Chapitre 1

Anneaux commutatifs, anneaux de polynômes : rappels et compléments

1.1 Définitions et exemples de base

Définition 1.1.1. Un anneau (resp. anneau commutatif) est un groupe abélien $(A, +)$ muni d'une seconde opération $m : A \times A \to A$, notée multiplicativement (i.e. le plus souvent sans symbole : $m(a, b) = ab$ ou avec un point si besoin),

qui est associative (resp. associative et commutative),
admet un élément neutre (appelé unité et souvent noté 1),
et est distributive à gauche et à droite par rapport à l'addition.

Remarque 1.1.2. Dans ce chapitre on ne s'intéresse qu'aux anneaux commutatifs.

Remarques 1.1.3.

1. Pour $x \in A$: $0.x = x.0 = 0$, et $(-1).x = -x = x.(-1)$.
2. Pour $x \in A$, $y \in A$, on a : $(-x)y = x(-y) = -(xy)$ et $(-x)(-y) = xy$.
3. Sauf pour l'anneau réduit au seul élément 0 (anneau nul), l'élément unité est non nul.

Définition 1.1.4. a) Un élément d'un anneau A est dit inversible si et seulement s'il est symétrisable pour la seconde opération.
b) Un élément non nul x d'un anneau A est un diviseur de zéro si et seulement si son produit avec un autre élément non nul vaut zéro :

$$\exists y \neq 0,\ xy = 0 \text{ ou } yx = 0\ .$$

On note $A^\times$ l'ensemble des éléments inversibles de A.

Proposition 1.1.5. *Si A est un anneau non nul, l'ensemble $A^\times$ des éléments inversibles est un groupe multiplicatif.*

Définition 1.1.6. a) Un corps est un anneau non nul ($1 \neq 0$) dans lequel tout élément non nul est inversible, i. e. $A^\times = A - \{0\}$.
b) Un anneau intègre est un anneau non nul sans diviseur de zéro ; un anneau commutatif intègre est aussi appelé *domaine d'intégrité*.

Exercice 1.1.7. Montrer qu'un anneau fini intègre est un corps.

Exemples 1.1.8.

1. L'anneau des entiers : $\mathbb{Z}$; les décimaux : $\mathbb{D}$.
2. Le corps des rationnels : $\mathbb{Q}$; les réels : $\mathbb{R}$; les complexes : $\mathbb{C}$.
3. Les anneaux de congruences : $\mathbb{Z}/n\mathbb{Z}$, $n \geq 2$; les corps $\mathbb{Z}/p\mathbb{Z}$ pour p premier.
4. Les anneaux de fonctions : si A est un anneau et X un ensemble, les applications de X vers A forment un anneau noté $\mathcal{A}(X, A)$.

Définition 1.1.9. Un sous-anneau d'un anneau A est une partie B de A qui est un anneau avec les opérations induites de A, et la même unité que A.

Proposition 1.1.10. *Une partie B d'un anneau A est un sous-anneau si et seulement si :*

B est un sous-groupe additif,
B est stable par multiplication, et
B contient l'unité de A.

Exemples 1.1.11.

1. L'ensemble des entiers de Gauss
$$\mathbb{Z}[i] = \{a + ib;\ a \in \mathbb{Z}, b \in \mathbb{Z}\}$$
forme un sous-anneau de $\mathbb{C}$.
2. Les fonctions complexes continues sur un intervalle I : $\mathcal{C}(I, \mathbb{C})$ forment un sous-anneau de $\mathcal{A}(I, \mathbb{C})$.

Exercice 1.1.12. Déterminer les éléments inversibles de $\mathbb{Z}[i]$.

Définition 1.1.13. Soit A et B deux anneaux. Une application $f : A \to B$ est un morphisme d'anneau si et seulement si f respecte les opérations et l'élément unité. Un isomorphisme d'anneau est un morphisme bijectif.

Définition 1.1.14. Soit A un anneau commutatif. Une algèbre sur A est un anneau B muni d'un morphisme d'anneau

$$\eta : A \to B \ .$$

Définition 1.1.15. Soient B_1 et B_2 deux algèbres sur l'anneau commutatif A, avec morphismes de structure $\eta_i : A \to B_i$. Un morphisme d'algèbre de B_1 vers B_2 est un morphisme d'anneau $f : B_1 \to B_2$ tel que :

$$\eta_2 = f \circ \eta_1 \ .$$

1.2 Anneaux de polynômes

Soit A un anneau commutatif et X une *indéterminée* (un symbole). On note $A[X]$ l'ensemble des suites d'éléments de A avec un nombre fini de termes non nul, notées comme combinaisons linéaires des X^n, $n \geq 0$: les éléments de $A[X]$ s'écrivent sous la forme :

$$P = \sum_n a_n X^n = \sum_{n=0}^{N} a_n X^n \ .$$

$A[X]$ est muni des opérations :

$$(\sum_n a_n X^n) + (\sum_n b_n X^n) = \sum_n (a_n + b_n) X^n \ .$$

$$(\sum_n a_n X^n) \times (\sum_m b_m X^m) = \sum_p c_p X^p \ , c_p = \sum_k a_k b_{p-k} \ .$$

Proposition 1.2.1. *$A[X]$ est une algèbre sur A.*

Remarque 1.2.2. L'application qui définit la structure d'algèbre est injective, d'image les polynômes constants ; A est identifié au sous-anneau de $A[X]$ formé par les polynômes *constants*.

Proposition 1.2.3 (Propriété universelle)**.** *Soit B une algèbre sur l'anneau commutatif A, et b un élément de B, alors il existe un unique morphisme d'algèbre $E_b : A[X] \to B$ tel que $E_b(X) = b$.*

Remarque 1.2.4. E_b est appelé morphisme d'évaluation et $E_b(P)$ est noté $P(b)$.

Définition 1.2.5. Le degré d'un polynôme non nul $P = \sum_n a_n X^n$ est le plus grand n pour lequel $a_n \neq 0$ (convention : $\deg(0) = -\infty$).

Proposition 1.2.6. *Si A est un anneau commutatif intègre, alors :*
a) $\deg(PQ) = \deg(P) + \deg(Q)$,
b) les inversibles de $A[X]$ sont les inversibles de A, et
c) $A[X]$ est un anneau intègre.

1.3 Anneaux quotients

Définition 1.3.1. Un idéal d'un anneau commutatif A est un sous-groupe additif I de A, tel que : $IA \subset I$.

Remarque 1.3.2. Dans le cas non commutatif, il y a une notion d'idéal à droite et d'idéal à gauche ; on précise parfois idéal bilatère.

Exemples 1.3.3. Dans $\mathbb{Z}$ tous les sous-groupes additifs sont de la forme $n\mathbb{Z}$; ce sont tous des idéaux.

Proposition 1.3.4. *Soit $f : A \to B$ un morphisme d'anneau. Le noyau de f est un idéal de A et l'image de f est un sous-anneau de B.*

Proposition 1.3.5. *Soit I un idéal d'un anneau A, alors la multiplication de A induit sur le groupe additif quotient une structure d'anneau.*

Proposition 1.3.6 (Factorisation d'un morphisme d'anneau)**.** *Soit $f : A \to B$ un morphisme d'anneau, I un idéal de A et $p : A \to A/I$ la projection* canonique*. Le morphisme f factorise par le quotient A/I (i.e. il existe un morphisme d'anneau $g : A/I \to B$ tel que $f = g \circ p$) si et seulement si $I \subset \mathrm{Ker}(f)$. Le morphisme g a même image que f et est injectif si et seulement si $I = \mathrm{Ker}(f)$.*

Corollaire 1.3.7 (Premier théorème d'isomorphisme des anneaux)**.** *Soit $f : A \to B$ un morphisme d'anneau, alors le quotient $A/\mathrm{Ker}(f)$ est isomorphe à l'image de f.*

Exercice 1.3.8 (Second théorème d'isomorphisme des anneaux). Soient B un sous-anneau de A, et I un idéal de A.

1. Démontrer que $B + I$ est un sous anneau de A.
2. Démontrer que $B \cap I$ est un idéal de B et que : $(B+I)/I$ est isomorphe à $B/(B \cap I)$.

Exercice 1.3.9 (Troisième théorème d'isomorphisme des anneaux). Soient $I \subset J$ deux idéaux de l'anneau A. Démontrer que J/I est un idéal de A/I, et que $A/J)$ est isomorphe à $(A/I)/(J/I)$.

1.4 Propriétés des idéaux

1.4.1 Constructions d'idéaux

Proposition 1.4.1. *L'intersection d'une famille non vide d'idéaux est un idéal.*

Corollaire 1.4.2. *Soit E une partie d'un anneau A, alors il existe un plus petit idéal qui contient E. On l'appelle l'idéal engendré par E, et on le note (E), ou $(E)_A$ s'il y a ambiguïté.*

Proposition 1.4.3 (Somme et produit)**.** *a) L'idéal engendré par $I \cup J$ est :*

$$I + J = \{i + j,\ i \in I\ j \in J\}\ .$$

On appelle cet idéal la somme de I et J.
b) L'idéal engendré par l'ensemble des produits ij, $i \in I$ $j \in J$ est :

$$\{\sum_k\ i_k j_k,\ \forall k\ i_k \in I\ j_k \in J\}\ .$$

Cet idéal est appelé le produit de I et J et noté (IJ).

Exercice 1.4.4. Soit A un anneau **commutatif**.

1. Démontrer que l'idéal engendré par $a \in A$ est Aa.
2. Démontrer que l'idéal engendré par $\{a_1, \ldots, a_n\} \subset A$ est $Aa_1 + \cdots + Aa_n$.

Définition 1.4.5. Un idéal principal est un idéal engendré par un élément. Un idéal de génération finie est un idéal engendré par une partie finie.

Proposition 1.4.6. *Tous les idéaux de $\mathbb{Z}$ sont principaux.*

Exercice 1.4.7. Quel est l'idéal engendré par un élément inversible ?

Exercice 1.4.8.
1. Quels sont les idéaux d'un corps ?
2. Montrer que si A est un corps, tout morphisme d'anneau $f : A \to B$ est injectif.
3. Montrer qu'un anneau commutatif qui a deux idéaux est un corps.

1.4.2 Idéaux maximaux

Définition 1.4.9. Un idéal I d'un anneau commutatif A est maximal si et seulement si A/I est un corps.

Le vocabulaire est justifié par la proposition suivante :

Proposition 1.4.10. *Dans un anneau commutatif non nul A, un idéal I est maximal si et seulement si c'est un élément maximal pour l'inclusion parmi les idéaux distincts de A.*

Théorème 1.4.11. *Tout anneau commutatif non nul contient au moins un idéal maximal.*

Corollaire 1.4.12. *Dans un anneau commutatif A, tout idéal distinct de A est contenu dans un idéal maximal.*

Remarque 1.4.13. La preuve générale du théorème précédent utilise le lemme de Zorn. Dans beaucoup d'anneaux le résultat est élémentaire et indépendant du lemme de Zorn.

fin du cours 14/09

1.4.3 Idéaux premiers

Définition 1.4.14. Un idéal I d'un anneau commutatif est premier si et seulement si A/I est un anneau intègre.

Remarque 1.4.15. Un anneau intègre est par définition non nul, l'anneau lui-même n'est donc pas un idéal premier.

Remarque 1.4.16. On peut reformuler la définition : L'idéal I de l'anneau A est premier si et seulement si $I \neq A$ et

$$\forall a,\ \forall b\ ab \in I \Rightarrow a \in I \text{ ou } b \in I\ .$$

Remarque 1.4.17. Dans un anneau commutatif tout idéal maximal est premier.

Dans $\mathbb{Z}$ l'idéal nul est premier mais n'est pas maximal. Les autres idéaux premiers sont les $p\mathbb{Z}$ avec p premiers. Ils sont maximaux.

1.5 Divisibilité dans les anneaux commutatifs intègres

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

Remarque 1.5.1. Il y a équivalence entre :

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

Proposition 1.5.2. *a) Sur A la relation $x \sim y \Leftrightarrow \exists u \in A^\times \ \ y = ux$ 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. L'existence n'est pas garantie, mais il y a toujours unicité comme classe d'éléments associés. Donnons une formulation précise naïve.

Définition 1.5.3. 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 :

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

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

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

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

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

Définition 1.5.4. $p \in A$ 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 1.5.5. *Si l'idéal pA est premier (on dit que p est premier), alors p est irréductible.*

1.6 Anneaux principaux

Définition 1.6.1. Un anneau principal est un anneau commutatif intègre dans lequel tout idéal est principal (engendré par un seul élément).

Définition 1.6.2. 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 1.6.3. L'application d est appelée un stathme (ou une norme).

Proposition 1.6.4. *Tout anneau euclidien est principal.*

Exemples 1.6.5. L'anneau $\mathbb{Z}$, les anneaux $\mathbb{K}[X]$ avec $\mathbb{K}$ un corps sont des anneaux euclidiens.

Théorème 1.6.6. *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 1.6.7. *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 $(m) = \bigcap_{a \in E} aA$.

Corollaire 1.6.8. *Dans un anneau principal toute partie non vide de A a un PGCD et un PPCM.*

Théorème 1.6.9 (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 1.6.10. *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 1.6.11. *Dans un anneau principal, tout idéal premier non nul est maximal.*

Proposition 1.6.12 (Lemme de Gauss)**.** *Dans un anneau principal A, si $a|bc$ et a est premier avec b, alors $a|c$.*

Corollaire 1.6.13 (Lemme d'Euclide)**.** *Dans un anneau principal A, si un élément premier divise un produit, alors il divise l'un des facteurs.*

Proposition 1.6.14. *Dans un anneau principal, toute suite croissante d'idéaux est stationnaire.*

Théorème 1.6.15. *Dans un anneau principal, il existe une décomposition en facteurs irréductibles, unique aux inversibles près et à l'ordre près des facteurs (essentiellement unique).*

1.7 Anneaux factoriels

Définition 1.7.1. 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 1.7.2. *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.

Proposition 1.7.3. *Dans un anneau factoriel toute famille finie a un PGCD et un PPCM.*

Proposition 1.7.4 (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 $a|c$.*

1.8 Corps des fractions

Dans cette section on considère des anneaux commutatifs intègres.

Définition 1.8.1. Une partie multiplicative d'un anneau commutatif intègre A est une partie S de $A - \{0\}$ contenant l'unité et multiplicativement stable.

Etant donné une partie multiplicative S d'un anneau (commutatif intègre) A. On définit $S^{-1}A$ comme le quotient de $S \times A$ par la relation :

$$(s, a) \sim (s', a') \Leftrightarrow sa' = as' \ .$$

On note $\frac{a}{s}$ la classe de (s, a) dans l'ensemble quotient $S^{-1}A$.

Théorème 1.8.2. *Les opérations :*

$$\frac{a}{s} + \frac{a'}{s'} = \frac{as' + sa'}{ss'} \ ,$$

$$\frac{a}{s} \times \frac{a'}{s'} = \frac{aa'}{ss'} \ ,$$

sont bien définies et munissent $S^{-1}A$ d'une structure d'anneau qui contient $\frac{A}{1} \approx A$ comme sous-anneau.

Théorème 1.8.3 (Propriété universelle)**.** *Pour tout morphisme d'anneau $f : A \to B$ qui envoie les éléments de S sur des inversibles, il existe une unique extension $F : S^{-1}A \to B$. Le noyau de F est l'idéal $S^{-1}\mathrm{Ker(f)}$; en particulier si f est injective alors F est aussi injective.*

Exemples 1.8.4.
1. Si on prend $S = A - \{0\}$, on obtient le corps des fractions de A : $\mathcal{Q}(A)$.
2. Pour $A = \mathbb{Z}$, $S = \{10^n,\ n \in \mathbb{N}\}$, on construit les décimaux.
3. Pour $A = \mathbb{K}[X]$, avec $\mathbb{K}$ un anneau commutatif, et $S = \{X^n,\ n \in \mathbb{N}\}$, on obtient l'anneau des polynômes de Laurent noté $\mathbb{K}[X, X^{-1}]$.
4. Pour $A = \mathbb{K}[X]$, avec $\mathbb{K}$ un corps commutatif, le corps des fractions obtenu est le corps des fractions rationnelles, noté $\mathbb{K}(X)$.

1.9 Critères d'irréductibilité

On étudie dans cette section l'irréductibilité des polynômes à coefficients dans un **anneau factoriel**. On utilisera la notation $\doteq$ pour une égalité modulo un inversible de l'anneau.

Définition 1.9.1. Soit A un anneau factoriel.
a) Le contenu $c(P)$ d'un polynôme $P \in A[X]$ est le PGCD de ses coefficients.
b) Un polynôme $P \in A[X]$ est primitif si et seulement si son contenu vaut 1 : $c(P) \doteq 1$.

Remarque 1.9.2. On suppose que l'anneau A est factoriel.
1. Un polynôme irréductible non constant de $A[X]$ est nécessairement primitif.
2. Si $P \in A[X]$ est primitif et irréductible dans $\mathcal{Q}(A)[X]$, alors il est irréductible dans $A[X]$. Nous allons étudier la réciproque.

16/09/2011

Lemme 1.9.3. *Soit f un élément irréductible dans l'anneau factoriel A. La surjection canonique $\pi : A \to A/fA$ s'étend en un morphisme d'anneau :*

$$\begin{array}{rccc} \Pi : & A[X] & \to & A/fA\,[X] \\ & P = \sum_k a_k X^k & \mapsto & \sum_k \overline{a}_k X^k \end{array} ,$$

et induit un isomorphisme : $A[X]/fA[X] \approx A/fA\,[X]$.

Corollaire 1.9.4. *Si f est un élément premier dans A, alors f est premier dans $A[X]$.*

Proposition 1.9.5. *Le produit de deux polynômes primitifs à coefficients dans un anneau factoriel est un polynôme primitif.*

Corollaire 1.9.6. *Pour P et Q dans $A[X]$, avec A factoriel, on a $c(PQ) \doteq c(P)c(Q)$.*

Corollaire 1.9.7. *Soit A un anneau factoriel. Si $P \in A[X]$ est divisible dans $\mathcal{Q}(A)[X]$ par un polynôme primitif $Q \in A[X]$, alors P est divisible par Q dans $A[X]$.*

Proposition 1.9.8. *Un polynôme $P \in A[X]$ non constant et primitif est irréductible dans $A[X]$ si et seulement s'il l'est dans $\mathcal{Q}(A)[X]$.*

Les polynômes constants irréductibles dans $A[X]$ sont les irréductibles de A. Les polynômes non constants irréductibles dans $A[X]$ sont les polynômes non constants primitifs de $A[X]$ qui sont irréductibles dans $\mathcal{Q}(A)[X]$.

Théorème 1.9.9 (Factorialité des anneaux de polynômes)**.** *Si A est un anneau factoriel, alors l'anneau $A[X]$ est factoriel.*

Proposition 1.9.10 (Réduction des coefficients)**.** *Soit f est un élément premier de l'anneau factoriel A, et soit $P \in A[X]$ un polynôme primitif non constant. Si la réduction de P modulo f est irréductible, alors P est irréductible dans $A[X]$, donc dans $\mathcal{Q}(A)[X]$.*

Proposition 1.9.11 (Critère d'Eisenstein)**.** *Soient A un anneau factoriel, f un élément irréductible de A, et*

$$P = \sum_{k=0}^{n} a_k X^k$$

un polynôme non constant primitif dans $A[X]$.
Si : $f \not| a_n$, $\forall i < n$ $f | a_i$, et $f^2 \not| a_0$, alors P est irréductible dans $A[X]$.

Exercice 1.9.12. Montrer que si A est un anneau intègre, les diviseurs d'un monôme de $A[X]$ sont des monômes.