111: Anneaux principaux. Applications

Pierre Lissy

May 6, 2010

dans toute la suite A désigne un anneau commutatif. Son ensemble des inversibles sera noté A^*.

1 Définitions. Premières proriétés.

1.1 Idéaux d'un anneau commutatif

Définition 1. *Un sous-ensemble I de A est appelé idéal ssi c'est sous-groupe additif de A absorbant.*

Exemple 1. *Idéal principal: de la forme aA, noté (a). Idéal de type fini : $a_1A + a_2A + \dots a_nA$, noté $(a_1, \dots, a_n)$ A, 0 sont des idéaux de A.*

Proposition 1. *L'intersection d'un nombre qqe d'idéaux est un idéal, la somme finie (infinie dénombrable) de deux idéaux est un idéal.*

Remarque 1. *Faux en général avec la réunion.*

Proposition 2. *la réunion de deux idéaux est un idéal ssi l'un est inclus dans l'autre. Par contre une réunion 'finie ou dénombrable) croissante d'idéaux est un idéal.*

Corollaire 1. *Soit X un sous-ensemble de A, on appelle idéal engendré par X le plus petit idéal contenant X. C'est aussi l'intersection de tous les idéaux contenant X. L'idéal engendré par un élément a est (a), celui*

Définition 2. *On appelle idéal produit l'idéal engendré par les produits. Il est inclus dans l'intersection.*

Remarque 2. *Inclusion réciproque fausse: l'idéal produit de $n\mathbb{Z}$ et $m\mathbb{Z}$ est $nm\mathbb{Z}$, l'intersection est $nvm\mathbb{Z}$.*

Proposition 3. *L'ensemble A/I peut être muni d'une structure d'anneau telle que la projection canonique soit un morphisme d'anneaux. De plus les idéaux de A et ceux de A/I sont en bijection par la préimage de la projection.*

Proposition 4. *Un anneau (commutatif intègre) est un corps ssi ses seuls idéaux sont lui-même et 0.*

1.2 Anneaux principaux

Définition 3. *Un anneau est principal ssi il est intègre et tous ces idéaux sont principaux.*

Exemple 2. *Tout corps est un anneau principal.*

Il existe des anneaux intègres non principaux.

Exemple 3. *$\mathbb{Z}[X]$ est un anneau intègre non principal car si l'on considère l'idéal engendré par X et 2, il n'est pas principal.*

Il existe des anneaux n'admettant que des idéaux principaux et non intègres.

Exemple 4. *$\mathbb{Z}/4\mathbb{Z}$ est non intègre mais tout idéal est principal (car les seuls idéaux sont 0 et $\mathbb{Z}/4\mathbb{Z}$)*

1.3 Comparaison avec les anneaux noethériens

Définition 4. *Un anneau est dit noethérien ssi tout idéal est de type fini.*

Proposition 5. *Dans un anneau principal, tout idéal est de type finie, ie.c un anneau principal est noethérien*

Remarque 3. *Réciproque fausse : $\mathbb{Z}[X]$ est noethérien (th de transfert de Hilbert) mais n'est pas principal.*

1.4 Comparaison avec les anneaux euclidiens

Définition 5. *Un anneau est dit euclidien ssi on peut le munir d'un stasthme, ie d'une application $\varphi : A \setminus 0 \to \mathbb{N}$ telle que pour tout a et b on peut trouver q et r tels que $a = bq + r$ et $r=0$ ou $\varphi(r) < \varphi(b)$.*

On a deux exemples importants.

Exemple 5. *$\mathbb{Z}$ muni de la valeur absolue est euclidien*

Exemple 6. *Si $\mathbb{K}$ est un corps alors $\mathbb{K}[X]$ muni du degré est euclidien.*

Exemple 7. *[1]L'anneau $\mathbb{Z}[i]$ est euclidien (norme évidente). L'algèbre des séries formelles $k[[X]]$ est aussi euclidien (stasthme = norme), l'anneau des nombres décimaux.*

Exemple 8. *On montre que les anneaux $\mathbb{Z}[\sqrt{d}]$ sont euclidiens pour $d = 2, 3, 7, 11$.*

Théorème 1. *$A[X]$ principal ssi A est un corps.*

Tout anneau n'est pas euclidien. On a la condition nécessaire suivante [1]:

Proposition 6. *A euclidien $\Rightarrow$ Il existe un élément de A non inversible tel que la restriction à $A^* \cup 0$ de la projection canonique de A sur $A/(x)$ soit surjective.*

Exemple 9. *L'anneau $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ n'est pas euclidien.*

Les anneaux euclidiens sont importants par le théorème suivant.

Théorème 2. *Tout anneau euclidien est principal.*

La réciproque est fausse.

Exemple 10. *L'anneau $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ est principal non euclidien.*

1.5 Stabilité de la notion d'anneau principal

Comme vu précédemment, la notion d'anneau principal n'est pas stable par passage à $A[X]$ (sauf si A est un corps), n'est pas stable par passage au quotient en général (un quotient n'est pas forcément intègre). Par contre si on quotiente par un idéal premier on verra plus tard qu'on obtient un corps donc un anneau principal.

Rappelons quand même que la notion d'anneau noethérien est stable par passage à l'anneau des polynômes à plusieurs variables, celle d'anneau factoriel à l'anneau des polynômes à plusieurs variables et à l'anneau des séries formelles.

2 Arithmétique dans un anneau principal

2.1 Divisibilité

Définition 6. *On dit que a divise b ($a|b$) ssi il existe q tq $b=aq$.*

Théorème 3. *$a|b \Leftrightarrow (b) \subset (a)$*

Définition 7. *Deux éléments sont dit associés ssi $a|b$ et $b|a$. C'est une relation d'équivalence.*

Proposition 7. *a et b sont associés ssi $(a)=(b)$ ssi $\exists q \in A^*$ tq $a = qb$.*

2.2 Elements premiers, irréductibles

Définition 8. *Un élément p est dit premier ssi $p|ab \Rightarrow p|a$ ou $p|b$.*

Exemple 11. *Dans $\mathbb{Z}$ les nombres premiers sont des éléments premiers.*

Définition 9. *Un element est dit irréductible ssi $p = ab \Rightarrow a \in A^*$ ou $b \in A^*$.*

Exemple 12. *Les éléments irréductibles de $\mathbb{Z}$ sont les nombres premiers. Les elements irréductibles de $K[X]$ sont les X-a dès que K est algébriquement clos, ce sont les polynomes de degré un ou de degré 2 ayant un discriminant strictement négatif dans le cas réel. Les élements irréductibles d'un corps sont tous les élements de K^*.*

Théorème 4. *p premier ssi l'idéal (p) est 1er, ie A/I est intègre.*

Théorème 5. *p irréductible ssi (p) est maximal dans l'ensemble des idéaux principaux.*

Corollaire 2. *Tout élement premier est irréductible*

Définition 10. *Deux éléments sont dit premiers entre eux ssi leurs seuls diviseurs communs sont les inversibles.*

Théorème 6 (chinois)**.** *[1] Si a et b sont premiers etre eux alors $A/(ab) \simeq A/(a) \times A/(b)$.*

2.3 Comparaison avec les anneaux factoriels

Définition 11. *Un anneau est dit factoriel ssi il est intègre et que tout élement s'écrit de manière unique (à permutation près et aux inversibles) comme produit d'irréductibles.*

Dans un anneau intègre, ce n'est pas parce qu'il existe une décomposition en irréductibles qu'elle est unique.

Exemple 13. *Dans $\mathbb{Z}[i\sqrt{5}]$, $9 = 3 * 3 = (2 + i\sqrt{5})(2 - i\sqrt{5})$.*

dans un anneau intègre, il n'existe pas forcément de décomposition en irréductibles.

Exemple 14. *trouver*

Remarque 4. *On peut plutôt que de prendre tous les irréductibles choisir dans chaque classe d'irréductibles un représentant, ce qui donne un ensemble $\mathcal{P}$ de représentants. On a alors unicité a permutation près.*

Exemple 15. *Dans $\mathbb{Z}$ on prend en général les entiers naturels, dans $\mathbb{K}[X]$ on prend les polynômes unitaires.*

Par contre, on a le théorème important suivant.

Théorème 7. *Tout anneau principal est factoriel*

Réciproque fausse.

Exemple 16. *$\mathbb{Z}[X]$ est non principal (déjà vu) mais est factoriel (par le théorème de transfert de Gauss)*

Par contre, on peut montrer les résultats plus fins suivants.

Proposition 8. *Tout anneau intègre noethérien, tout élément admet une décomposition en irréductibles.*

Théorème 8. *Soit A un anneau intègre tel que tout élement admet une décomposition en irréductibles. On a les équivalences suivantes:*

1. *A est factoriel*
2. *si p est irréductible, $p|ab$ implique $p|a$ ou $p|b$.*
3. *p irréductible ssi p premier*
4. *$a|bc$ et a premier avec b implique que $a|c$*

Dans un anneau principal on a donc toutes les propriétés précédentes.

2.4 PGCD, PPCM

Définition 12. *On appelle pgcd de deux éléments a et b tout diviseur de d maximal au sens suivant: tout autre diviseur commun de a et b est un diviseur de d. On appelle ppcm de deux éléments tout multiple minimal.*

Dans un anneau commutatif intègre qqe, le pgcd et le ppcm de deux éléments n'existent pas nécessairement.

Exemple 17. *[1]dans $\mathbb{Z}[i\sqrt{5}]$, 3 et $2+i\sqrt{5}$ n'ont pas de ppcm, 9 et $3(2+i\sqrt{5})$ n'ont pas de pgcd.*

Proposition 9. *Deux pgcd d'un élément diffèrent d'un inversible, idem pour le ppcm. On identifiera donc la classe d'équivalence des pgcd avec n'importe lequel de ses représentants.*

On a le théorème important suivant.

Théorème 9. *Dans un anneau principal, le pgcd et le ppcm de deux éléments existent: le pgcd de a et b est un élement d tel que $dA = aA + bB$ et le ppcm est un élement m tel que $mA = aA \cup bA$.*

Corollaire 3 (Bezout)**.** *Il existe u,v, au+bv=d*

Egalité de Bézout fausse en général dans un anneau factoriel.

Exemple 18. *[1]$K[X,Y]$ est factoriel, les élements X et Y sont premiers entre eux mais pourtant l'idéal engendré par X et Y n'est pas égal à $K[X,Y]$ tout entier!*

Corollaire 4. *Dans un anneau principal, a et b premiers entre eux ssi il existe u,v tq au+bv=1*

Remarque 5. *Sens réciproque vrai dans n'importe quel anneau intègre.*

En fait, on a aussi existence du pgcd dans un anneau factoriel.

Lemme 1. *Tout élement d'un anneau factoriel peut s'écrire de manière unique sous la forme $u\prod_{\mathcal{P}} p_i^{v(p_i)}$ où les $v(p_i)$ sont nuls sauf un nombre fini d'entre eux.*

Théorème 10. *un pgcd de a est b est le produit des p_i et de l'inf des $v(p_i)$, on obtient un ppcm avec le sup. De plus, le ppcm est bien un générateur de $A \cap B$, mais c'est en général pas le cas pour le pgcd.*

Il existe des anneaux non factoriels ou on peut définir un ppcm et un pgcd.

Exemple 19. *Les fonctions entières: ni principal ni factoriel mais on peut définir le pgcd et le ppcm.*

3 Applications

3.1 Classification des classes d'équivalence des matrices à coeff dans un anneau principal

En général, dans le cas d'un anneau principal, deux matrices ayant même rang ne sont pas équivalentes.

Exemple 20. *On se place dans $\mathbb{Z}$, qui est lui-même un espace de matrices. Les matrices inversibles sont 1 et -1. Alors les matrices 1 et 2 ont même rang (à savoir 1), mais elles ne peuvent pas être équivalentes.*

Théorème 11. *Toute matrice à coefficients dans un anneau principal est équivalente à une matrice quasi-diagonale D où les coefficients diagonaux vérifient $d_1|d_2 \ldots |d_n$. De plus , si on considère une autre décomposition sous la même forme (ie D') alors les coefficients d_i et d'_i sont associés. Autrement dit les nombres d_i sont uniques aux inversibles près. Ils sont appelés invariants de Smith de la matrice.*

Corollaire 5. *Deux matrices sont équivalentes ssi elles ont les mêmes invariants de Smith.*

Corollaire 6. *Une matrice est inversible ssi ses invariants de Smith sont* $(1, 1, \dots 1)$. *Les matrices inversibles forment donc une classe*

En général, on a donc un nombre infini de classes d'équivalence.

Théorème 12. *Dans le cas d'un anneau euclidien, on peut de manière effective juste avec des opérations élémentaires sur les lignes transformer une matrice* M *en une matrice échelonnée suivant les lignes (ie la ligne numéro i a strictement moins de 0 que la ligne (i-1), et ceci pour tout i).*$LM=E$, *où* E *est echelonnnée et* L *est un produit de matrices élémentaires. De même on peut obtenir avec des opérations élémentaires sur les colonnes une matrice échelonnée suivant les colonnes.*

Corollaire 7. *On peut de manière effective en utilisant une matrice* L *et une matrice* C *transformer* M *en sa matrice des invariants de Smith.*

Enfin, signalons une manière effective d'avoir accès aux invariant sde similitude par le théorème suivant.

Théorème 13. *Les invariants de similitude de* A *sont exactement les invariants de Smith de* $XI_n - A$.

3.2 Théorème des deux carrés

Définition 13. *Un résidu quadratique modulo p est un carré de* $\mathbb{F}_p$.

Proposition 10. *Il y a (p+1)/2 résidus quadratiques dans* $\mathbb{F}_p$ *((p-1)/2 si on exclut 0)*

Proposition 11. a *est un résidu quadratique ssi l'équation* $x^2 - a = 0$ *a une solution dans* $\mathbb{F}_p$ *ssi il existe un diviseur premier de la forme* $x^2 - 5y^2$ *avec* x *et* y *premiers entre eux.*

Corollaire 8. -1 *est un carré dans* K *ssi* q *est congru à 1 modulo 4.*

Lemme 2. *Un nombre premier est somme de deux carrés ssi il vaut 2 ou est congru à 1 modulo 4.*

Application 1 (Théorème des deux carrés)**.** *Un entier est somme de deux carrés ssi la valuation de tous les nombres premiers congrus à 3 modulo 4 est paire.*

3.3 Eléments algébriques, construction des corps finis.

3.4 Polynômes annulateurs d'un endomorphisme

3.5 Polynômes annulateurs d'un élément par rapport à un endomorphisme

Developpements:

References

[1] Perrin

[2] Combes

[3] Quérré

[4] Lelong-Ferrand Arnaudiès Algèbre