GÉNÉRALITÉS SUR LES ANNEAUX

Chapitre 5

Ce polycopié est très largement inspiré du polycopié utilisé par mon prédécesseur K. Koufany, que je remercie pour son travail de rédaction.

Table des matières

1. Anneaux

Définition 1.1. — *Un* **anneau** *est un ensemble A muni de deux lois de compositions internes, une addition et un produit, vérifiant les conditions suivantes.*

1. *Muni de l'addition, A est un groupe commutatif, que nous noterons $(A, +)$.*

2. Le produit est associatif et distribue l'addition, c'est-à-dire, pour tout $x, x', y, y' \in A$,

$$(x + x')y = xy + x'y \quad et \quad x(y + y') = xy + xy'.$$

Si le produit est commutatif, on dit que l'anneau A est **commutatif**.

L'élément neutre pour $(A, +)$ sera noté 0_A. Si le produit admet un élément neutre (noté généralement 1_A), on dit que A est un anneau **avec unité** ou encore que A est **unitaire**. L'opposé d'un élément $a \in A$ (i.e. le symétrique pour $+$) sera noté $-a$ et on notera $a - b$ pour $a + (-b)$.

Si n est un entier naturel et a un élément de A, l'élément na de A est défini par

$$na = \begin{cases} 0 & \text{si } n = 0 \\ a + (n-1)a = \underbrace{a + \cdots + a}_{n \text{ fois}} & \text{si } n \geq 1 \end{cases}$$

et pour m entier relatif négatif, on pose $ma = -((-m)a)$, ce qui permet de définir na pour tout $n \in \mathbb{Z}$.

Si n est un entier naturel et a un élément de A, l'élément a^n de A est défini par

$$a^n = \begin{cases} 1 & \text{si } n = 0 \\ a \cdot a^{n-1} = \underbrace{a \cdot \cdots \cdot a}_{n \text{ fois}} & \text{si } n \geq 1 \end{cases}$$

Dans un anneau unitaire, on supposera que $0_A \neq 1_A$ (sans quoi l'anneau est réduit à $\{0_A\}$). Un anneau unitaire admet donc au moins deux éléments. Si A est un anneau unitaire et $P(X) = \sum_{k=0}^{n} \alpha_k X^k$ un polynômes à coefficients entiers relatifs, l'élément $P(a) = \sum_{k=0}^{n} \alpha_k a^k$ est aussi dans A.

Les anneaux considérés dans ce chapitre et les suivants, seront tous unitaires.

Exemple 1.2. — (a) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ muni des opérations usuelles sont des anneaux commutatifs et unitaires.

(b) $\mathbb{N}$ n'est pas un anneau, car $(\mathbb{N}, +)$ n'est pas un groupe.

(c) $\mathbb{Z}[i] := \{a + ib \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ muni de l'addition et la multiplication est un anneau commutatif et unitaire. On l'appelle *anneau des entier de Gauss*.

(d) Pour tout entier $n \geq 1$, $\mathbb{Z}/n\mathbb{Z}$ muni des opérations usuelles est un anneau commutatif et unitaire; le neutre pour l'addition est $\bar{0}$ et le neutre pour la multiplication est $\bar{1}$

(e) L'ensemble $\mathcal{M}_n(\mathbb{R})$, des matrices carrées $n \times n$ à coefficients réels, muni de l'addition et la multiplication est un anneau unitaire non commutatif. Le neutre pour l'addition est la matrice nulle et le neutre pour la multiplication est la matrice identifié I_n.

Plus généralement, si A est un anneau commutatif et unitaire, l'ensemble $\mathcal{M}_n(A)$ des matrices carrées $n \times n$ à coefficients dans A est un anneau unitaire non commutatif pour les opérations d'addition et multiplication définies par

$$\begin{cases} A + B = ((a_{ij} + b_{ij}))_{1 \leq i,j \leq n} \\ AB = ((\sum_{k=1}^{n} a_{ik} b_{kj}))_{1 \leq i,j \leq n} \end{cases}$$

où $A = (a_{ij})_{1 \leq i,j \leq n}$, $B = (b_{ij})_{1 \leq i,j \leq n}$ et $a_{i,j}, b_{ij} \in A$.

La proposition suivante est facile à vérifier.

Proposition 1.3. — *Soit A un anneau. On a les règles de calcul suivantes :*
(1) $a0_A = 0_A a = 0_A$;
(2) $(-a)b = a(-b) = -(ab)$;
(3) $(-a)(-b) = ab$;
(4) $(a - b)c = ac - bc$;
(5) $a(b - c) = ab - ac$;
(6) $n(ab) = (an)b = a(nb)$;
(7) $a\left(\sum_{k=1}^{m} b_k\right) = \sum_{k=1}^{m} ab_k$;
(8) $\left(\sum_{k=1}^{m} b_k\right) a = \sum_{k=1}^{m} b_k a$
où $a, b, c, b_1, \cdots, b_m$ sont des éléments de A; m un entier naturel non nul et n un entier relatif.

Proposition 1.4. — *Soit A un anneau unitaire.*
(1) Soit a, b deux éléments de A qui commutent, alors pour tout entier naturel n on a la formule du binôme de Newton

$$(a + b)^n = \sum_{k=0}^{m} \binom{n}{k} a^k b^{n-k}$$

(2) Soit a, b deux éléments de A qui commutent, alors pour tout entier naturel n on a

$$b^{n+1} - a^{n+1} = (b - a) \sum_{k=0}^{n} a^k b^{n-k}$$

Démonstration. — Les deux formules se montrent comme dans le cas connu $A = \mathbb{R}$. □

Un élément x de A est une **unité** de A, ou **inversible**, s'il existe $y \in A$ tel que $xy = 1_A = yx$. Cet inverse y est alors unique et noté x^{-1}. L'ensemble des éléments inversibles est noté $A^\times$.

Proposition 1.5. — *Soit A un anneau unitaire. L'ensemble $A^\times$ des éléments inversibles de A est un groupe pour le produit.*

Supposons A commutatif et unitaire. Deux éléments a et b de A sont dits **associés** s'il existe $u \in A^\times$ tel que $b = ua$. On définit ainsi une relation d'équivalence.

L'anneau A est **intègre** si $A \neq \{0\}$ et si pour tout $x, y \in A$, la relation $xy = 0_A$ implique $x = 0_A$ ou $y = 0_A$. Si A n'est pas intègre, il existe $x \neq 0_A$ et $y \neq 0$ tels que $xy = 0_A$. On dit alors que x et y sont des **diviseurs de zéro**.

Soit $a \in A$, l'application

$$f : \mathbb{Z} \ni n \mapsto na \in A$$

est un homomorphisme du groupe $(\mathbb{Z}, +)$ dans dans le groupe $(A, +)$. Le noyau de f est un sous-groupe de $(\mathbb{Z}, +)$, et il est donc de la forme $\mathrm{Ker}(f) = n\mathbb{Z}$ où n est un entier positif ou nul. Si f n'est pas injectif, alors $n \neq 0$; c'est l'ordre de x dans le groupe $(A, +)$.

Supposons A unitaire et prenons $a = 1_A$. Dans ce cas n est appelé la **caractéristique** de l'anneau A. Nous la noterons $\mathrm{car}(A)$. C'est le plus petit entier strictement positif tel que $n1_A = 0_A$. Cet entier vérifie aussi $\forall a \in A, na = 0$, car $na = a + a + \cdots + a = (1 + 1 + \cdots + 1)a = 0a = 0$. On a $\mathrm{car}(A) \neq 1$ car $1_A \neq 0_A$.

Si f est injectif, alors $n = 0$ et l'anneau A est de caractéristique zéro. Autrement dit, $\mathrm{car}(A) = 0$ si $(\forall n \in \mathbb{Z}),\ (n1_A = 0_A \Rightarrow n = 0)$.

Si A est intègre et si $\mathrm{car}(A) = n \neq 0$, alors n est un nombre premier. En effet, si $n = qr$, avec $q, r \in \mathbb{N}$, la relation $0_A = p1_A = (q1_A)(r1_A)$ donne $q1_A = 0_A$ ou $r1_A = 0_A$. Alors n divise q ou n divise r. Comme $n = qr$ il en résulte $n = q$ ou $n = r$. Ainsi n est premier.

En particulier si $n = p$ est un nombre premier, alors pour tout k tel que $1 \leq k \leq p-1$, l'entier p divise l'entier $\binom{p}{k}$ (puisque $k!\binom{p}{k} = p(p-1)\cdots(p-k+1)$ et que $p \wedge k = 1$). Il en résulte que dans un anneau A, intègre, unitaire, de caractéristique un nombre premier p, si $x, y \in A$ commutent, alors la formule du binôme de Newton est réduite à

$$(x + y)^p = x^p + y^p.$$

Exemples 1.6. —

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont tous intègres et de caractéristique 0.
2. Soit $n \in \mathbb{N}$, avec $n \geq 2$. Alors $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif et unitaire (d'élément neutre $\overline{1}$). Sa caractéristique est n. Le groupe des unités de $\mathbb{Z}/n\mathbb{Z}$ est
$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{k} \mid 0 \leq k \leq n-1,\ \mathrm{pgcd}(k, n) = 1\}.$$
L'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est premier.
3. L'ensemble $\mathbb{R}[X]$ est un anneau unitaire, commutatif, intègre et de caractéristique 0.

4. Le groupe des unité de l'anneau $\mathbb{Z}$ est $\mathbb{Z}^\times = \{1, -1\}$. Deux éléments sont associés s'ils sont égaux ou opposés.
   On a aussi $\mathbb{K}^\times = \mathbb{K}^* = \mathbb{K} \setminus \{0\}$, pour $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
5. Soit X un ensemble et A un anneau. L'ensemble $\mathcal{F}(X, A)$ des applications de X dans A est un anneau pour l'addition et du produit usuels des applications. Il est commutatif (respectivement unitaire) si A l'est.
6. Soit G un groupe commutatif. L'ensemble $A = \mathrm{End}(G)$, des endomorphismes du groupe G, muni de l'addition habituelle des applications et du produit de composition des applications, est un anneau unitaire non commutatif. Le groupe $A^\times$ des unités de l'anneau $\mathrm{End}(G)$ est le groupe $\mathrm{Aut}(G)$ des automorphismes du groupe G.
7. Si A est un anneau commutatif unitaire et $n \in \mathbb{N}^*$, l'ensemble $\mathcal{M}_n(A)$ des matrices à coefficients dans A, muni de l'addition et du produit usuels, est un anneau unitaire. Pour $n \geq 2$, il n'est pas commutatif, ni intègre. Le groupe $\mathcal{M}_n(A)^\times$ des unités de $\mathcal{M}_n(A)$ est le groupe $GL(n, A)$ des matrices $\mathcal{M} \in M_n(A)$ dont le déterminant $\det(M)$ est inversible dans l'anneau A.
8. L'ensemble $\mathbb{Z}[X]$ des polynômes à coefficients dans $\mathbb{Z}$, muni des lois usuelles $+$ et $\times$ est un anneau commutatif unitaire.

2. Morphismes d'anneaux

Définition 2.1 **(Homomorphisme d'anneaux)**. — *Soient A et B deux anneaux unitaires. On appelle* **homomorphisme** (*ou* **morphisme**) *d'anneaux de A dans B une application f de A dans B telle que :*
(1) $f(1_A) = 1_B$*;*
(2) $\forall a, b \in A,\ f(a + b) = f(a) + f(b)$*,*
(3) $\forall a, b \in A,\ f(ab) = f(a)f(b)$*.*
On note $\mathrm{Hom}(A, B)$ *l'ensemble des morphismes d'anneau de A dans B.*

Tout $f \in \mathrm{Hom}(A, B)$ est en particulier un homomorphisme du groupe commutatif $(A, +)$ dans le groupe commutatif $(B, +)$.

On a donc $f(0_A) = 0_B$ et $f(-a) = -f(a)$ pour tout $x \in A$.

Le noyau $\mathrm{Ker}(f) = \{a \in A \mid f(a) = 0_B\}$ est un sous-groupe de $(A, +)$ et f est injective si et seulement si $\mathrm{Ker}(f) = \{0_A\}$. On peut montrer que pour toute partie non vide X de A, $f^{-1}(f(X)) = X + \mathrm{Ker}(f)$. On aussi $f(A^\times) \subset B^\times$.

Un homomorphisme de A dans lui même est appelé un **endomorphisme** de l'anneau A. On note $\mathrm{End}(A)$ l'ensemble des endomorphismes de l'anneau A.

Un endomorphisme de l'anneau A qui est bijectif est appelé un **automorphisme** de l'anneau A. L'ensemble $\mathrm{Aut}(A)$ des automorphismes de l'anneau

A est un groupe pour la composition des applications, d'éléments neutre Id_A.

Exemple 2.2. — 1. Si A est un anneau. Pour out $a \in A$, on définit l'application $f_a : A \to A$, par $\forall x \in A$, $f_a(x) = ax$. Alors f_a est un morphisme d'anneaux de A dans A et l'application $a \mapsto f_a$ est un morphisme d'anneaux injectif de A dans $End(A)$.

3. Sous-anneaux

Définition 3.1 **(Sous-anneau)**. — *On appelle* **sous-anneau** *d'un anneau A, une partie non vide B de A telle que :*

1. *$(B, +)$ est un sous-groupe du groupe commutatif $(A, +)$.*
2. *B est stable par le produit : $\forall x, y \in B$, $xy \in B$.*

On en déduit que B est lui même un anneau quand on restreint à B l'addition et le produit de A. Si A est commutatif (resp. intègre), alors B est commutatif (resp. intègre). Si A est unitaire et si $1_A \in B$, alors la caractéristique de B est égale à celle de A.

Exemple 3.2. — 1. Les sous-groupes additifs du groupes $(\mathbb{Z}, +)$ sont les parties $k\mathbb{Z}$, où $k \in \mathbb{N}$. Ces sous-groupes sont les seuls sous-anneaux de $\mathbb{Z}$.
2. $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$, $\mathbb{Q}$ est un sous-anneau de $\mathbb{R}$ et $\mathbb{R}$ est un sous-anneau de $\mathbb{C}$.
3. L'ensemble $\mathbb{Z}[\sqrt{2}] := \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{R}$.
4. L'ensemble $\mathbb{Z}[i] := \mathbb{Z} + i\mathbb{Z}$, des entiers de Gauss, est un sous-anneau de $\mathbb{C}$.

Proposition 3.3 **(Caractérisation)**. — *Une partie B d'un anneau A est un sous-anneau si, et seulement si*

(a) $B \neq \emptyset$ (ce qui est équivalent à $0_A \in B$);
(b) $\forall x, y \in B$ on a $x - y \in B$ et $xy \in B$.

Démonstration. — Découle de la définition d'un sous-anneau. □

Proposition 3.4. — *Soit $f : A \to B$ un homomorphisme d'anneaux.*
Si A_1 est un sous-anneau de A, alors $f(A_1)$ est un sous-anneau de B.
Si B_1 est un sous-anneau de B, alors $f^{-1}(B_1)$ est un sous-anneau de A.
En particulier, $\mathrm{Ker}(f) = f^{-1}(\{0_B\})$ *et* $\mathrm{Im}(f) = f(A)$ *sont des sous-anneaux de A et B respectivement.*

Démonstration. — $f(A_1)$ et $f^{-1}(B_1)$ sont des sous-groupe additifs de B et A respectivement car f est en particulier un homomorphisme de groupes additifs de $(A,+)$ dans $(B,+)$. Ce sont des anneaux car ils sont stables par produits :

$$y, y' \in f(A_1) \iff \exists x, x' \in A_1 \ f(x) = y, f(x') = y' \Rightarrow yy' = f(xx') \in f(A_1).$$
$$x, x' \in f^{-1}(B_1) \iff f(x) \in B_1 \text{ et } f(x') \in B_1 \Rightarrow f(xx') = f(x)f(x') \in B_1$$
$$\iff xx' \in f^{-1}(B_1).$$

□

Proposition 3.5. — *Soient A un anneau et $(B_i)_{i\in\Lambda}$ une famille quelconque de sous-anneaux de A. Alors $\cap_{i\in\Lambda} B_i$ est un sous-anneau de A.*

Démonstration. — Il est claire que $(\cap_{i\in\Lambda} B_i, +)$ est un sous-groupe abélien de $(A,+)$. Si $x, y \in \cap_{i\in\Lambda} B_i$, alors $\forall i \in \Lambda$, $x, y \in B_i$. Comme B_i est un sous-anneau de A, $xy \in B_i$ et ceci pour tout $i \in \Lambda$. Ainsi $xy \in \cap_{i\in\Lambda} B_i$. □

Proposition 3.6 **(Sous-anneau engendré par une partie)**
Soient A un anneau commutatif et Ω une partie non-vide de A. Soit $\langle\Omega\rangle$ l'intersection de tous les sous-anneaux de A contenant Ω. Alors $\langle\Omega\rangle$ est le plus petit sous-anneau de A contenant Ω. Ses éléments sont les sommes finies $\sum x_1 \cdots x_k$ de produits en nombre fini d'éléments de $\Omega \cup (-\Omega)$. Le sous-anneau $\langle\Omega\rangle$ est appelé **sous-anneau engendré par** *Ω.*

Démonstration. — D'après la proposition précédente,

$$\langle\Omega\rangle := \bigcap_{\substack{B \text{ ss-an de } A \\ \Omega \subset B}} B$$

est un sous-anneau de A, il contient Ω. Comme il est contenu dans tous les sous-anneaux B, tels que $\Omega \subset B$, c'est le plus petit des sous-anneaux contenant Ω.

L'ensemble des sommes finies $\sum x_1 \cdots x_k$ de produits en nombre fini d'éléments de $\Omega \cup (-\Omega)$ est clairement stable par la différence et par le produit. C'est donc un sous-anneau de A. Il contient Ω et donc contenu dans $\langle\Omega\rangle$. Par minimalité de $\langle\Omega\rangle$, il est égal à $\langle\Omega\rangle$. □

Exemple 3.7. — *Si A est un anneau et $\Omega = \{a\}$ où $a \in A$, alors le sous-anneau de A engendré par a est*

$$\langle\Omega\rangle = \{k_1 a + \cdots + k_r a^r, \ r \in \mathbb{N}^*, k_i \in \mathbb{Z}\}.$$

En effet, d'une part si $H \subset A$ est un sous-anneau contenant a, par stabilité par le produit il doit contenir les élémets a^i. Puisque H est en particulier un sous-groupe, il doit alors contenir tous les éléments $k_i a^i$ pour $k_i \in \mathbb{Z}$. Finalement, par stabilité par la somme il doit contenir tous les éléments de la forme $k_1 a + \cdots + k_r a^r$.

Si on note $K = \{k_1 a + \cdots + k_r a^r,\ \ r \in \mathbb{N}^*, k_i \in \mathbb{Z}\}$*, on peut vérifier que* K *contient* 0*, et est stable par différences et par produits, donc il est un sous-anneau, ce qui termine la preuve du résultat.*

Exemple 3.8. — *Spécialisant l'exemple précédent avec* $A = \mathbb{Z}[X]$ *et* $a = X^2$*, le sous-anneau de* $\mathbb{Z}[X]$ *engendré par* X^2 *est l'ensemble des polynômes pairs et nuls en* 0 *(c'est-à-dire les* $\sum_{i=1}^{n} k_i X^{2i}$*). Notons* B *ce sous-anneau.*

4. Idéaux d'un anneau

Définition 4.1 **(Idéal)**. — *Soit* A *un anneau commutatif. On appelle* **idéal** *de l'anneau* A*, un sous-groupe* I *de* $(A, +)$ *tel que :*

$$\forall a \in A\ \forall x \in I\ \ ax \in I. \tag{1}$$

Dans un anneau quelconque A, il existe au moins deux idéaux, à savoir $\{0\}$ et A.

Soit A est un anneau unitaire. Si I est un idéal qui contient l'unité 1_A de A, alors $I = A$. En effet, pour tout $a \in A$, $a = a1_A \in I$. Plus généralement, si I contient un élément inversible u de A, alors $1_A = u^{-1}u \in I$ et donc $I = A$.

Un idéal de A est un sous-anneau de A car (1) montre que $xy \in I$ pour tout $x \in I$ et pour tout $y \in I$. la réciproque est fausse ; par exemple $\mathbb{Z}$ est un sous-anneau de $\mathbb{R}$ mais n'est pas un idéal de $\mathbb{R}$.

Exemples 4.2. — Les ensembles $k\mathbb{Z}$ sont des idéaux de l'anneau $\mathbb{Z}$. D'une façon générale, si A est un anneau, alors pour tout $a \in A$, l'ensemble $aA = \{ax\ :\ x \in A\}$ est un idéal de A. C'est l'**idéal de** A **engendré par** a.

Proposition 4.3. — *Soit* $f : A \to B$ *un morphisme d'anneaux.*

(1) Si J *est un idéal de* B*, alors* $f^{-1}(J)$ *est un idéal de* A*. En particulier, le noyau* $\mathrm{Ker}(f) = f^{-1}\{(0_B\})$ *de* f *est un idéal de* A*.*

(2) Si f *est surjectif, alors pour tout idéal* I *de* A*, l'image* $f(I)$ *est un idéal de* B*.*

Démonstration. — (1) $(f^{-1}(J), +)$ est un sous-groupe abélien de $(A, +)$. De plus si $a \in A$ et $x \in f^{-1}(J)$, alors $f(x) \in J$ et $f(ax) = f(a)f(x) \in J$. D'où $ax \in f^{-1}(J)$.

(2) $(f(I), +)$ est un sous-groupe abélien de $(B, +)$. De plus si f est surjectif et si $b \in B$ et $y = f(x) \in f(I)$ avec $x \in I$, alors il existe $a \in A$ tel que $b = f(a)$. D'où $by = f(a)f(x) = f(ax) \in f(I)$, car $ax \in I$. □

Proposition 4.4. — *Soit* A *un anneau commutatif et soit* $(I_k)_{k\in\Lambda}$ *une famille d'idéaux de* A*.*

(1) $\cap_{k\in\Lambda} I_k$ *est un idéal de* A.
(2) L'ensemble $\sum_{k\in\Lambda} I_k = I_1 + I_2 + \cdots$ *des élément de* A *qui sont somme finie* $x_{i_1} + \cdots + x_{i_p}$ *d'éléments de* $\cup_{k\in\Lambda} I_k$ *est un idéal de* A. *C'est le plus petit idéal de* A *contenant* I_k *pour tout* $k \in \Lambda$.
En particulier, si I *et* J *sont deux idéaux de* A, *alors* $I + J = \{x + y;\ x \in I, y \in J\}$ *est un idéal de* A.

Démonstration. — Le preuve de (1) est immédiate. Pour (2), il suffit de le faire pour deux idéaux I et J. □

Proposition 4.5 **(Idéal engendré par une partie)**
Soit A *un anneau unitaire et commutatif. Soit* Ω *une partie de non vide de* A. *L'intersection de tous les idéaux de* A *contenant* Ω *est un idéal de* A. *C'est le plus petit idéal de* A *contenant* Ω. *De plus cet idéal s'écrit*

$$I = \{a_1x_1 + \cdots + a_px_p;\ \ p \in \mathbb{N}^*, x_1, \cdots, x_p \in \Omega, a_1, \cdots, a_p \in A\}.$$

Cet idéal est appelé, **idéal de** A **engendré par** Ω.

Démonstration. — La démonstration est similaire à celle de la proposition 3.6
□

Proposition 4.6. — *L'idéal engendré par un élément* $a \in A$ *est* aA, *soit l'ensemble des éléments de la forme* ab, *avec* $b \in A$.

Démonstration. — Par propriété d'un idéal, tout idéal H contenant a doit contenir aA. Réciproquement, on vérifie que $K := aA$ est un idéal, ce qui prouve la proposition. □

5. Quotient par un idéal

On suppose dans ce paragraphe que A est un anneau commutatif. Soit I un idéal de A. Comme I est en particulier un sous groupe abélien du groupe additif $(A, +)$ on peut considérer le groupe quotient A/I des classes d'équivalences pour la congruence modulo I :

$$x \equiv y \pmod{I} \iff x - y \in I.$$

Autrement dit, la classe d'un élément $x \in A$ est $\overline{x} = x + I$. Cette relation d'équivalence est compatible avec le produit de l'anneau A, dans le sens où, pour tout $x, y \in A$, la condition $x \equiv y \pmod{I}$ implique que $ax \equiv ay$ et pour tout $a \in A$.

Proposition 5.1. — *Soient* A *un anneau commutatif et* I *un idéal de* A. *Le quotient* A/I, *muni des opérations* $\overline{x}\dot{+}\overline{y} = \overline{x+y}$ *et* $\overline{x}\dot{\times}\overline{y} = \overline{xy}$ *est un anneau.*

Si de plus A est unitaire d'élément unité 1_A, alors A/I est unitaire d'élément unité $\overline{1}_A$.

Démonstration. — On sait déjà que A/I est un groupe pour la loi $\dot{+}$. De plus la loi $\dot{\times}$ est associative, distribue la somme $\dot{+}$. Il est clair ensuite que si 1_A est l'élément neutre de A alors $\overline{1}_A$ est l'élément neutre pour A/I. □

Remarque 5.2. — *Le but de cette remarque est d'illustrer le fait que le quotient A/B d'un anneau par un sous-anneau n'a pas en général pas une structure d'anneau. Considérons en effet l'Exemple 3.8, et imaginons que A/B acquière une structure d'anneau par les lois $\dot{+}$ et $\dot{\times}$ définies dans la Proposition précédente. Alors on aurait $\overline{0}\dot{\times}\overline{X} = \overline{0}$, et aussi $\overline{X^2}\dot{\times}\overline{X} = \overline{X^3}$. Or, $\overline{0} = \overline{X^2}$, mais $\overline{0} \neq \overline{X^3}$. Il y a donc une contradiction à supposer que $\dot{\times}$ est bien définie.*

Par contre, si on considère l'idéal *I engendré par X^2, qui est donc l'espace des polynômes s'écrivant sous la forme $\sum_{i=2}^{n} k_i X^i$, le quotient A/I est alors l'ensemble des classes $k_0\overline{1} + k_1\overline{X}$. Il est muni du produit défini par*

$$\begin{cases} \overline{1}\dot{\times}\overline{1} = \overline{1} \\ \overline{1}\dot{\times}\overline{X} = \overline{1} \\ \overline{X}\dot{\times}\overline{X} = 0\,. \end{cases}$$

***Proposition 5.3* (factorisation canonique).** — *Soit $f : A \to B$ un morphisme d'anneaux commutatifs. Alors $\mathrm{Ker}(f) = \{x \in A \mid f(x) = 0\}$ est un idéal de A et $\mathrm{Im}(f) = f(A)$ est un sous-anneau de B. Il existe un unique isomorphisme d'anneaux $\overline{f} : A/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ vérifiant $\forall x \in A$, $\overline{f}(\overline{x}) = f(x)$.*

Démonstration. — L'application f est en particulier un morphisme du groupe $(A, +)$ vers le groupe $(B, +)$ et $\mathrm{Ker}(f)$ est en particulier un sous-groupe (distingué) de $(A, +)$. En en déduit d'après le théorème de factorisation canonique des morphismes de groupes qu'il existe un unique isomorphisme $\overline{f}$ du groupe $A/\mathrm{Ker}(f)$ vers le groupe $f(A)$ vérifiant $\overline{f}(\overline{x}) = f(x)$ pour tout $x \in A$. Il reste alors à vérifier que $\overline{f}$ est un morphisme d'anneaux. Mais si $\overline{x}, \overline{y} \in A/\mathrm{Ker}(f)$ alors $\overline{f}(\overline{x}\dot{\times}\overline{y}) = \overline{f}(\overline{xy}) = f(xy) = f(x)f(y) = \overline{f}(\overline{x})\overline{f}(\overline{y})$. □

Exemple 5.4. — Soit $\Phi : \mathbb{R}[X] \to \mathbb{C}$ défini par : i $P(X) = \sum_{k=0}^{n} a_k X^k$ est un polynôme de $\mathbb{R}[X]$, alors $\Phi(P) = P(i) = \sum_{k=0}^{n} a_k i^k$. Il est clair que Φ est un morphisme d'anneaux.
De plus, si $P \in \mathrm{Ker}\,\Phi$, alors $P(i) = 0$, ce qui veut dire que i est une racine de P. Comme P est à coefficients réels, le complexe conjugué $\overline{i} = -i$ est aussi racine de P. Par conséquent P est divisible par le polynôme $X^2 + 1$. On en déduit que $\mathrm{Ker}\,\Phi = \langle X^2 + 1\rangle$ est l'idéal de $\mathbb{R}[X]$ engendré par $X^2 + 1$. Or, Φ est clairement surjectif, d'où l'isomorphisme d'anneaux

$$\mathbb{R}[X]/\langle X^2 + 1\rangle \simeq \mathbb{C}.$$

Corollaire 5.5. — *Soit A un anneau commutatif et unitaire et soit $I \subset J$ deux idéaux de A. Alors les anneaux A/J et $(A/I)/(J/I)$ sont isomorphes,*

$$(A/I)/(J/I) \simeq A/J.$$

Démonstration. — Tout d'abord, les idéaux de l'anneau quotient A/I sont de la forme J/I où J est un idéal de A contenant I.

Soit $f : A \to A/J$ et $g : A \to A/I$ les morphismes canoniques. Comme $\operatorname{Ker} f = J$ et $I \subset J$, il existe donc un morphisme $\bar{f} : A/I \to A/J$ tel que $\bar{f} \circ g = f$. On a aussi $\operatorname{Im} \bar{f} = \operatorname{Im} f = A/J$, donc $\bar{f}$ est surjectif. De plus, si $\bar{x} \in A/I$, alors

$$\bar{x} \in \operatorname{Ker} \bar{f} \iff \bar{f}(\bar{x}) = 0_A \iff f(x) = 0_A \iff x \in \operatorname{Ker} f = J.$$

Ainsi $\operatorname{Ker} \bar{f} = J/I$. Par factorisation canonique, l'anneau $(A/I)/(J/I)$ est isomorphe à l'anneau A/J. □

Proposition 5.6. — *Soit A un anneau et $I \subset A$ un idéal. Notons $p : A \to A/I$ l'application quotient, $\mathcal{I}_I(A)$ l'ensemble des idéaux de A contenant I, et $\mathcal{I}(A/I)$ l'ensemble des idéaux de l'anneau quotient A/I. L'application*

$$\begin{array}{rccc} \varphi & : & \mathcal{I}_I(A) & \to & \mathcal{I}(A/I) \\ & & J & \mapsto & p(J) \end{array}$$

est une bijection croissante (pour l'ordre donné par l'inclusion des idéaux) et son inverse ψ est donné par $\psi(K) = p^{-1}(K)$.

Démonstration. — Tout d'abord, puisque p est surjective, pour $J \in \mathcal{I}_I(A)$, $p(J)$ est bien un idéal de A/I, par la Proposition 4.3. On vérifie que φ est bijective en observant que $\varphi \circ \psi(K) = K$ pour $K \in \mathcal{I}(A/I)$ et que $\psi \circ \varphi(J) = J$ pour $J \in \mathcal{I}_I(A)$. Si $J_1, J_2 \in \mathcal{I}_I(A)$ avec $J_1 \subset J_2$, alors clairement $p(J_1) \subset p(J_2)$, ce qui montre que φ est croissante. Un raisonnement similaire montre que ψ est croissante. □

6. Idéaux maximaux

Définition 6.1. — *Soit A un anneau commutatif et unitaire et I un idéal de A.*
On dit que I est un **idéal maximal** *si $I \neq A$ et si les seuls idéaux de A contenant I sont soit I soit A.*

Remarque 6.2. — *La Proposition 5.6 donne par restriction une bijection entre les idéaux maximaux de A contenant I et les idéaux maximaux de A/I.*

Définition 6.3. — *Un ensemble E est dit* **totalement ordonné** *si, et seulement si, E est ordonné et que deux éléments quelconques de E sont comparables.*

Un ensemble ordonné E est dit **inductif** *si, et seulement si, toute partie de E totalement ordonnée admet un majorant.*

***Lemme 6.4* (Lemme de Zorn).** — *Un ensemble ordonné inductif E possède un élément maximal.*

Le théorème suivant est une conséquence du lemme de Zorn et démontre l'existence d'idéaux maximaux dans tout anneau unitaire commutatif.

***Théorème 6.5* (de Krull).** — *Tout anneau commutatif unitaire a un moins un idéal maximal.*

Démonstration. — Soit A un anneau commutatif unitaire. Soit E l'ensemble de tous les idéaux de A distincts de A,

$$E = \{J \text{ idéal de } A \mid J \neq A\}.$$

L'ensemble E est non vide, car contient au moins l'idéal $\{0_A\}$. L'inclusion définit une relation d'ordre dans E. Ce n'est pas un ordre total, mais seulement un ordre partiel (c'est-à-dire que, si $I, J \in E$ quelconques, on n'a pas forcément $I \subseteq J$ ou $J \subseteq I$).

Soit $F = (I_k)_{k\in X}$ une famille d'éléments de E totalement ordonnée par l'inclusion ($\forall k, \ell \in X$, on a $I_k \subseteq I_\ell$ ou $I_\ell \subseteq I_k$). On peut facilement vérifier qu'alors

$$I = \bigcup_{k\in X} I_k$$

est un idéal de A. (Rappelons qu'en général une réunion d'idéaux n'est pas un idéal, mais le fait que I soit ici un idéal provient du fait que tous les I_k sont emboités puisque la famille est totalement ordonnée).

L'idéal I est distinct de A (car sinon on aurait $1 \in I$, donc il existerait $k \in X$ tel que $1 \in I_k$, d'où $I_k = A$, ce qui contredirait $I_k \in E$). Donc $I \in E$, et il est clair que tout $I_k \in F$ vérifie $I_k \subseteq I$. On en déduit E est inductif.

D'après le Lemme de Zorn, E admet un majorant (un element maximal), noté M. Cela signifie que, si $J \in E$ tel que $M \subseteq J$, alors on a $J = M$. En d'autres termes, quel que soit un idéal J de A tel que $J \neq A$ et $M \subseteq J$, on a $J = M$. □

Corollaire 6.6. — *Soit A un anneau commutatif unitaire.*

(a) Tout idéal distinct de A est contenu dans un idéal maximal de A.
(b) Tout élément de A non inversible dans A est contenu dans un idéal maximal de A.

Démonstration. — Soit $I \subsetneq A$ un idéal. D'après le théorème de Krull l'anneau A/I admet un idéal maximal, et la Remarque 6.2 implique que A possède un idéal maximal contenant I. Ceci montre le point (a). Le point (b) en découle :

en effet, étant donné $a \in A$ non inversible, aA est un idéal strict car $1 \notin aA$, et on peut donc appliquer le point (a) à cet idéal. □

Exemple 6.7. — Les idéaux maximaux de l'anneau $\mathbb{Z}$, sont de la forme $p\mathbb{Z}$ avec p premier. En effet, un idéal de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$, où $n \in \mathbb{N}$. Cet idéal est maximal, si pour tout autre idéal $k\mathbb{Z}$ de $\mathbb{Z}$ tel que $n\mathbb{Z} \subset k\mathbb{Z}$, on a $k\mathbb{Z} = n\mathbb{Z}$ ou $k\mathbb{Z} = \mathbb{Z}$. Cela signifie alors que si $k|n$, alors $k = n$ ou $k = 1$ et donc n est premier.

7. Corps

Définition 7.1. — *Un* **corps** *est un anneau K unitaire (d'élément neutre $1_K \neq 0_K$) dans lequel tout élément non nul x possède un inverse x^{-1}.*
Si le produit est commutatif, on dira que le corps K est commutatif.
On appelle **sous-corps** *d'un coprs K un sous-anneau L de K contenant l'unité 1_K de K et tel que, pour tout élément non nul $x \in L$, on ait $x^{-1} \in L$.*

Remarque 7.2. — (1) Les exemples élémentaires de corps sont $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$. L'anneau $\mathbb{Z}$ n'est pas un corps, car tout élément $n \neq \pm 1$ n'est pas inversible dans $\mathbb{Z}$.

(2) Si p est un entier premier, alors $\mathbb{Z}/p\mathbb{Z}$ est un corps commutatif.

(3) Un corps K est un anneau unitaire dont le groupe des unités vérifie, $K^\times = K \setminus \{0_K\} =: K^*$.

(4) Un corps K est nécessairement intègre : si $xy = O_K$ et si $x \neq 0_K$, alors x est inversible et $y = x^{-1}(xy) = 0_K$.

(5) L'intersection d'une famille $(K_i)_{i\in\Lambda}$ de sous-corps d'un corps K est un sous-corps de K.
Si X est une partie non vide d'un corps K, le sous-corps de K engendré par X est l'intersection de tous les sous-corps de K contenant X.

(6) Les corps que nous allons considérer dans ce chapitre et les suivants seront toujours supposés commutatifs.

Proposition 7.3. — *Soit K un anneau commutatif et unitaire. K est un corps, si, et seulement si, les seuls idéaux de K sont $\{0_K\}$ et K.*

Démonstration. — Supposons que K est un corps. Soit I un idéal de K. Si $I \neq \{0_K\}$, alors il existe $x \in I$ non nul, donc inversible. On a $1_K = x^{-1}x \in I$ et donc $I = K$.
Réciproquement, supposons que les seuls idéaux de K sont $\{0_K\}$ et K. Soit $x \neq 0_K$ un élément de K et $I = xK$ l'idéal de K engendré par x. Comme $x \in I$, on a $I = K$. Par conséquent $1_K \in K = I = xK$ et il existe un élément non nul $y \in K$ tel que $xy = 1_K$. Cela signifie que x est inversible et que K est un corps. □

8. Quotient par un idéal maximal, idéal premier

Proposition 8.1. — *Soit A un anneau commutatif et unitaire. Pour qu'un idéal I de A soit maximal, il faut et il suffit que A/I soit un corps.*

Démonstration. — D'après la proposition 7.3, l'anneau A/I est un corps si et seulement si $\{0_A\}$ et A/I sont les ses seuls idéaux, ce qui signifie que I et A sont les seuls idéaux de A contenant I, c-est-à-dire que I est maximal. □

Corollaire 8.2. — *L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si p est un nombre premier.*

Démonstration. — Cela découle du fait déjà vu : l'idéal $p\mathbb{Z}$ est maximal si et seulement si p est un nombre premier. □

Définition 8.3. — *Soit A un anneau commutatif et unitaire. Un idéal I de A est dit* **idéal premier** *si, $I \neq A$ et si pour tout $x, y \in A$,*

$$xy \in I \Rightarrow x \in I \quad ou \quad y \in I.$$

C'est-à-dire si dans A/I la condition $\bar{x}\bar{y} = \bar{0}_A$ implique $\bar{x} = \bar{0}_A$ ou $\bar{y} = \bar{0}_A$, ce qui signifie que A/I est un anneau intègre.

Proposition 8.4. — *Tout idéal maximal de A est un idéal premier.*

Démonstration. — Si l'idéal I est maximal, A/I est un corps et donc intègre, ce qui veut dire que I est premier. □

Remarque 8.5. — *La réciproque est fausse : un idéal premier, n'est pas forcément maximal : l'idéal $\{0\}$ de $\mathbb{Z}$ est premier, mais pas maximal.*

On a le diagramme suivant :

$$\begin{array}{ccc} I \text{ maximal} & \Leftrightarrow & A/I \text{ corps} \\ \Downarrow & & \Downarrow \\ I \text{ premier} & \Leftrightarrow & A/I \text{ intègre} \end{array}$$

9. Corps de fractions d'un anneau intègre

Soit A un anneau intègre. On définit sur l'ensemble $A \times A \setminus \{0_A\}$ la relation suivante

$$(a, s)\mathcal{R}(a', s') \Longleftrightarrow as' = a's.$$

La relation $\mathcal{R}$ est une relation d'équivalence. En effet, il est claire que cette relation est refléxive et symétrique. Vérifions qu'elle est transitive.

Soit $(a, s), (a', s'), (a'', s'') \in A \times A \setminus \{0_A\}$. Si $(a, s)\mathcal{R}(a', s')$ et $(a', s')\mathcal{R}(a'', s'')$, alors $as' = a's$ et $a's'' = a''s'$, d'où $as's'' = a'ss''$ et $a's''s = a''s's$ ce qui implique $s'(as'') = s'(a''s)$ ou encore $s'(as'' - a''s) = 0_A$. Comme A est intégère et que $s' \neq 0_A$, on a $as'' = a''s$ ce qui veut dire $(a, s)\mathcal{R}(a'', s'')$.

Notons $\overline{(a,s)}$ la classe d'un élément $(a,s) \in A \times A \setminus \{0_A\}$. Si $u = \overline{(a,s)}$ et $v = \overline{(a',s')}$ sont deux éléments de $(A \times A \setminus \{0_A\})/\mathcal{R}$, on pose

$$\begin{aligned} u+v &= \overline{(as'+a's, ss')} \\ uv &= \overline{(aa', ss')} \end{aligned}$$

Ces deux lois sont bien définies, c-à-d ne dépendent pas des représentants choisis. En effet, si (b,t) est un autre représentant de u et (b',t') un autre représentant de v, alors $(a,s)\mathcal{R}(b,t)$ et $(a',s')\mathcal{R}(b',t')$, donc

$$at = bs \tag{2}$$

$$a't' = b's' \tag{3}$$

En multipliant (2) par $t's'$ et (3) par ts et en ajoutant les relations on obtient

$$(as'+a's)tt' = (bt'+b't)ss'$$

d'où $(as'+a's, tt')\mathcal{R}(bt'+b't, ss')$ et donc $\overline{(a,s)+(a',s')} = \overline{(b,t)+(b',t')}$.
On montre de même que $\overline{(a,s)\times(a',s')} = \overline{(b,t)\times(b',t')}$

Il est facile de vérifier que l'ensemble quotient $K := A \times A \setminus \{0_A\}/\mathcal{R}$ muni de ces deux lois est un corps commutatif, appelé **corps des fractions** de l'anneau A. L'élément neutre pour l'addition est $\overline{(0_A,1_A)}$, l'élément neutre pour la multiplication est $\overline{(1_A,1_A)}$, l'opposé de $\overline{(a,s)}$ est $\overline{(-a,s)}$. En plus tout élément $(a,s) \in A \setminus \{0_A\} \times A \setminus \{0_A\}/\mathcal{R}$ est inversible pour la multiplication d'inverse $\overline{(s,a)}$.
On note aussi parfois les fractions $\overline{(a,s)}$ par $\frac{a}{s}$.

Comme $\overline{(a,1_A)} + \overline{(b,1_A)} = \overline{(a+b,1_A)}$ et que $\overline{(a,1_A)(b,1_A)} = \overline{(ab,1_A)}$, alors l'application

$$\begin{array}{cccc} \varphi & A & \to & K \\ & a & \mapsto & \overline{(a,1_A)} \end{array}$$

est un morphisme d'anneaux. De plus,

$$\varphi(a) = 0_K \iff \overline{(a,1_A)} = \overline{(0_A,1_A)} \iff (a,1)\mathcal{R}(0_A,1_A) \iff a = 0_A$$

donc φ est injectif. On en déduit que A peut être considéré comme un sous-anneau de K.