Chapitre 1

Introduction à la structure d'anneau

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 certains ouvrages, l'existence d'un élément unité n'est pas demandée on précise alors le cas échéant : anneau avec unité ou anneau unitaire.

Remarques 1.1.3.

1. Pour tout $x \in A$: $0.x = x.0 = 0$, 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 q'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 $\mathcal{A}(X, A)$.
5. Quaternions : Les matrices 2×2 de la forme

$$\begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix},$$

avec α et β complexes, forment un corps non commutatif noté $\mathbb{H}$.

Exemple 1.1.9. Le produit $A \times B$ de deux anneaux est un anneau, avec les opérations définies composante par composante.

Définition 1.1.10. 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 1.1.11. *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.

Définition 1.1.12. Le centre d'un anneau A est l'ensemble des éléments de A qui commutent avec tous les autres. On le note $Z(A)$:

$$x \in Z(A) \Leftrightarrow \forall y \in A \ , \ xy = yx \ .$$

Proposition 1.1.13. *Le centre d'un anneau A est un sous-anneau.*

Exercice 1.1.14. Déterminer le centre du corps des quaternions $\mathbb{H}$.

Exemples 1.1.15.

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

Définition 1.1.17. 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 1.1.18. Soit A un anneau commutatif. Une algèbre sur A est un anneau B muni d'un morphisme d'anneau

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

Un morphisme d'algèbres sur A est un morphisme d'anneau $f : B_1 \to B_2$ tel que : $\eta_2 = f \circ \eta_1$, où les $\eta_i : A \to B_i$ sont les morphismes de structure.

Définition 1.1.19. 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 Exemples : polynômes, matrices, anneau de groupe

1.2.1 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.

1.2.2 Série formelles

Dans la définition précédente de l'anneau des polynômes, si on ne demande plus que la suite des coefficients soit à support fini, on obtient l'anneau des séries formelles à coefficients dans l'anneau commutatif A, noté $A[[X]]$. Les éléments de $A[[X]]$ s'écrivent :

$$S = \sum_n a_n X^n \ ,$$

sans aucune condition sur le support, ni sur la convergence quand celle-ci pourrait avoir un sens. Les opérations sont définies avec les mêmes formules que pour les polynômes.

Exercice 1.2.7. Caractériser les éléments inversibles de $A[[X]]$, lorsque A est un anneau commutatif intègre.

Exercice 1.2.8 (Nombres de Catalan). On note c_n le nombre de parenthésages d'un mot constitué de $n + 1$ symboles. Montrer que la série formelle $C = \sum_n c_n X^n$ satisfait une équation de degré 2. Résoudre l'équation et déduire le calcul de c_n..

1.2.3 Anneaux de matrices

Soit A un anneau commutatif, alors l'ensemble des matrices carrés d'ordre n à coefficients dans A, muni des formules d'addition et de multiplication habituelles, forme un anneau noté $\mathcal{M}_n(A)$; l'application qui à un élément de A associe la matrice scalaire correspondante définit une structure d'algèbre. Si A est un sous anneau de B, alors $\mathcal{M}_n(A)$ est un sous-anneau de $\mathcal{M}_n(B)$.

Proposition 1.2.9. *Les éléments inversibles dans $M \in \mathcal{M}_n(A)$ sont les matrices de déteerminant inversible.*

1.2.4 Anneau de groupe

Soient G un groupe, noté multiplicativement et A un anneau commutatif. On note $A[G]$ l'ensemble des familles, indexées par G et à support fini, d'éléments de A. La famille de termes λ_g, $g \in G$, est notée :

$$\sum_g \lambda_g g \ .$$

L'ensemble $A[G]$ est naturellement un groupe abélien. On obtient un anneau (et même une algèbre sur A), avec le produit (et le morphisme $\lambda \mapsto \lambda e$) :

$$(\sum_g \lambda_g g)(\sum_h \mu_h h) = \sum_u \sum_{gh=u} \lambda_g \mu_h u \ .$$

Remarque 1.2.10. Dans le cas où $\mathbb{K}$ est un corps, $\mathbb{K}[G]$ est un espace vectoriel de base G.

Exercice 1.2.11.

1. Montrer que l'algèbre $\mathbb{C}[\mathcal{S}_3]$ du groupe symétrique $\mathcal{S}_3$ n'est pas intègre.
2. Déterminer le centre de l'algèbre $\mathbb{C}[\mathcal{S}_3]$ (on rappelle que le groupe $\mathcal{S}_3$ est engendré par deux éléments).
3. Déterminer les idempotents centraux de l'algèbre $\mathbb{C}[\mathcal{S}_3]$, i.e. les éléments p du centre qui vérifient $p^2 = p$.
4. Un idempotent central z est minimal si et seulement si, pour tout idempotent central w, on a : $zw = 0$ ou $zw = z$.
   Montrer que l'unité de l'algèbre $\mathbb{C}[\mathcal{S}_3]$ s'écrit comme somme d'idempotents centraux minimaux.
5. Montrer que l'algèbre $\mathbb{C}[\mathcal{S}_3]$ est isomorphe à un produit d'algèbres de matrices.

1.3 Anneaux quotients

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

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).*

Remarque 1.4.3. Dans le cas non commutatif, il y a un idéal à gauche engendré par E et un idéal à droite engendré par E.

13/09/2010

Proposition 1.4.4 (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), ou simplement IJ.

Exercice 1.4.5. 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 $Aa_1 + \cdots + Aa_n$.

Exercice 1.4.6. Décrire l'idéal engendré par un élément a dans un anneau A non nécessairement commutatif.

Définition 1.4.7. Un idéal principal est un idéal engendré par un élément. Un idéal de génération finie est un idéal engendré par une partie finie.

Proposition 1.4.8. *Tous les idéaux de $\mathbb{Z}$ sont principaux.*

Exercice 1.4.9. Quel est l'idéal engendré par un élément inversible ?

Exercice 1.4.10.
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 1.4.11. Un idéal I d'un anneau A est maximal si et seulement si : $I \neq A$ et les seuls idéaux qui contiennent I sont I et A.

Proposition 1.4.12. *Dans un anneau commutatif non nul A, un idéal I est maximal si et seulement si A/I est un corps.*

Théorème 1.4.13. *Tout idéal est contenu dans un idéal maximal.*

Remarque 1.4.14. 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.

Définition 1.4.15. Le radical de Jacobson $\mathrm{Rad}(A)$ d'un anneau commutatif A est l'intersection de ses idéaux maximaux.

Exercice 1.4.16. Montrer qu'un élément a d'un anneau commutatif A appartient au radical de Jacobson si et seulement si pour tout $x \in A$, $1 - xa$ est inversible.

Définition 1.4.17. Un anneau commutatif A est un anneau local si et seulement s'il n'a qu'un seul idéal maximal.

Exercice 1.4.18. Montrer qu'un anneau commutatif est local si et seulement si l'ensemble de ses éléments non inversibles forment un idéal.

1.4.3 Idéaux premiers

Définition 1.4.19. Un idéal I d'un anneau commutatif est premier si et seulement si A/I est un anneau intègre.

Remarque 1.4.20. Un anneau intègre est par définition non nul, l'anneau lui-même n'est donc pas un idéal premier.

Remarque 1.4.21. 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 1.4.22. 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. 14/9/2010

Définition 1.4.23. Un élément x d'un anneau A est nilpotent si et seulement s'il existe un entier n tel que $x^n = 0$. Le plus petit n tel que $x^n = 0$ est l'ordre de nilpotence de x.

Proposition 1.4.24. *L'ensemble des éléments nilpotents d'un anneau commutatif A forme un idéal* $\mathrm{Nil}(A)$ *appelé le nilradical de A.*

Proposition 1.4.25. *Le nilradical d'un anneau commutif A est égal à l'intersection de ses idéaux premiers.*

1.5 Anneaux de fractions

Dans cette section on considère des anneaux commutatifs intègres.

Définition 1.5.1. 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 1.5.2. *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 1.5.3 (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}Ker(f) ; en particulier si f est injective alors F est aussi injective.*

Exemples 1.5.4.

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 $\mathbb{K}(X)$.
5. Pour $A = \mathbb{K}[[X]]$, avec $\mathbb{K}$ un anneau commutatif et $S = \{X^n,\ n \in \mathbb{N}\}$, on obtient l'anneau des séries de Laurent noté $\mathbb{K}[[X]][X^{-1}]$.
6. Pour $A = \mathbb{K}[[X]]$, avec $\mathbb{K}$ un corps commutatif, le corps des fractions est noté $K((X))$ (c'est le corps des séries de Laurent : voir l'exercice qui suit).
7. Si $\mathfrak{p}$ est un idéal premier, alors $S = A - \mathfrak{p}$ est une partie multiplicative et $S^{-1}A$ noté $A_{\mathfrak{p}}$ s'appelle l'anneau *localisé* en $\mathfrak{p}$. C'est un anneau local.

Exercice 1.5.5. Soit $\mathbb{K}$ un corps commutatif.

1. Montrer que dans l'anneau des séries formelles $\mathbb{K}[[X]]$ les éléments non inversibles forment un idéal $\mathfrak{p}$. Cet idéal est-il maximal ?
2. Montrer que $\mathbb{K}[[X]]$ a un seul idéal maximal.
3. Montrer que l'anneau des séries de Laurent $\mathbb{K}[[X]][X^{-1}]$ est égal au corps des fractions $\mathbb{K}((X))$.