

Chapitre 2

Propriétés arithmétiques des anneaux commutatifs intègres

2.1 Divisibilité dans les anneaux commutatifs intègres

Soit A un anneau commutatif intègre. On note avec une barre verticale la relation de divisibilité.

Remarque 2.1.1. Il y a équivalence entre :

- (i) $x|y$ et $y|x$,
- (ii) $\exists u \in A^\times \quad y = ux$,
- (iii) $(x) = (y)$.

Proposition 2.1.2. a) Sur A la relation $x \sim y \Leftrightarrow \exists u \in A^\times \quad y = ux$ est une relation d'équivalence.

Les classes d'équivalence sont appelées classes d'éléments associés.

c) La relation divise induit une relation d'ordre sur les classes d'éléments associés.

La relation d'ordre précédente permet de définir les notions de PGCD et de PPCM comme borne inférieure et borne supérieure. L'existence n'est pas garantie, mais il y a toujours unicité comme classe d'éléments associés. Donnons une formulation précise naïve.

Définition 2.1.3. Soit A un anneau commutatif intègre, et F un ensemble d'éléments de A .

a) d est (un) PGCD de F si et seulement si :

$$\forall x \in F \quad d|x, \text{ et}$$

$$\forall \delta \in A - \{0\} (\forall x \in F \ \delta|x) \Rightarrow \delta|d .$$

b) m est (un) PPCM de F si et seulement si :

$$\forall x \in F \ x|m , \text{ et}$$

$$\forall \mu \in A - \{0\} (\forall x \in F \ x|\mu) \Rightarrow m|\mu .$$

Définition 2.1.4. $p \in A$ est irréductible si et seulement si p a deux classes de diviseurs : A^\times et pA^\times .

On va relier cette notion à celle d'idéal.

Proposition 2.1.5. Si l'idéal pA est premier (on dit que p est premier), alors p est irréductible.

2.2 Anneaux euclidiens

Définition 2.2.1. Un anneau A est euclidien si et seulement s'il existe une application $d : A - \{0\} \rightarrow \mathbb{N}$ satisfaisant la condition suivante : pour tout couple (a, b) , avec $b \neq 0$, il existe un couple (q, r) tel que :

$$a = bq + r \text{ et } (r = 0 \text{ ou } d(r) < d(b)) .$$

Remarque 2.2.2. L'application d est appelée un stathme (ou une norme).

Exemples 2.2.3. L'anneau \mathbb{Z} , les anneaux $\mathbb{K}[X]$ avec \mathbb{K} un corps sont des anneaux euclidiens.

Proposition 2.2.4. L'anneau des entiers de Gauss $\mathbb{Z}[i]$ est euclidien.

- Exercice 2.2.5.*
1. Montrer que l'anneau des décimaux est euclidien.
 2. Montrer que l'anneau des polynômes de Laurent $\mathbb{K}[X, X^{-1}]$, avec \mathbb{K} un corps commutatif, est euclidien.
 3. Pour un anneau euclidien A et S une partie multiplicative, est-ce que l'anneau $S^{-1}A$ est euclidien ?

2.3 Anneaux principaux

Définition 2.3.1. Un anneau principal est un anneau commutatif intègre dans lequel tout idéal est principal (engendré par un seul élément).

Proposition 2.3.2. Tout anneau euclidien est principal.

Théorème 2.3.3. Soient a et b deux éléments d'un anneau principal A .

- a) d est PGCD de a et b si et seulement si $(d) = (a) + (b)$.
- b) m est PPCM de a et b si et seulement si $(m) = (a) \cap (b)$.

Plus généralement :

Théorème 2.3.4. Soit F une partie non vide d'un anneau principal A .

- a) d est PGCD de F si et seulement si d est générateur de l'idéal engendré par F .
- b) m est PPCM de F si et seulement si $(m) = \bigcap_{a \in F} aA$.

23/09/2010

Corollaire 2.3.5. Dans un anneau principal toute partie non vide de A a un PGCD et un PPCM.

Théorème 2.3.6 (Bezout). Dans un anneau principal A , deux éléments ont 1 comme PGCD (sont premiers entre eux) si et seulement s'il existe un couple (u, v) tel que :

$$ua + vb = 1 .$$

Théorème 2.3.7. Soit p un élément non nul d'un anneau principal. Les énoncés suivants sont équivalents :

- a) p est irréductible ;
- b) l'idéal (p) est premier (p est premier) ;
- c) l'idéal (p) est maximal.

Corollaire 2.3.8. Dans un anneau principal, tout idéal premier non nul est maximal.

Proposition 2.3.9 (Lemme de Gauss). Dans un anneau principal A , si $a|bc$ et a est premier avec b , alors $a|c$.

Corollaire 2.3.10 (Lemme d'Euclide). Dans un anneau principal A , si un élément premier divise un produit, alors il divise l'un des facteurs.

Proposition 2.3.11. Dans un anneau principal, toute suite croissante d'idéaux est stationnaire.

Théorème 2.3.12. Dans un anneau principal, il existe une décomposition en facteurs irréductibles, unique aux inversibles près et à l'ordre près des facteurs (essentiellement unique).

2.4 Anneaux factoriels

Définition 2.4.1. Un anneau commutatif intègre est factoriel si et seulement si tout élément non nul et non inversible se décompose de manière essentiellement unique comme produits d'éléments irréductibles.

Théorème 2.4.2. *Un anneau A est factoriel si et seulement si :*

- a) *Toute suite croissante d'idéaux principaux est stationnaire, et*
- b) *tout élément irréductible de A est premier.*

Remarque 2.4.3. On rappelle qu'il est toujours vrai dans un anneau commutatif intègre qu'un élément premier est irréductible. Dans un anneau factoriel l'unicité de la décomposition en irréductibles assure que si un irréductible p est décomposé en produit : $p = ab$, alors a ou b est associé à p , et donc l'idéal (p) est premier.

Exemple 2.4.4. L'anneau $\mathbb{Z}[\sqrt{5}]$ n'est pas factoriel.

Proposition 2.4.5. *Dans un anneau factoriel toute famille finie a un PGCD et un PPCM.*

Proposition 2.4.6 (Lemme de Gauss). *Dans un anneau factoriel A , si $a|bc$ et a est premier avec b (i.e. 1 est PGCD de a et b), alors $a|c$.*

27/09/2010

Définition 2.4.7. Un anneau noethérien est un anneau dans lequel tout idéal est de type fini, c'est à dire engendré par une partie finie.

Remarque 2.4.8. Dans le cas non commutatif, on peut définir les notions de noethérien à gauche et noethérien à droite. On pourra considérer des anneaux noethériens qui ne sont pas intègres.

Remarque 2.4.9. Un anneau principal est noethérien.

Proposition 2.4.10. *L'anneau $\mathbb{Z}[X]$ est noethérien.*

Exercice 2.4.11. 1. Montrer que si l'anneau A est principal, alors $A[X]$ est noethérien.

2. (*) Montrer que si A est un anneau commutatif noethérien, alors $A[X]$ est noethérien.

Proposition 2.4.12. *Un anneau commutatif est noethérien si et seulement si toute suite croissante d'idéaux est stationnaire.*

Proposition 2.4.13. *Soit A un anneau commutatif intègre. Si A est noethérien, alors A est factoriel si et seulement si tout élément irréductible de A est premier.*

Exercice 2.4.14. Montrer que $\mathbb{Z}[X]$ est un anneau factoriel.

2.5 Le théorème chinois

L'énoncé habituel dans \mathbb{Z} , ou $\mathbb{K}[X]$ avec \mathbb{K} un corps commutatif, se généralise à un anneau principal sans changement.

Théorème 2.5.1 (Théorème chinois). *Soient a et b deux éléments premiers entre eux dans un anneau principal A , alors les anneaux $A/(ab)$ et $A/(a) \times A/(b)$ sont isomorphes.*

Remarque 2.5.2. Le théorème s'étend à une famille finie d'éléments deux à deux premiers entre eux.

Dans le cas d'un anneau non principal, on ne dispose plus du théorème de Bezout et il convient de préciser le vocabulaire.

Définition 2.5.3. a) Dans un anneau intègre commutatif, deux éléments sont premiers entre eux si et seulement si 1 est PGCD.

b) Dans un anneau intègre commutatif A , deux éléments a et b sont copremiers ou étrangers si et seulement si : $(a) + (b) = A$.

Théorème 2.5.4 (Théorème chinois). *Soient a et b deux éléments étrangers dans un anneau commutatif intègre A , alors les anneaux $A/(ab)$ et $A/(a) \times A/(b)$ sont isomorphes.*

Plus généralement :

Théorème 2.5.5. *Dans un anneau commutatif intègre A , soient I et J deux idéaux de somme égale à A (comaximaux), alors les anneaux $A/(I \cap J)$ et $A/I \times A/J$ sont isomorphes.*

2.6 L'algorithme d'Euclide

Dans cette section, on considère un anneau A euclidien, de stathme N .

Proposition 2.6.1. *Soient : $a \in A, b \in A$. On a pour tout $m \in A$:*

$$\text{PGCD}(a, b) = \text{PGCD}(b, a - mb) .$$

On peut en particulier appliquer la proposition précédente au cas où $m = q$ est le quotient dans la division euclidienne de a par b .

```

Fonction PGCD( $a, b$ );
Si ( $N(b) > N(a)$ ) Alors
    |  $a \leftrightarrow b$ ;
Fin Si
Effectuer la division euclidienne de  $a$  par  $b$ ;  $r \leftarrow$  (reste);
Si ( $r$  est nul) Alors
    | Retourner  $b$ ;
Sinon
    | Retourner PGCD( $b, r$ );
Fin Si

```

Algorithme 1: Algorithme d'Euclide, forme récursive

```

Fonction PGCD( $a, b$ );
 $a \leftarrow |a|$ ;  $b \leftarrow |b|$ ;
Si ( $N(b) > N(a)$ ) Alors
    |  $a \leftrightarrow b$ ;
Fin Si
Tant que ( $b$  est non nul) faire
    | Effectuer la division euclidienne de  $a$  par  $b$ ;  $r \leftarrow$  (reste);
    |  $a \leftarrow b$ ;  $b \leftarrow r$ ;
Fait
Retourner  $a$ ;

```

Algorithme 2: Algorithme d'Euclide, forme non récursive

Proposition 2.6.2. *L'algorithme d'Euclide retourne un PGCD de a et b .*

```

Fonction PGCDE( $a, b$ ) ; [la fonction retourne 3 éléments de l'anneau]
Si ( $N(b) > N(a)$ ) Alors
    |  $a \leftrightarrow b$  ; echange  $\leftarrow$  Vrai ;
Fin Si
Effectuer la division euclidienne de  $a$  par  $b$  ;  $r \leftarrow$  reste ;  $q \leftarrow$  quotient ;
Si ( $r$  est nul) Alors
    | Retourner ( $b, 0, 1$ ) ;
Sinon
    | ( $d, u', v'$ )  $\leftarrow$  PGCDE( $b, r$ ) ;
    |  $u \leftarrow v'$  ;  $v \leftarrow (u' - qv')$  ;
Fin Si
Si (echange est Vrai) Alors
    | Retourner ( $d, v, u$ ) ;
Sinon
    | Retourner ( $d, u, v$ ) ;
Fin Si

```

Algorithme 3: Algorithme d'Euclide étendu, forme récursive

```

Fonction PGCDE( $a, b$ ) ; [la fonction retourne 3 éléments de l'anneau]
Si ( $N(b) > N(a)$ ) Alors
    |  $a \leftrightarrow b$  ; echange  $\leftarrow$  Vrai ;
Fin Si
 $u' \leftarrow 1$  ;  $v' \leftarrow 0$  ;  $u'' \leftarrow 0$  ;  $v'' \leftarrow 1$  ;
Tant que ( $b$  est non nul) faire
    | Effectuer la division euclidienne de  $a$  par  $b$  ;
    |  $r \leftarrow$  reste ;  $q \leftarrow$  quotient ;
    |  $a \leftarrow b$  ;  $b \leftarrow r$  ;  $u \leftarrow u'$  ;  $v \leftarrow v'$  ;
    |  $u' \leftarrow u''$  ;  $v' \leftarrow v''$  ;  $u'' \leftarrow u - qu''$  ;  $v'' \leftarrow v - qv''$  ;
Fait
Si (echange est Vrai) Alors
    | Retourner ( $d, v', u'$ ) ;
Sinon
    | Retourner ( $d, u', v'$ ) ;
Fin Si

```

Algorithme 4: Algorithme d'Euclide étendu, forme non récursive

Proposition 2.6.3. *L'algorithme d'Euclide étendu retourne un PGCD de a et b et un couple de Bezout.*

Exercice 2.6.4 (Théorème de Lamé). On note (F_n) la suite de Fibonacci :

$$F_0 = 0, F_1 = 1, F_{n+2} = F_n + F_{n+1}.$$

1. Déterminer le PGCD de F_n et F_{n+1} .
2. Combien de divisions euclidiennes nécessite l'algorithme d'Euclide appliqué à F_n et F_{n+1} ?
3. Soient a et b deux entiers de PGCD égal à d , tels que : $0 < b < a$. Montrer que si l'algorithme d'Euclide appliqué à a et b nécessite n divisions, alors :

$$a \geq dF_{n+2}, b \geq dF_{n+1}.$$

4. On note $N(a, b)$ le nombre de divisions euclidiennes requis par l'algorithme d'Euclide appliqué à a et b .
 - (a) Montrer que : $b > \alpha^{N(a,b)-1}$, où $\alpha = \frac{1+\sqrt{5}}{2}$ est le nombre d'or.
 - (b) Montrer que $N(a, b)$ est majoré par 5 fois le nombre de chiffres de l'écriture de b en base 10.
 - (c) Quel est le couple d'entiers à 3 chiffres pour lequel l'algorithme d'Euclide nécessite le plus de divisions euclidiennes ?

2.7 Anneau d'entiers quadratiques

Soit d un entier relatif sans facteurs carrés (pas de multiplicité dans sa décomposition en facteurs premiers). Lorsque d est négatif, on note \sqrt{d} le complexe $i\sqrt{-d}$.

Proposition 2.7.1. *a) L'ensemble des $a + b\sqrt{d}$, $a \in \mathbb{Q}$, $b \in \mathbb{Q}$ est un sous-corps de \mathbb{C} noté $\mathbb{Q}(\sqrt{d})$.*

b) L'ensemble des $a + b\sqrt{d}$, $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ est un sous-anneau noté $\mathbb{Z}[\sqrt{d}]$.

Proposition 2.7.2. *L'application $\tau : a + b\sqrt{d} \mapsto a - b\sqrt{d}$ définit un automorphisme du corps $\mathbb{Q}(\sqrt{d})$.*

Définition 2.7.3. On appelle trace et norme les applications respectives T et N de $\mathbb{Q}(\sqrt{d})$ dans \mathbb{Q} , définies par : $T(x) = x + \tau(x)$, $N(x) = x\tau(x)$.

On note $\mathcal{O}_{\sqrt{d}}$ l'ensemble des éléments x de $\mathbb{Q}(\sqrt{d})$ pour lesquels $T(x)$ et $N(x)$ sont entiers.

- Proposition 2.7.4.** a) $\mathcal{O}_{\sqrt{d}}$ est un sous-anneau de $\mathbb{Q}(\sqrt{d})$.
 b) Pour d pair ou congru à 3 modulo 4 on a $\mathcal{O}(\sqrt{d}) = \mathbb{Z}[\sqrt{d}]$.
 c) Pour d congru à 1 modulo 4, $\mathcal{O}(\sqrt{d})$ est l'ensemble des $a + b\omega$, $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$, avec $\omega = \frac{1+\sqrt{d}}{2}$.

La norme étant multiplicative, les inversibles de l'anneau $\mathcal{O}(\sqrt{d})$ sont les éléments de norme ± 1 .

- Exercice 2.7.5.* 1. Montrer que $\mathbb{Z}[\sqrt{-5}]$ n'est pas un anneau factoriel.
 2. Montrer que $\mathbb{Z}[\sqrt{-2}]$ est un anneau euclidien.
 3. Montrer que $\mathcal{O}_{\sqrt{-3}}$ est un anneau euclidien.

- Exercice 2.7.6.* 1. Déterminer les inversibles de l'anneau des entiers de Gauss $\mathbb{Z}[i]$.
 2. Montrer que si z est un entier de Gauss premier, alors sa norme $N(z) = z\bar{z}$ est soit un entier premier, soit le carré d'un entier premier.
 3. Déterminer les entiers de Gauss qui sont premiers.
 4. Quels sont les entiers naturels qui s'écrivent comme somme de deux carrés?

04/10/2010