4 Anneaux et Corps

1 Anneaux et idéaux

1.1 Rappel sur la définition

La définition des anneaux est bien connue. Commençons par une remarque : dans un anneau, l'addition est toujours commutative (cela fait partie de la définition), mais il n'est pas imposé que la multiplication soit commutative : les anneaux de matrices (carrées) en sont un exemple, ainsi que les anneaux d'endomorphismes. Nous décidons de nous limiter aux anneaux commutatifs (et aux corps commutatif), mais nous signalerons de temps à autre ce qui se passe pour des anneaux non commutatifs. Par contre pour nous, et contrairement à d'autres auteurs, un anneau contiendra toujours un neutre pour la multiplication.

1.2 Éléments particuliers d'un anneau commutatif

On notera 0_A et 1_A les deux neutres d'un anneau A.

Proposition 47. – *0_A est absorbant : pour tout $a \in A$, $0 \times a = 0$.*
– *$1_A \neq 0_A$ sauf si A est réduit à 0 (anneau nul).*
– *Si on note $-a$ l'opposé de a, on a :*

$$-a = (-1)a, \qquad (-a)b = a(-b) = -(ab) \qquad \textit{etc..}$$

Définition 20. Un élément a d'un anneau est **inversible** s'il existe a^{-1} dans l'anneau tel que $aa^{-1} = a^{-1}a = 1$. On dit également que c'est une **unité** [1].

Proposition 48. *L'ensemble $A^\times$ des éléments d'un anneau qui sont inversibles est un groupe pour le produit.*

Démonstration. L'essentiel résulte du calcul :

$$abb^{-1}a^{-1} = 1_A$$

■

Une propriété utile pour les calculs :

Définition 21. $a \in A$ est **régulier** si

$$\forall (x, y) \in A^2, \qquad (ax = ay) \Rightarrow (x = y)$$

1. Dans un anneau non commutatif, un élément peut n'être inversible que à gauche ou que à droite.

Cette propriété est moins forte que l'inversibilité car

Proposition 49. *Si $a \in A$ est inversible, alors a est régulier.*

Démonstration.
$$(ax = ax') \Rightarrow (a^{-1}(ax) = a^{-1}(ax')) \Rightarrow x = x'$$
■

La notion «contraire» est également utile.

Définition 22. Un élément a d'un anneau A est un **diviseur de zéro**, s'il est non nul, et s'il existe b non nul tel que $ab = 0$.

Proposition 50. *$a \in A$ est non nul et non diviseur de zéro si et seulement si il est régulier.*

Démonstration. Supposons a non nul et non diviseur de zéro

$$\forall (b, b') \in A^2, \qquad ab = ab' \Rightarrow a(b - b') = 0 \Rightarrow b = b'$$

et dans l'autre sens, si $ab = 0$, on a $ab = a0$, donc si a est régulier, $b = 0$ et a n'est pas diviseur de zéro. ■

L'ensemble des réguliers peut contenir strictement l'ensemble des inversibles, c'est par exemple le cas dans $\mathbb{Z}$. Parmi les anneaux connus :

1. Les inversibles de $\mathbb{Z}$ sont 1 et -1. Les éléments réguliers sont tous les éléments non nuls.
2. Les inversibles et les réguliers de $\mathbb{Z}/n\mathbb{Z}$ sont les $\overline{k}$ où k est premier à n.

Terminons ces généralités par deux définitions :

Définition 23. – Un anneau commutatif non nul est **intègre** s'il n'a pas de diviseur de zéro.
– Un anneau commutatif non nul est un **corps commutatif** si tous ses éléments non nuls sont inversibles.

Comme un inversible n'est jamais diviseur de zéro, un corps est intègre.

Théorème 51. *Si A est un anneau fini, alors A est intègre si et seulement si A est un corps.*

Démonstration. On a déjà dit qu'un corps est intègre. Supposons A fini, et considérons, pour $a \in A$ non nul, l'application $x \mapsto ax$. C'est une application de A dans A. Puisque A est intègre elle est injective : $ax = ay \Rightarrow x = y$. Puisque A est fini elle est bijective : cela implique que 1_A admet un antécédent, a est inversible. ■

1.3 Sous-anneaux

Si A est un anneau, un sous-ensemble non vide B est un **sous-anneau** de A s'il est un sous-anneau pour les mêmes opérations, et avec le même élément neutre $1_A = 1_B$ [2]. On vérifie facilement que :

Proposition 52. *B est un sous-anneau de A si et seulement si*
$\forall (x, y) \in B^2, \qquad x + y \in B,\ xy \in B.$

2. Si A n'est pas l'anneau nul, $\{0_A\}$ n'est donc pas un sous-anneau de A.

$$\forall x \in B, \qquad -x \in B.$$
$$1_A \in B.$$

L'intersection d'une famille non vide $(B_i)_{i\in I}$ de sous-anneaux de A est un sous-anneau de A, ce qui permet de donner la définition :

Définition 24. Si A est un anneau et X un sous-ensemble non vide de A, le sous-anneau de A engendré par X est l'intersection des sous-anneaux de A qui le contiennent. C'est aussi le plus petit anneau de A qui contient X.

Par exemple, si A est l'anneau des fonctions définies sur $\mathbb{R}$ à valeurs dans $\mathbb{R}$, le sous-anneau des fonctions polynômes est le sous-anneau engendré par la fonction $x \mapsto x$, le sous-anneau des polynômes trigonométriques est le sous-anneau engendré par les fonctions $x \mapsto \sin x$ et $x \mapsto \cos x$. De même, $\mathbb{D}$ est un sous-anneaux de $\mathbb{Q}$.

1.4 Morphismes

Comme on définit des applications linéaires, on peut définir des applications entre anneaux qui préservent les opérations.

Définition 25. Soit A et B deux anneaux. Un **morphisme d'anneaux** est une application $f : A \to B$ telle que, pour tout (a, b) de A^2 :

$$f(a+b) = f(a) + f(b), \qquad f(ab) = f(a)f(b), \qquad f(1_A) = 1_B$$

On vérifie facilement qu'on a également : $f(0_A) = 0_B$ en calculant $f(0_A + 0_A)$. Un exemple de morphisme de $\mathbb{C}[X]$ dans lui-même : $P(X) \mapsto P(X+a)$. Par contre $P(X) \mapsto P(X)^2$ ne définit pas un morphisme d'anneaux. Remarquons qu'on ne peut déduire $f(1_A) = 1_B$ de $f(ab) = f(a)f(b)$.

Proposition 53. *Soit f un morphisme d'anneaux de A dans B. Alors :*

- *Si C est un sous-anneau de A, $f(C)$ est un sous-anneau de B.*
- *Si D est un sous-anneau **non nul** de B, $f^{-1}(D)$ est un sous-anneau de A.*

Deux cas particuliers, avec les mêmes notations :

Définition 26. Le noyau d'un morphisme est $\mathrm{Ker}(f) = f^{-1}(0)$; son image est $\mathrm{Im}(f) = f(A)$.

L'image est un sous-anneau mais pas le noyau en général (exception avec l'anneau nul). De plus :

Proposition 54. *Un morphisme d'anneaux f de A vers B est injectif si et seulement si* $\mathrm{Ker}\, f$ *est réduit à $\{0\}$. Il est surjectif si et seulement si* $\mathrm{Im}\, f = B$.

1.5 Idéaux

Il se trouve que la notion de sous-anneau n'est pas la plus riche ni la plus intéressante : en particulier, elle ne permet pas de définir des quotients car la relation d'équivalence $a \equiv b \iff a-b \in B$ n'est en général pas compatible avec le produit lorsque B est seulement un sous-anneau de A. Pour définir des quotients, il faut utiliser des **idéaux** (dans le cas non commutatif, il faudra des **idéaux bilatères**).

Définition 27. Si A est un anneau commutatif, un sous-ensemble non vide I s'appelle un idéal si :
– $\forall x \in I,\ \forall y \in I, \qquad x+y \in I \ \text{ et } \ -x \in I$
– $\forall a \in A,\ \forall x \in I, \qquad ax \in I$

Notons que $\{0_A\}$ et A lui-même sont des idéaux. On les appelle parfois **idéaux triviaux**, les autres sont des idéaux propres. Un exemple particulièrement intéressant est donné par la définition :

Définition 28. Soit $a \in A$. On appelle **idéal principal** engendré par a l'ensemble des multiples de a. Il est noté aA, ou plus rapidement (a).

Pour que cette définition soit acceptable, il faut vérifier que c'est un idéal, ce qui est immédiat. Nous connaissons les idéaux de $\mathbb{Z}$ et de $K[X]$, ils sont tous principaux. Donnons un exemple dans $K[X,Y]$: l'ensemble des polynômes sans terme constant est un idéal propre de $K[X,Y]$.

Remarque 5. Un idéal est forcément un sous-groupe pour l'addition. En ce qui concerne la multiplication, la contrainte est différente que pour un sous-anneau, mais on ne demande pas que 1_A soit dans l'idéal.

Par contre :

Proposition 55. *Si un idéal de A contient une unite (=un inversible) alors cet idéal est A tout entier.*

Démonstration. Si A contient u inversible d'inverse u^{-1}, il contient $u^{-1}u = 1_A$ par la seconde propriété, donc $a = a1_A$ où a est quelconque, toujours par la seconde propriété. ■

Pour prolonger la fin de la remarque :

Proposition 56. *Un anneau $A \neq \{0\}$ est un corps si et seulement si il ne contient aucun idéal que les idéaux triviaux.*

Démonstration. Si A est un corps, tout idéal non nul contient un inversible, donc coïncide avec A. Réciproquement, soit a un élément non nul de A. Alors $Aa = (a)$ est un idéal non nul donc coïncidant avec A. Comme A contient 1_A, il existe a' tel que $a'a = 1_A$, a admet un inverse. ■

Les idéaux ont aussi des propriétés vis-à-vis des morphismes :

Théorème 57. *Soit $f : A \to B$ un morphisme d'anneaux commutatifs. Alors,*
– *Si $I \subset A$ est un idéal de A, alors $f(I)$ est un idéal* ***de l'anneau*** *$f(A)$.*
– *Si $J \subset B$ est un idéal de B, alors $f^{-1}(J)$ est un idéal de A.*
– *En particulier, le noyau d'un morphisme d'anneaux est toujours un idéal.*

Démonstration. Attention à la différence entre les deux cas, image directe et image réciproque. Regardons le premier cas : si j et j' sont dans $f(I)$, b dans $f(A)$, alors il existe i et i' dans I et a dans A tels que :

$$j = f(i),\ j' = f(i'),\ b = f(a)$$

Comme f est un morphisme et $\mathcal{I}$ un idéal, on a :

$$j - j' = f(i - i') \in f(I),\ bj = f(ai) \in f(I)$$

Remarquer que l'image de I n'est pas forcément un idéal de B. La suite de la démonstration est immédiate. Enfin, le dernier point découle de ce que $\{0\}$ est un idéal. ■

1.6 Anneaux quotients

Dans ce paragraphe, nous allons généraliser dans un anneau quelconque la construction faite pour l'anneau $\mathbb{Z}/n\mathbb{Z}$ ou dans les quotients de $K[X]$. À tout idéal on peut associer une relation $\equiv$ définie par :

$$x \equiv y \iff x - y \in \mathcal{I}$$

Proposition 58. *$\equiv$ est une relation d'équivalence, compatible avec les opérations.*

Démonstration.

1. $0 \in \mathcal{I}$, d'où la réflexivité. Si on suppose $x \equiv y$, alors $x - y \in \mathcal{I}$ donc $-(x - y) \in \mathcal{I}$ et $y \equiv x$, la relation est symétrique. Enfin,

$$\left.\begin{array}{l} x \equiv y \\ y \equiv z \end{array}\right\} \Rightarrow \left\{\begin{array}{l} x - y \in \mathcal{I} \\ y - z \in \mathcal{I} \end{array}\right\} \Rightarrow (x - y) + (y - z) \in \mathcal{I}$$

   et $x \equiv z$, la relation est transitive.

2. Si $x \equiv x'$ alors $xy \equiv x'y$ et si $y \equiv y'$ alors $x'y \equiv x'y'$. Et donc

$$x \equiv x' \text{ et } y \equiv y' \Rightarrow xy \equiv x'y \equiv x'y'$$

   On vérifie de même que :

$$x \equiv x' \text{ et } y \equiv y' \Rightarrow x + y \equiv x' + y'$$

■

Il est alors possible de considérer l'ensemble des classes d'équivalence, c'est ce qu'on appelle l'**anneau quotient**, noté $A/\mathcal{I}$, et de le munir d'une structure d'anneau :

Théorème 59. – *Les classes d'équivalence sont de la forme $a + \mathcal{I}$, abrégé en $\overline{a}$ s'il n'y a pas d'ambiguïté.*
– *Si on pose $\overline{a} + \overline{b} = \overline{a + b}$ et $\overline{a}\,\overline{b} = \overline{ab}$, ces opérations sont bien définies.*
– *$A/\mathcal{I}$ est alors un anneau d'éléments neutres $\overline{0}$ et $\overline{1}$.*
– *L'application $\pi : A \to A/\mathcal{I}$ définie par $a \mapsto \overline{a}$ est appelée **projection**. C'est un morphisme surjectif dont le noyau est $\mathcal{I}$.*

Démonstration.
– Si $b \equiv a$ alors il existe $i \in \mathcal{I}$ tel que $b - a = i$ d'où $b \in a + \mathcal{I}$, et réciproquement.

– La proposition précédente montre que :

$$\overline{a} = \overline{a'} \text{ et } \overline{b} = \overline{b'} \Rightarrow \overline{a+b} = \overline{a'+b'}$$

ce qui montre bien la cohérence de la définition de la somme de deux classes. Il en va de même pour la définition du produit.
– C'est une simple écriture : les propriétés d'associativité, de distributivité, etc. de l'anneau A sont transmises au quotient.
– La surjectivité découle de la définition du quotient. De plus, l'image réciproque de $\overline{0}$ est l'ensemble des a tels que $a \equiv 0$, c'est $\mathcal{I}$.

■

Noua allons terminer cette étude des anneaux quotients par deux théorèmes importants.

Théorème 60. ***Théorème d'isomorphisme.*** *Si $f : A \to B$ est un morphisme d'anneau, alors :*

$$A/\operatorname{Ker}(f) \simeq \operatorname{Im}(f)$$

($\simeq$ désigne un isomorphisme d'anneaux).

Démonstration. Décrivons cet isomorphisme, noté $\overline{f}$: on pose $\overline{f}(\overline{a}) = f(a)$. Il faut vérifier que cela de dépend pas du représentant choisi pour la classe de a :

$$\overline{a} = \overline{b} \Rightarrow a - b \in \operatorname{Ker}(f) \Rightarrow f(a-b) = 0 \Rightarrow f(a) = f(b)$$

$$\overline{f}(\overline{a+b}) = f(a+b) = f(a) + f(b) = \overline{f}(\overline{a}) + \overline{f}(\overline{b})$$

idem pour le produit et pour l'image de $1_{A/\operatorname{Ker} f}$: c'est bien un morphisme d'anneaux. Il est surjectif par choix de l'ensemble d'arrivée, et injectif car son noyau est l'ensemble des $\overline{a}$ pour tous les $a \in \operatorname{Ker} f$, c'est donc $\{\overline{0}\}$. ■

Voici une application :

Soit $\phi : \mathbb{R}[X] \to \mathbb{C}$ défini par $P \mapsto P(i)$. On voit facilement que ϕ est un morphisme. Son noyau est constitué des polynômes à coefficients réels dont i est racine : ce sont les multiples de X^2+1 (car si i est racine, -1 aussi). Le morphisme ϕ est surjectif (prendre les polynômes de degré inférieur à 1) et donc

$$\mathbb{R}[X]/(X^2+1) \simeq \mathbb{C}$$

(on peut aussi comprendre que le quotient est une « définition » de $\mathbb{C}$, c'est ce qu'a fait Cauchy en 1847).

Le second, théorème de correspondance permet de décrire les idéaux d'un quotient.

Théorème 61. ***Théorème de correspondance.*** *Soit A/I un anneau quotient, où I est un idéal de A. Si on note p la projection, les idéaux de A/I sont les $p(J)$, J décrivant l'ensemble des idéaux de A contenant I.*

À titre d'exemple, on peut décrire les idéaux de $\mathbb{Z}/12\mathbb{Z}$ ils sont en bijection avec les idéaux engendrés par les diviseurs de 12. Commençons par un lemme :

Lemme 62. *Soit p un application surjective de E dans F et soit K un sous-ensemble de F. Alors $p(p^{-1}(K)) = K$.*

dém. du lemme. Soit $y \in p^{-1}(K)$. Alors $p(y) \in K$ donc $p(p^{-1}(K)) \subset K$. Pour l'autre inclusion, on a besoin de la surjectivité. Soit $k \in K$. Alors, par surjectivité, il existe $y \in E$ tel que ■

dém. du théorème. Les $p(J)$ sont des idéaux, car p est un morphisme surjectif. Si maintenant K est un idéal de l'anneau quotient, alors $p^{-1}(K)$ est un idéal de A ; il contient I car K contient $\overline{0}$. De plus, comme p est surjective, $K = p(p^{-1}(K)$ (lemme facile). Enfin, si J est un idéal de A contenant I, on a $p^{-1}(p(J)) = J$: si $a \in p^{-1}(p(J))$, alors $p(a) \in p(J)$, donc il existe $j \in J$ tel que $a \equiv j$, soit $a - j \in I$, mais on en déduit que a est somme de deux éléments de J puisque J contient I. On a donc $p^{-1}(p(J)) \subset J$; l'autre inclusion est immédiate : si $j \in J$, alors j est un antécédent de $p(j)$ donc appartient à $p^{-1}(p(J)$. En définitive, la correspondance décrite est bijective. ■

Donnons un exemple d'application : les idéaux de $\mathbb{Z}/12\mathbb{Z}$ sont au nombre de six, dont quatre sont non triviaux.

2 Opérations sur les idéaux - Anneaux produits - théorème chinois

2.1 Opérations sur les idéaux

Un peu comme les sous-espaces vectoriels, on peut « combiner » les anneaux. Soit A un anneau commutatif.

Définition 29. – Si I et J sont des idéaux, $I \cup J$ et $I + J$ (ensemble des sommes d'un élément de I et d'un élément de J) sont des idéaux. De plus $I + J$ est le plus petit idéal qui contient à la fois I et J.
– Si I et J sont des idéaux, on note IJ l'ensemble des sommes de produits de la forme ij où $i \in I$ et $j \in I$.

Les démonstrations sous-entendues dans ces énoncés sont immédiates. Attention cependant à la définition du produit de deux idéaux. On pourra également remarquer que IJ est inclus dans $I \cap J$.

2.2 Produit d'anneaux

Pour énoncer le célèbre théorème chinois, nous allons avoir également besoin de la notion de produit d'anneaux.

Définition 30. Si A et B sont deux anneaux, on appelle **anneau produit** le produit cartésien $A \times B$ muni des opérations :

$$(a, b) + (a', b') = (a + a', b + b') \qquad \text{et} \qquad (a, b)(a', b') = (aa', bb')$$

Il faut bien sûr vérifier que c'est un anneau. Cela n'offre pas de difficulté, et on peut définir de même le produit d'une famille d'anneaux. Attention, le produit de deux corps n'est pas un corps : chercher les inversibles du produit $\mathbb{R} \times \mathbb{R}$. Plus généralement, le produit de deux anneaux intègres n'est pas intègre. Dans le même ordre d'idées, $A \times \{0_B\}$ est un idéal de $A \times B$, a une

structure d'anneau (isomorphe à A), mais n'est pas un sous-anneau de $A \times B$, car il n'a pas le même élément neutre pour le produit.

2.3 Le théorème chinois

On se place dans un anneau, et on considère deux idéaux I et J qui ont la propriété suivante :

$$I + J = A$$

Définition 31. Deux idéaux qui vérifient $I + J = A$ sont dits **étrangers**.

Théorème 63. ***Théorème chinois.*** *Soit A un anneau, I et J deux idéaux étrangers. On a alors $IJ = I \cap J$ et il existe un isomorphisme d'anneaux*

$$A/IJ \simeq A/I \times A/J$$

Démonstration. Pour le premier point : on sait déjà que $IJ \subset I \cap J$. Réciproquement, prenons e dans $I \cap J$ et $i + j = 1_A$ (en utilisant $I + J = A$) : on a donc $e = ei + ej$, et, puisque $e \in J$ et $i \in I$, et $e \in I$ et $j \in J$, on a bien $e \in IJ$.

Passons au second point : on part de l'application $a \mapsto (a+I, a+J)$ de A dans $A/I \times A/J$. C'est un morphisme d'anneaux puisque les « projections » le sont. Son noyau est formé des éléments de A qui se projettent en $(\overline{0}, \overline{0})$, c'est-à-dire qui sont dans I et dans J. C'est donc l'idéal $I \cap J = IJ$. Reste à montrer la surjectivité. Soit $(\alpha + I, \beta + J)$, on cherche un élément a de A tel que a vérifie

$$\begin{cases} a \equiv \alpha \pmod{I} \\ a \equiv \beta \pmod{J} \end{cases}$$

Prenons comme ci-dessus : $1_A = i + j$. On en déduit $j \equiv 1_A \pmod{I}$ et $i \equiv 1_A \pmod{J}$ il suffit alors de combiner pour obtenir $a = x\beta + y\alpha$ qui est bien solution du problème. ■

Le théorème chinois revient donc à résoudre un système de congruences simultanées, c'est effectivement ce qu'on trouve dans les mathématiques chinoises [3]. Dans le cas particulier de $\mathbb{Z}$, les idéaux étrangers sont les idéaux principaux engendrés par des nombres premiers entre eux, et le théorème chinois s'écrit :

Théorème 64. *Si $m \wedge n = 1$, alors*

$$\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

En itérant le processus, on voit donc que les $\mathbb{Z}/p^k\mathbb{Z}$ sont les "briques" de base qui permettent de construire tous les $\mathbb{Z}/n\mathbb{Z}$.

Le théorème chinois se généralise à plus de deux idéaux, mais, attention, il faut que les idéaux soit étrangers deux à deux : il ne suffit pas que la somme de tous les idéaux soit A.

3. Dans la version initiale, il s'agissait de trouver les nombres congrus à 2 modulo 3, congrus à 3 modulo 5 et à 2 modulo 7. Ce sont les nombres de la forme $23 + 105k$.

3 Divisibilité dans les anneaux intègres. Anneaux euclidiens, principaux et factoriels

3.1 Vocabulaire

On préfère à partir de maintenant se limiter à un **anneau commutatif intègre** A : certaines notions pourront être définies dans des anneaux plus généraux, mais elles ont moins d'intérêt et des propriétés différentes. Signalons un moyen intéressant de fabriquer des anneaux intègres : on choit un nombre complexe α et un considère les morphismes

$$\phi : \mathbb{Z}[X] \to \mathbb{C}$$

définis par $P \mapsto P(\alpha)$. L'image d'un tel morphisme est un sous-anneau de $\mathbb{C}$, donc un anneau intègre. Il est noté $\mathbb{Z}[\alpha]$. Ainsi, $\mathbb{Z}[i]$ s'appelle l'anneau des entiers de Gauss. On peut parfois remplacer $\mathbb{Z}$ par $\mathbb{Q}$ ou $\mathbb{R}$.

Définition 32. – Les éléments inversibles seront appelés unités.
- Si a et b sont dans A, $a|b$ s'il existe $c \in A$ tel que $b = ac$. Cette notion dépend de l'anneau, par exemple 2 divise $X - 1$ dans $\mathbb{R}[X]$ mais pas dans $\mathbb{Z}[X]$.
- On dit que a et b sont **associés** s'il existe une unité u telle que $a = bu$. Cette relation est une relation d'équivalence.
- Une proposition : $a \mid b$ et $b \mid a$ si et seulement si a et b sont associés et si et seulement si $(a) = (b)$. La démonstration utilise l'intégrité.
- On dit que deux éléments a et b de A sont premiers entre eux s'ils ont pour seuls diviseurs communs les unités.
- On dit que $a \in A \setminus (A^\times \cup \{0\})$ est **irréductible** si :

$$\forall (b, c) \in A^2, \qquad (a = bc) \Rightarrow \big(b \in A^\times \text{ ou } c \in A^\times\big)$$

Une affirmation à vérifier dans cette définition : si $a \mid b$ et $b \mid a$, alors a et b sont associés. En effet, il existe alors c et c' tels que $b = ca$ et $a = bc'$. On en déduit $a = acc'$. Si a est nul, b aussi, et a et b sont associés, sinon, par intégrité, $cc' = 1$ et a et b sont associés. Dans $\mathbb{Z}$ les irréductibles sont les nombres premiers (et leurs opposés).

On peut définir un ppcm et un pgcd de deux nombres : m est un ppcm de a et b si $(a) \cup (b) = (m)$. Mais attention, il n'existe pas toujours.... De même, on dira que d est un pgcd de a et b si $\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(d)$. Attention, encore une fois il n'existe pas toujours.

3.2 Idéaux premiers et idéaux maximaux

Dans ce paragraphe nous allons donner des définition et des théorèmes qui restent vrais pour des anneaux commutatifs non intègres. Mais nous les appliquerons le plus souvent à des anneaux intègres.

Définition 33. On dit qu'un idéal I de l'anneau A est premier si le quotient A/I est intègre.

Proposition 65. *I est premier s'il a la propriété suivante :*

$$\forall (a, b) \in A^2, \quad \textit{si } ab \in I, \quad \textit{alors } a \in I \textit{ ou } b \in I$$

La démonstration est une simple traduction... Remarquons qu'un anneau intègre est un anneau pour lequel (0) est un idéal premier.

Définition 34. On dit qu'un idéal I de l'anneau A est maximal si le quotient A/I est un corps.

Théorème 66. *Un idéal I de l'anneau A est maximal si et seulement si il est maximal, au sens de l'inclusion, dans l'ensemble des idéaux stricts de A.*

C'est une application immédiate du théorème de correspondance et de la recherche des idéaux d'un corps. Signalons également que A est un corps si et seulement si (0) est un idéal maximal de A. De même il est immédiat, puisqu'un corps est toujours intègre, que

Théorème 67. *Tout idéal maximal est premier.*

Démonstration. A/I corps implique A/I intègre. ■ Dans $\mathbb{Z}$, comme dans $K[X]$, les idéaux premiers et maximaux sont les idéaux principaux engendrés par les irréductibles... Mais ce n'est pas si simple pour les anneaux commutatifs quelconques.

Exercice 3. Si ϕ est un morphisme d'anneau, montrer que l'image réciproque d'un idéal premier est premier, mais que l'image réciproque d'un idéal maximal n'est pas toujours un idéal maximal.

On peut démontrer, mais ce n'est pas un théorème facile, qu'un anneau admet toujours des idéaux maximaux, et même qu'un idéal strict est toujours contenu dans un idéal maximal (th. de Krull).

Nous allons maintenant décrire les anneaux qui généralisent les propriétés de $\mathbb{Z}$. Il y a trois notions, et nous nous plaçons dans le cadre des anneaux **intègres**.

3.3 Définitions

Définition 35. Un anneau A **euclidien** est un anneau intègre tel qu'il existe $\phi : A \setminus \{0\} \to \mathbb{N}$ telle que :

$$\begin{array}{ll} (1) & b \mid a \Rightarrow \phi(b) \leqslant \phi(a) \\ (2) & \forall a \in A,\ \forall b \in A \setminus \{0\},\ \exists q, r \in A \\ & \left\{ \begin{array}{lcl} a & = & bq + r \\ r & = & 0 \ \text{ ou } \ \phi(r) < \phi(b) \end{array} \right. \end{array}$$

Remarque 6. L'application ϕ porte le nom de (du mot grec signifiant mesure) : on prend la valeur absolue pour $\mathbb{Z}$, le degré pour $K[X]$. Notons que la définition de la division euclidienne ne demande pas forcément l'unicité du couple (q, r) (que l'on appelle **quotient** et **reste**).

Il existe d'autres anneaux euclidiens : on montrer par exemple que l'anneau des entiers de Gauss (noté $\mathbb{Z}[i]$), formé des complexes dont les parties réelle et imaginaire sont des entiers, est euclidien pour le stathme $|z|^2$.

On continue :

Définition 36. Un anneau A, commutatif intègre, est dit **principal** si tout idéal de A est principal.

Les corps sont principaux : ils n'ont que deux idéaux, qui sont principaux. mais ce ne sont pas des anneaux principaux « intéressants ».

Dernière définition :

Définition 37. Un anneau A commutatif intègre est **factoriel** si tout élément de A, non nul et non inversible, s'écrit de façon unique comme produit d'irréductibles.

Bien sûr, nos deux anneaux favoris $\mathbb{Z}$ et $K[X]$ sont à la fois euclidiens, principaux et factoriels. Les trois définitions sont liées par le théorème suivant :

Théorème 68. *Tout anneau euclidien est principal. Tout anneau principal est factoriel.*

Démonstration. Nous ne démontrerons pas la première affirmation : la démonstration est en tout point semblable à celle que nous avons fait deux fois. $\mathcal{I}$ un idéal, différent de l'idéal nul, et x_0 un élément non nul de $\mathcal{I}$ de stathme minimal (ne pas oublier que les stathmes sont à valeurs entières). Si maintenant x est un élément quelconque de $\mathcal{I}$, on peut écrire $x = x_0q + r$ avec $r = 0$ ou $\phi(r) < \phi(x_0)$; comme $r = x - x_0q \in \mathcal{I}$, et le choix de x_0 impose que $r = 0$. En définitive $x = x_0q$ et $\mathcal{I} = (x_0)$.

La démonstration de la seconde implication est plus délicate, elle n'est pas au programme..

Faisons un raisonnement par l'absurde : soit $\mathcal{E}$ l'ensemble des éléments x de A, non nuls ni inversibles, qui ne se décomposent pas en irréductibles, et supposons que $\mathcal{E}$ soit non vide. Alors, $\mathfrak{F} = \{(x) \mid x \in \mathcal{E}\}$ est un ensemble non vide. Montrons que cet ensemble, muni de la relation d'inclusion, admet (au moins un) élément maximal. En effet, (nouveau raisonnement par l'absurde), si ce n'était pas vrai, on pourrait construire une chaîne infinie :

$$(x_1) \subsetneq (x_2) \subsetneq \ldots \subsetneq (x_n) \subsetneq \ldots$$

où les x_i sont dans $\mathcal{E}$. Alors l'ensemble $U = \bigcup_{n\geqslant 1}(x_n)$ est un idéal : si a et b sont dans U, il existe un certain n tel que a et b soient tous les deux dans (x_n), donc $a + b \in (x_n) \subset U$, même raisonnement pour l'autre propriété. U est donc principal, c'est-à-dire qu'il existe $x \in A$ tel que $U = \bigcup_{n\geqslant 1}(x_n) = (x)$.
Mais alors, x est dans $\bigcup_{n\geqslant 1}(x_n)$, donc $x \in (x_{n_0})$ pour un n_0, et donc alors $(x) = (x_{n_0})$ et $\bigcup_{n\geqslant 1}(x_n) = (x_{n_0})$, ce qui est absurde au vu des hypothèses.
Soit donc (x_0) maximal dans $\mathfrak{F}$. Alors x_0 n'est pas inversible, ni irréductible (sinon il se décomposerait en produit d'irréductibles) dont il peut s'écrire $x_0 = ab$ et donc $(x_0) \subset (a)$, $(x_0) \subset (b)$. Les inclusions sont strictes puisque ni a ni b ne sont associés à x_0. Par maximalité, a et b ne sont pas dans $\mathcal{E}$, donc se décomposent en irréductibles, mais alors x_0 aussi se décompose en irréductibles, il y a contradiction.
Il faut maintenant montrer l'unicité. Commençons par remarquer que si p est irréductible et si u est une unité, alors pu est irréductible. Supposons maintenant que :

$$p_1p_2 \ldots p_s = q_1q_2 \ldots q_r$$

Notre objectif est de montrer que $r = s$ et que les p_i sont égaux, à l'ordre et à des unités près aux q_j. Pour cela nous allons utiliser le théorème qui dit que dans un anneau principal, tout irréductible est premier (voir la démonstration plus bas). On peut alors en effet dire que q_1 divisant le produit $p_1 \ldots p_s$, divise un des p_i, et, par irréductibilité des p_i, on peut écrire que $q_1 = p_iu$ où u est une unité. On peut alors simplifier et reprendre le même raisonnement. À la fin, on aura $r = s$ car un irréductible n'est pas un produit d'unités. ■

Il n'est pas facile de trouver un anneau principal qui n'est pas euclidien ; le plus simple (!) est $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$. Par contre, observons que $K[X,Y]$ est factoriel (voir plus loin) mais qu'il n'est pas principal : l'idéal engendré par X et Y est $(X)+(Y)$, il n'est pas principal (raisonnement par l'absurde facile).

3.4 Propriétés des anneaux factoriels

Les propriétés qui sont vraies pour les anneaux factoriels sont données dans la liste suivante :

Théorème 69. *Dans un anneau factoriel*

1. *Les notions d'élément irréductible et d'élément premier sont identiques.*
2. *La notion d'éléments premiers entre eux reste possible et on dispose du théorème de Gauss.*
3. *Dans un anneau factoriel, tout couple (a,b) admet un pgcd et un ppcm.*

Démonstration.

1. On sait déjà que tout premier est un irréductible ; soit A un anneau factoriel et $a \in A$ un élément irréductible. Supposons que $a \mid bc$; cela signifie que dans la décomposition en irréductibles de bc, il y a l'irréductible a (à une unité près) et donc que la décomposition en irréductibles de b ou de c contient a, et donc a divise b ou c. C'est ce qu'on appelle parfois le lemme d'Euclide.
2. Même idée, on suppose que a divise bc et que a et b sont premiers entre eux, et on regarde la décomposition en irréductibles de $bc = ak$.
3. On compare les décompositions en irréductibles de a et de b pour exhiber un pgcd et un ppcm de (a,b). Remarquons qu'on a toujours $ab = ppcm(a,b)pgcd(a,b)$ aux unités près.

■

Enfin le théorème suivant permet de construire des anneaux factoriels :

Théorème 70. *Si A est factoriel, alors $A[X]$ est factoriel.*

La démonstration est un peu délicate, elle est admise.

3.5 Propriétés des anneaux principaux

Donnons maintenant les propriétés des anneaux principaux :

Théorème 71. *Dans un anneau principal*

1. *Les notions d'idéal premier et d'idéal maximal coïncident.*
2. *a et b sont premiers entre eux si et seulement si $(a)+(b) = A$. (les idéaux sont étrangers). C'est le théorème de Bezout.*
3. *Le pgcd d et le ppcm m peuvent être définis par :*

$$(a)+(b) = (d),\ (a)\cap(b) = (m)$$

Démonstration.

1. Si I est maximal, il est premier, c'est toujours vrai. Si I est premier, il est principal, donc de la forme (p) où p est premier. Si J est un idéal tel que $I \subsetneq J \subset A$, alors J est de la forme $J = (q)$. Mais la première inclusion prouve que q divise p, sans lui être associé. Comme p est irréductible, donc premier, q est une unité, $J = A$ et I est maximal.
2. C'est la démonstration habituelle.
3. Idem

■

Il est intéressant de noter que ces énoncés peuvent être mis en défaut lorsque l'anneau A est factoriel sans être principal.

Enfin, ce qui différentie les anneaux euclidiens des anneaux principaux, c'est que la division euclidienne permet d'avoir un algorithme qui décide si deux éléments sont premiers entre eux, et avoir une solution de l'équation de Bezout.

Certaines des propriétés des anneaux factoriels peuvent être démontrée de façon différente dans les anneaux principaux : par exemple le théorème de Gauss...

Démonstration. (théorème de Gauss dans un anneau principal) Soit A un anneau principal, et p irréductible. Supposons que $p \mid ab$ et soit $\mathcal{I}$ l'idéal engendré par p et a. On peut écrire :

$$\mathcal{I} = \{z \in A \mid \exists x \in A, \exists y \in A,\ z = xp + ya\}$$

Comme l'anneau est principal, $\mathcal{I}$ est principal, et il existe d tel que $\mathcal{I} = dA$. Donc p et a qui sont dans $\mathcal{I}$ sont des multiples de d. Comme p est irréductible, d est soit une unité, soit un associé de p. Si c'est un associé de p, p divise a et c'est terminé ; si c'est une unité, alors $\mathcal{I} = A$ et $1 = xp + ya$ pour un x et un y de A. En multipliant par b on voit que p divise b. Remarquer la ressemblance de la démonstration avec celle du lemme de Gauss dans $\mathbb{Z}$. ■

4 Corps

4.1 Caractéristique d'un anneau, d'un corps

Puisque 1_A est un élément de l'anneau A, celui-ci contient aussi $1_A + 1_A$, $1_A + 1_A + 1_A$, ..., et leurs opposés. Ces éléments sont notés 2.1_A, 3.1_A ou par abus 2, 3,..., mais ils ne sont pas forcément distincts. Plus précisément :

Définition 38. Si A est un anneau, l'application $k \mapsto k.1_A$ de $\mathbb{Z}$ dans A est un morphisme d'anneaux. Son noyau est de la forme $n\mathbb{Z}$ et n s'appelle la **caractéristique** de A.

L'application est un morphisme,

$$k.1_A + k'.1_A = (k + k').1_A \qquad \text{et} \qquad (k.1_A)(k'.1_A) = (kk').1_A$$

et ce morphisme est rarement surjectif (quand l'est-il ?). On peut démontrer les propriétés suivantes :

Proposition 72. *Soit A un anneau de caractéristique n. Alors,*
(i) si $n = 0$, alors A est infini,
(ii) si A est intègre alors $n = 0$ ou $n = p$ nombre premier.

(iii) Si A est commutatif et $n = p$ premier, alors :

$$\begin{array}{rccc} f: & A & \longrightarrow & A \\ & a & \longmapsto & a^p \end{array}$$

est un morphisme d'anneaux (appelé «morphisme de Frobenius»).

Démonstration.
(i) Le théorème d'isomorphisme dit que notre morphisme a une image isomorphe à $\mathbb{Z}$, qui est infini ; on dit que $\mathbb{Z}$ s'injecte dans A.
(ii) Cette fois, en raisonnant par l'absurde, on voit que si A est de caractéristique non nulle et non première, il contient un sous-anneau isomorphe à $\mathbb{Z}/n\mathbb{Z}$, qui n'est intègre que si n est premier.
(iii) On commence par le lemme :

$$0 < k < p \Rightarrow p \text{ divise } \binom{p}{k} = \frac{p(p-1)\dots(p-k+1)}{k!}$$

En effet, dans l'égalité $k!\binom{p}{k} = p(p-1)\dots(p-k+1)$, le nombre p divise le second membre, et il est premier à $k!$ lorsque $k < p$. On applique alors le lemme de Gauss.
Si maintenant on considère l'application $a \mapsto a^p$, on a

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

tandis que $(ab)^p = a^p b^p$. Remarquons que pour ces deux propriétés on utilise la commutativité de l'anneau.

■

4.2 Corps premier

Proposition 73. *La caractéristique d'un corps K est soit nulle, soit égale à p, avec p premier.*
– Si elle est nulle, K contient un corps isomorphe à $\mathbb{Q}$.
– Si elle est égale à p, K contient un corps isomorphe à $\mathbb{Z}/p\mathbb{Z}$

Ce n'est que le cas particulier de la proposition précédente appliquée

4.3 Corps des fractions

Soit A un anneau intègre. La construction des rationnels à partir des entiers peut se généraliser.

Théorème 74. *Si A est un anneau commutatif intègre, la relation*

$$(a,b) \sim (a',b') \iff ab' = a'b$$

définie sur $A \times A^*$ est une relation d'équivalence. Le quotient peut être muni d'opérations qui en font un corps.