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 $A - \{0\}$ 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 :

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

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

Exercice 2.1.4. Soient x et y deux éléments non nuls dans un anneau commutatif intègre A.

1. Montrer que si x et y ont un PGCD noté d, alors il y a une bijection entre les diviseurs communs à x et y, et les multiples communs à x et y qui divisent $m = \frac{xy}{d}$.
2. Montrer qu'il y a équivalence entre :
   (i) x et y ont un PGCD,
   (ii)x et y ont un PPCM,
   (iii) l'idéal $(x) \cap (y)$ est un idéal principal (engendré par un élément).

Définition 2.1.5. $p \in A$ est irréductible si seulement si p a deux classes de diviseurs : $A^\times$ et $pA^\times$.

On va relier cette notion à celle d'idéal.

Proposition 2.1.6. *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 $d : A - \{0\} \longrightarrow \mathbb{N}$ 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.

Exercice 2.2.4.
1. Montrer que l'anneau des entiers de Gauss $\mathbb{Z}[i]$ est euclidien.
2. Montrer que l'anneau des décimaux est euclidien.
3. Montrer que l'anneau des polynômes de Laurent $\mathbb{K}[X, X^{-1}]$, avec $\mathbb{K}$ un corps commutatif, 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 E.
b) m est PPCM de F si et seulement si $(m) = \bigcap_{a \in E} aA$.

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 :*

$$ua + vb = 1 \ .$$

Fin du cours du 25/09

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'uncité 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 $\mathbb{Z}[X]$ est factoriel et non principal. On verra que si A est factoriel, alors $A[X]$ est 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 $a|c$.*

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

Remarque 2.4.8. Un anneau principal est noethérien.

Proposition 2.4.9. *Un anneau est noethérien si et seulement si toute suite croissante d'idéaux est stationnaire.*

Proposition 2.4.10. *Un anneau noethérien A est factoriel si et seulement si tout élément irréductible de A est premier.*

Fin du cours du 29/09

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 $m \in A$:*

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

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 ↔ b ;
Fin Si
Effectuer la division euclidienne de a par b ; r ← (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 ← |a| ; b ← |b| ;
Si (N(b) > N(a)) Alors
  | a ↔ b ;
Fin Si
Tant que (b est non nul) faire
  | Effectuer la division euclidienne de a par b ; r ← (reste) ;
  | a ← b ;b ← 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**
  $a \leftrightarrow b$;
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
  $(d, u', v') \leftarrow PGCDE(b, r)$;
  $u \leftarrow v'$; $v \leftarrow (u' - qv')$;
  Retourner (d, u, v) ;
Fin Si

Algorithme 3: Algorithme d'Euclide, forme 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. Ecrire un algorithme d'Euclide étendu non récursif.

Exercice 2.6.5 (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'algoritme d'Euclide nécessite le plus de divisions euclidiennes ?