus petit entier $n \in \mathbb{N}^*$ vérifiant cette propriété et on le note $\exp(G)$.

Développement 2 : [cf. BERHUY]

Lemme 40 : [Berhuy, p.344]
Si G est un groupe d'exposant fini, alors $\exp(G) = \text{PPCM}(\{o(x),\ x \in G\})$.
De plus, si G est fini, on a $\exp(G)$ qui divise $\text{Card}(G)$.

Exemple 41 : [Berhuy, p.345]
* Si G est cyclique d'ordre n, alors $\exp(G) = n$.
* On a $\exp(D_4) = 4$ et $\exp(\mathfrak{S}_3) = 6$.

Proposition 42 : [Berhuy, p.345]
Si G est un groupe abélien d'exposant fini, alors il existe un élément $x \in G$ d'ordre $\exp(G)$.

Corollaire 43 : [Berhuy, p.345]
Si G est un groupe abélien fini, alors on a l'équivalence :

$$(\exp(G) = \text{Card}(G)) \iff (G \text{ cyclique})$$

Remarque 44 : [Berhuy, p.346]
L'ensemble $\mathfrak{S}_3$ montre que les deux résultats précédents sont faux si G n'est pas supposé abélien.

Théorème 45 : [Berhuy, p.346]
Tout sous-groupe fini de $\mathbb{K}^\times$ est cyclique.

Remarque 46 : [Berhuy, p.346]
* En particulier, on en déduit que tout sous-groupe de $\mathbb{F}_q^\times$ est cyclique (avec $q = p^n$ où p est un nombre premier et n un entier naturel non nul).
* Si p est un nombre premier, on a alors que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique.

Dans toute la suite de cette sous-partie, on suppose que $(G, *)$ est d'ordre fini et abélien.

Théorème 47 : Théorème de structure [ADMIS] [Berhuy, p.358] :
Il existe des entiers $d_1, ..., d_s \geq 2$ vérifiant $d_1|d_2|...|d_s$ et tels que $G \cong \prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z}$.
De plus, la suite d'entiers $(d_1, ..., d_s)$ est unique, et ne dépend que de la classe d'isomorphisme de G.

Définition 48 : Facteurs invariants [Berhuy, p.361] :
Les entiers $d_1, ..., d_s$ fournis par le théorème précédent sont appelés les **facteurs invariants de** G.

Corollaire 49 : [Berhuy, p.362]
Deux groupes abéliens finis sont isomorphes si, et seulement si, ils ont les mêmes facteurs invariants.

Exemple 50 : [Berhuy, p.363]
$*$ Si $G = \mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, alors $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/180\mathbb{Z}$.
$*$ Il y a exactement 3 groupes abéliens d'ordre 120 (à l'isomorphisme près).

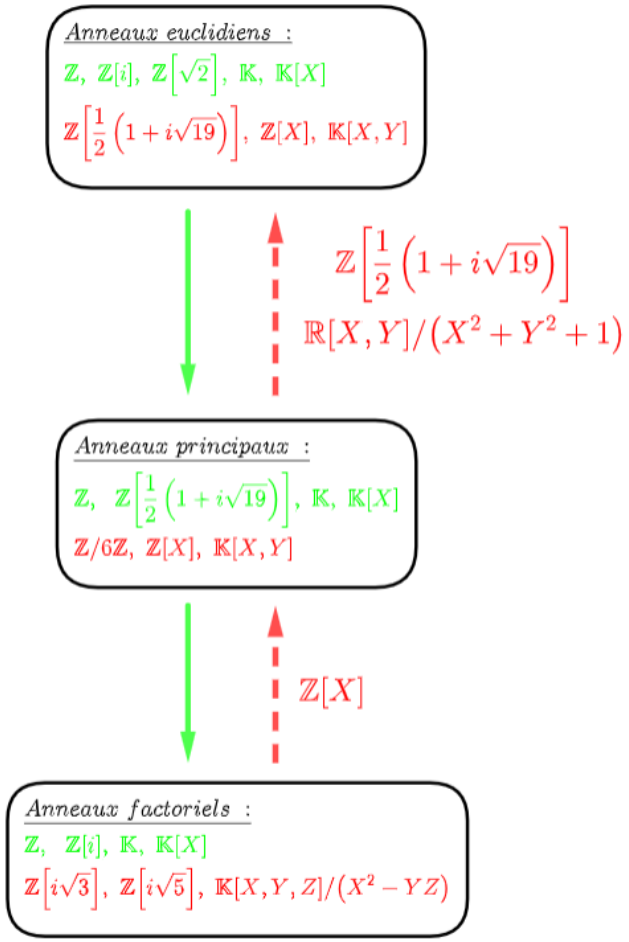
Remarque 51 :
La connaissance des facteurs invariants d'un groupe abélien semble donc extrêmement importante et il nous faut donc récupérer cette information : chose qu'il est possible de faire en appliquant l'algorithme de Smith au groupe abélien fini G qui peut être vu comme un $\mathbb{Z}$-module.

Corollaire 52 :
Pour tout diviseur d de l'ordre de G, il existe un sous-groupe de G d'ordre d.

Théorème 53 : [ADMIS] [Berhuy, p.364]
Si G est un groupe abélien de type fini, alors il existe des entiers naturels r, s et des entiers $d_1, ..., d_s \geq 2$ vérifiant $d_1|d_2|...|d_s$ tels que $G \cong \mathbb{Z}^r \times \prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z}$.
De plus, l'entier r et la suite d'entiers $(d_1, ..., d_s)$ sont uniques.

IV Annexe

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



IV.2 Algorithme d'Euclide

Entrée : $a, b \in A$, $b \neq 0_A$.
Sortie : d, u, v tels que $au + bv = d$ et $d = \text{PGCD}(a, b)$.
Algorithme : $u_0 = 1$, $u_1 = 0$, $v_0 = 0$, $v_1 = 1$, $r_0 = a$, $r_1 = b$, $i = 1$.
Tant que $r_i \neq 0$:
$r_{i+1} \longleftarrow r_{i-1} - q_i r_i$ (division euclidienne de r_{i-1} par r_i)
$u_{i+1} \longleftarrow u_{i-1} - q_i u_i$
$v_{i+1} \longleftarrow v_{i-1} - q_i v_i$
$i \longleftarrow i + 1$
Renvoyer r_{i-1}, u_{i-1}, v_{i-1}

Remarques sur le plan

— Il est important de savoir dans quels contextes sont définis les PGCD et PPCM pour savoir quelles propriétés utiliser.

— On peut également insister d'avantage sur les systèmes de congruence.

Liste des développements possibles

— Théorème des restes chinois + application.

— Exposant d'un groupe.

Bibliographie

— Daniel Perrin, *Cours d'algèbre*.

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

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