Anneaux et corps

Christophe Antonini[1], Olivier Teytaud[2], Pierre Borgnat[3], Annie Chateau[4], and Edouard Lebeau[5]

[1]Enseignant en CPGE, Institut Stanislas, Cannes
[2]Chargé de rechercher INRIA, Université d'Orsay, Orsay
[3]Chargé de recherche CNRS, ENS Lyon, Lyon
[4]Maitre de conférence, Université Montpellier-2, Montpellier
[5]Enseignant en CPGE, Lycée Henri Poincaré, Nancy

9 juillet 2022

Anneaux et corps puis quelques applications.

1 Anneaux et corps

Les anneaux trouvent historiquement leur source dans l'école allemande, et dans l'analyse des équations algébriques (comme d'ailleurs les groupes). L'étude du théorème de Fermat a aussi grandement favorisé le développement de la théorie des anneaux. Le poids de l'histoire se sent dans la terminologie : selon les auteurs, les anneaux ont toujours un élément neutre pour la multiplication ou non. De même, la commutativité est imposée ou non selon les cas, quoique de nos jours il est rare de restreindre les anneaux au cas commutatif. Il faut noter qu'un anneau est commutatif au niveau de la loi $\times$; la loi $+$ est elle toujours additive (bien sûr, on parle ici de lois $+$ et $\times$ en supposant que l'anneau est muni de ces deux lois dans cet ordre, mais il peut bien sûr s'agir d'autres lois). Un anneau, s'il est commutatif et intègre, peut toujours être plongé dans un corps, appelé corps des fractions ; $\mathbb{Z}$ se plonge ainsi dans $\mathbb{Q}$, et les polynômes dans les fractions rationnelles.

Une première grande justification de l'intérêt des anneaux est la notion d'idéal. En particulier, les annulateurs tendent à être des idéaux ; on en verra des applications en réduction d'endomorphisme. Réciproquement, les idéaux apportent beaucoup aux anneaux, comme on le verra au niveau de la décomposition des homomorphismes (section 1.3) : par les idéaux, on décompose les homomorphismes, et étudier les homomorphismes, c'est classifier les anneaux. De même qu'on classifie les groupes et qu'on les ramène à des éléments plus simples grâce notamment aux sous-groupes distingués, on classifie les anneaux.

On verra en section 1.4 (anneau commutatif) l'intérêt de l'introduction d'un grand nombre de catégories d'anneaux : anneaux noethériens, intègres, principaux, factoriels (on peut aller lire l'introduction de 1.4 pour être convaincu rapidement de l'intérêt de toutes ces notions qui font fréquemment peur au novice).

Après quelques définitions (1.1), on verra les idéaux et les anneaux quotients (1.2), avant de décomposer les homomorphismes (1.3). On parlera alors du cas des anneaux commutatifs (1.4), avant un peu de zoologie (1.5).

Des références pour aller plus loin sont [4, **?**, **?**, 2].

1.1 Définitions

Définition 0.1 **Anneau**
Un **anneau** est un triplet $(A, +, \times)$ tel que

- A est un ensemble non vide.
- $+$ est une loi de composition interne (c'est-à-dire une application de $A \times A$ dans A), telle que $(A, +)$ est un groupe commutatif.
- $\times$ est une loi de composition interne associative, ayant un élément neutre, distributive par rapport à $+$.

On appelle **unité** de $(A, +, \times)$ tout élément inversible pour $\times$.

Si en outre $\times$ est commutative, l'anneau est dit **commutatif**.

On note 0 l'élément neutre pour l'addition, 1 l'élément neutre pour la multiplication, le symétrique de $a \in A$ pour $+$ est noté $-a$, et le symétrique, lorsque a est une unité, de a pour $\times$ est noté a^{-1}.

$a \times b$ sera souvent abrégé $a.b$ ou même ab.

a et b appartenant à A sont dits **associés** si $a = b.x$ pour un certain x unité. La relation d'association est une relation d'équivalence.

On dit que a **divise** b, ou que a est un **diviseur** de b, ou que b est un **multiple** de a, pour a et b dans A, s'il existe x tel que $b = a.x$.

On dit que a est un **plus grand commun diviseur** ou **pgcd** des éléments $a_1, ..., a_n$, si pour tout i, $d|a_i$ et si pour tout d' $\forall i$ $d'|a_i$ implique $d'|d$. On dit que a est un **plus petit commun multiple** ou **ppcm** des éléments $a_1, ..., a_n$, si pour tout i, $a_i|d$ et si pour tout d', $\forall i$ $a_i|d'$ implique $d|d'$. $a \in A$ est dit **irréductible** si a n'est pas une unité et si $b|a$ implique que b est une unité ou que b est associé à a.

Intuition Les notions de ppcm et pgcd seront surtout utilisées dans le cadre d'anneaux principaux (voir partie 1.2), bien que leur définition puisse être utilisée dans un cadre plus général.

Dans les anneaux de polynômes, il est souvent utile de savoir si un polynôme est irréductible. Dans le cas de $\mathbb{Z}[X]$ (ou $\mathbb{Q}[X]$) le critère dit d'Eisenstein est un outil possible : si p (premier) divise tous les coefficients d'un polynôme sauf le coefficient du terme dominant et si p^2 divise le coefficient du terme constant, alors le polynôme est irréductible.

PROPOSITION 0.1
Quelques propriétés des irréductibles :

•$a \in A$ est irréductible si et seulement si a n'est pas une unité et si $b.c = a$ implique que b ou c est une unité.

•Dans $\mathbb{Z}$ les éléments irréductibles sont les nombres premiers.

On a ici imposé l'existence d'un élément neutre pour la multiplication ; selon les terminologies ce n'est pas toujours le cas. Si l'on ne suppose pas l'existence d'un élément neutre pour la définition d'un anneau, alors un anneau vérifiant en outre cette propriété sera appelé anneau **unitaire**. Dans la vie de tous les jours, les anneaux sont toujours unitaires. L'hypothèse de commutativité est très classique, mais ici cette hypothèse sera précisée quand elle est nécessaire.

Exemple 0.1 Exemples •$(, +, \times)$ est un anneau.

•$(¶(E), \Delta, \cap)$ est un anneau commutatif, avec Δ la différence symétrique, c'est-à-dire $A\Delta B = A \cup B - A \cap B$.

Remarque 0.1 Étant donné un anneau A non-unitaire, on peut le plonger dans un anneau unitaire de la façon suivante :

— Soit $\tilde{A} = A \times \mathbb{Z}$.

— Définissons les deux lois suivantes dans $\tilde{A}$:

  — $(a, m) + (b, n) = (a + b, m + n)$

  — $(a, m) \times (b, n) = (a.b + m.b + n.a, mn)$

  où l'on note $m.a = a + a + a + \cdots + a$ (m fois) comme à l'accoutumée.

— $\tilde{A}$ est un anneau unitaire, et l'on peut plonger A dans $\tilde{A}$ en associant $(a, 0) \in \tilde{A}$ à $a \in A$ (notons que si A était déjà unitaire, ce plongement ne serait pas un morphisme car ne conserverait pas l'élément neutre de la multiplication).

Propriétés des anneaux (notez que na, pour $n \in \mathbb{N}$ et $a \in A$, désigne $a+a+a+\cdots+a$ (a n fois), et a^n désigne $a \times a \times a \times \cdots \times a$ (a n fois)) :

•$1 \neq 0$, à moins que le cardinal de A soit 1.

•$a.0 = 0.a = 0$ pour tout $a \in A$.

•$-(a.b) = (-a).b = a.(-b)$ pour tous $(a,b) \in A^2$

•$(na).b = n.(ab) = a.(nb)$ pour tous $(a,b) \in A^2$ et $n \in \mathbb{N}$.

•L'ensemble des unités forme un groupe pour $\times$.

PROPOSITION 0.2 **Formule du binôme de Newton**

Soit a et b dans un anneau A. Si a et b commutent, alors

$$(a+b)^n = \sum_{k \in [0,n]} C_n^k a^k b^{n-k}$$

Démonstration *Par une récurrence sans difficulté, en se rappelant que* $C_n^p = C_{n-1}^p + C_{n-1}^{p-1}$

Exemple Maple

```
> (x+y)^3;
(x+y)^3
> expand(%);
x^3+3x^2y+3xy^2+y^3
```

DÉFINITION 0.2 **Diviseurs de 0, anneaux intègres, éléments nilpotents**

1. Un élément a est dit **diviseur à gauche de** 0 s'il existe $b \neq 0$ tel que $b.a = 0$.
   Un élément a est dit **diviseur à droite de** 0 s'il existe $b \neq 0$ tel que $a.b = 0$.
   Un élément est dit **diviseur de** 0 s'il est à la fois diviseur à gauche de 0 et diviseur à droite de 0.
   Un anneau est dit **sans diviseur de** 0 s'il n'admet pas de diviseur à gauche de 0 ou de diviseur à droite de 0 autre que 0 lui-même.
2. Un anneau est dit **intègre** si :
   •il est de cardinal > 1
   •il est commutatif
   •il est sans diviseur de 0
3. Un élément a est dit **nilpotent** s'il existe $n \in \mathbb{N}$ tel que $a^n = 0$. On appelle alors **indice de nilpotence de** a le plus petit n convenable non nul.

Remarque 0.2 Remarques : •$(, +, \times)$ est un anneau intègre.

•Tout anneau comporte un diviseur de 0 à gauche, un diviseur de 0 à droite, et un diviseur de 0 tout court ; il s'agit de 0 lui-même. Un anneau sans diviseur de 0 ne signifie donc pas que l'anneau ne comporte pas de diviseur de 0.

•Un anneau est sans diviseur de 0 s'il n'admet pas de diviseur à gauche de 0 autre que 0. En effet, si A n'admettant pas de diviseur à gauche de 0 admet un diviseur à droite de 0 autre que 0, alors $0 = ab$ pour a et b non nul, ce qui contredit le fait que 0 n'ait pas de diviseur à gauche.

•De même, un anneau est sans diviseur de 0 s'il n'admet pas de diviseur à droite de 0 autre que 0.

•Un anneau est sans diviseur de 0 si $ab = 0 \Rightarrow a = 0$ ou $b = 0$.

DÉFINITION 0.3 **Morphisme d'anneaux**
Une application f d'un anneau $(A, +, \times)$ vers un anneau $(B, +, \times)$ est un **morphisme d'anneaux** (ou **homomorphisme**) si :

•f est un morphisme du groupe $(A, +)$ vers le groupe $(B, +)$

•$f(x.y) = f(x).f(y)$ pour tout $(x, y) \in A^2$

•$f(1_A) = 1_B$

On appelle alors **noyau** de f l'ensemble $ker\ f$ des $x \in A$ tels que $f(x) = 0$.

On verra que les homomorphismes ont des propriétés de « transport » des idéaux et de décomposition des idéaux, ce qui explique l'intérêt des idéaux (cf section 1.3).

Remarque 0.3 Remarques : •Le noyau d'un morphisme d'anneaux est le noyau du morphisme de groupes sous-jacent.

•0 appartient au noyau de tout morphisme d'anneaux.

•L'image de l'inverse est l'inverse de l'image, pour chacune des deux lois.

DÉFINITION 0.4 **Produit d'anneaux**
On appelle **produit de deux anneaux** leur produit cartésien muni de l'addition terme à terme et de la multiplication terme à terme.

On vérifie facilement qu'un produit d'anneaux est un anneau.

DÉFINITION 0.5 **Sous-anneau**
Étant donné $(A, +, \times)$ un anneau, une partie B de A est un **sous-anneau** de A si

•$1 \in B$

•$(B, +)$ est un sous-groupe de $(A, +)$

•B est stable par multiplication

Propriétés •Un sous-anneau est un anneau, mais un anneau inclus dans un anneau n'en est pas nécessairement un sous-anneau ; en effet il faut considérer la condition $1 \in B$.

Par exemple l'ensemble des matrices de la forme

$$\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}$$

est un anneau inclus dans l'anneau des matrices 2×2, mais n'en est pas un sous-anneau.

•L'image réciproque d'un sous-anneau par un morphisme d'anneaux est un sous-anneau.

•L'image d'un sous-anneau par un morphisme d'anneaux est un sous-anneau.

THÉORÈME 0.3
Pour tout anneau $(A, +, \times)$, il existe un unique morphisme d'anneaux de $(\mathbb{Z}, +, \times)$ dans $(A, +, \times)$. Il est défini par $\phi(n) = 1_A + ... + 1_A$ n fois et $\phi(-n) = -1_A - 1_A \cdots - 1_A$ n fois pour $n > 0$.

Démonstration *On vérifie aisément que ϕ ainsi défini est bien un morphisme d'anneau. $\phi(1)$ est nécessairement égal à 1 et $\phi(0)$ à 0. Par récurrence, les propriétés des anneaux permettent de vérifier que les autres éléments sont aussi définis de manière unique.*

Remarque 0.4 ceci montre que tout anneau contient un sous-anneau minimal qui est $\phi(\mathbb{Z})$.

1.2 Idéaux, anneaux quotients

DÉFINITION 0.6 **Idéal à gauche, idéal à droite**

On se donne $(A, +, \times)$ un anneau et I une partie non vide de A.
I est un **idéal à gauche (resp. à droite)** de $(A, +, \times)$ si
•I est stable pour l'addition
•$A.I$ est inclus dans I (resp. $I.A$ est inclus dans I)

I est un **idéal** (parfois on dit **idéal bilatère**) si I est à la fois un idéal à gauche et un idéal à droite. A et $\{0\}$ sont toujours des idéaux de A ; on les appelle **idéaux triviaux** de A. Les autres idéaux sont appelés idéaux non triviaux (on dit parfois aussi **idéaux propres**) de A.

Exemple 0.2 Exemples Dans $\mathcal{M}_n(\mathbb{R})$, l'ensemble des matrices à première colonne nulle est un idéal à gauche, l'ensemble des matrices à première ligne nulle est un idéal à droite.

Propriétés •Un idéal contenant 1 ou toute autre unité de l'anneau est l'anneau tout entier.
•La réunion d'une suite croissante d'idéaux est un idéal.
•I idéal de A et J idéal de B ; alors $I \times J$ est un idéal de $A \times B$.
•L'intersection d'une famille d'idéaux est un idéal.

PROPOSITION 0.4
Quelques propriétés des idéaux et des morphismes d'anneaux :
•Le noyau d'un morphisme est un idéal.
•L'image réciproque d'un idéal par un morphisme est un idéal.
•L'image d'un idéal par un morphisme est un idéal de l'image de l'anneau (et pas nécessairement de l'anneau dans lequel l'image est incluse...).

DÉFINITION 0.7 **idéal engendré par une partie**
Une intersection d'idéaux étant un idéal, on peut définir l'**idéal engendré par une partie** de A comme l'intersection de tous les idéaux contenant cette partie. C'est donc aussi le plus petit idéal contenant cette partie. On note (E) l'idéal engendré par E.

⚠ *Attention 0.3* En toute rigueur (E) dépend de l'anneau et la notation devrait en rendre compte. Toutefois la notation (E) est la norme.

DÉFINITION 0.8 **idéal principal**
On appelle **idéal principal** un idéal I d'un anneau commutatif engendré par un singleton $\{x\}$. On note abusivement (x) pour $(\{x\})$.

On appelle **anneau principal** un anneau intègre tel que tout idéal est principal.

Un idéal I d'un anneau commutatif est dit **idéal maximal** s'il est différent de l'anneau tout entier et si tout idéal incluant I est égal à I ou à l'anneau lui-même.

On appelle **somme** d'une famille d'idéaux $(I_k)_{k\in K}$ l'ensemble des $\sum_{i\in J} x_i$ avec J fini inclus dans K et $x_i \in I_i$.

Un idéal est dit **de type fini** s'il est somme d'un nombre fini d'idéaux principaux.

Remarque 0.5 Remarques : •Un anneau principal est donc commutatif, non réduit à $\{0\}$, sans diviseur de 0 ; et tout idéal de cet anneau est principal.

•On notera bien qu'un idéal maximal n'est pas un idéal qui est maximal... Il est en fait maximal parmi les idéaux propres.

•Dans un anneau commutatif A, $(x) = \{x.a; a \in A\}$.

•Une somme d'idéaux est un idéal.

•La somme des idéaux I_k avec $I_k = (x_k)$ est l'idéal engendré par la famille des x_k.

Un idéal de type fini est donc un idéal engendré par un nombre fini d'éléments.

PROPOSITION 0.5
Si a et b sont associés alors $(a) = (b)$.

Dans un anneau intègre il y a réciproque.

Démonstration *Facile au vu de la dernière remarque.*

⚠ *Attention 0.4* Il n'y a pas de réciproque dans le cas général !

THÉORÈME 0.6 **Théorème de Bezout**

A est supposé principal.

•Un générateur de $I = (a_1) + (a_2) + ... + (a_n)$ est un pgcd des a_i.

• d, diviseur commun des a_i, est pgcd des a_i si et seulement s'il existe une famille $(\lambda_i)_{i\in[[1,n]]}$ tels que $d = \sum \lambda_i a_i$ (**relation de Bezout**).

•Un générateur de $I = (a_1) \cap (a_2) \cap ... \cap (a_n)$ est un ppcm des a_i.

Application 0.5 On verra une application amusante avec la cryptographie (section 1.7.4).

Démonstration *Le premier • est simple : un tel générateur d doit nécessairement diviser tous les a_i, et il doit nécessairement être dans l'idéal I, et donc tout élément qui divise tous les a_i, étant lui même un générateur de I, doit diviser d.*

Le second • est une simple traduction du fait que d soit bien dans I et soit un générateur de I.

Pour le troisième •, donnons-nous p un tel générateur ; il appartient à I, et donc est un multiple de chaque a_i ; si p' est un autre multiple des a_i, alors il est dans tous les (a_i), et donc appartient à I, et donc est un multiple de p.

Dans $A = \mathbb{Z}$ ou $A = \mathbb{K}[X]$ avec $\mathbb{K}$ un corps, il est utile de disposer d'un algorithme pratique permettant de découvrir une relation de Bezout entre a et b si une telle relation existe. Pour cela, il suffit de constater que a et b ont même pgcd que a et $a - qb$, pour tout q dans A, par exemple avec q le quotient dans la division euclidienne de a par b. Si a est divisible par b, le pgcd de a et b est simplement b ; sinon, on effectue une division euclidienne. Considérons un exemple pratique, cherchons le pgcd de 42 et 30.

$$30 \not| 42$$

$$42 = 1 \times 30 + 12$$

$$12 \not| 30$$

$$30 = 2 \times 12 + 6$$

$$12|6 \text{ et } 12 = 2 \times 6$$

Donc

$$6 = 30 - 2 \times 12 = 30 - 2 \times (42 - 30) = 3 \times 30 - 2 \times 42.$$

ce qui est bien la relation de Bezout attendue. Cet algorithme est appelé **algorithme de Bezout**. On utilise ci-dessous la notion d'anneau quotient (définition 0.10) par l'idéal I, qui est en fait l'anneau quotienté par la relation d'équivalence $a\mathcal{R}_I b \iff a - b \in I$.

DÉFINITION 0.9 **premier**
Un idéal I est dit **premier** si et seulement si l'anneau quotient A/I est intègre.

Un élément non nul d'un anneau est dit **premier** si et seulement l'idéal engendré par cet élément est premier.

Application 0.6 Les nombres premiers ont un grand nombre d'applications bien sûr, dont la cryptographie (section 1.7.4), mais aussi la constructions de suites quasi-aléatoire (voir la suite de Halton, ou bien la suite de Halton-Hammersley par exemple dans [1]), la construction de corps finis (section 1.6.3).

PROPOSITION 0.7
•Un idéal I de A est premier si et seulement s'il est différent de A et si $a.b \in I$ implique $a \in I$ ou $b \in I$.

•L'image réciproque d'un idéal premier par un homomorphisme d'anneaux est un idéal premier.

La première de ces deux propriétés est fondamentale car c'est généralement celle que l'on utilise pour montrer qu'un idéal est premier.

PROPOSITION 0.8
Un anneau commutatif est intègre si et seulement si (0) est un idéal premier.

Démonstration *(0) est un idéal premier si et seulement si $a.b \in (0) \rightarrow a \in (0)$ ou $b \in (0)$, si et seulement si $a.b = 0 \rightarrow a = 0$ ou $b = 0$, si et seulement si A est intègre.*

LEMME 0.9
Soit A un anneau. A est un corps si et seulement si A est non réduit à $\{0\}$ et ses seuls idéaux sont $\{0\}$ et A.

Démonstration *Supposons que les seuls idéaux de A soient $\{0\}$ et A.*

Soit x dans A, $x \neq 0$, $x.A$ est un idéal, autre que $\{0\}$, donc il contient tout A, donc en particulier il contient 1, donc il est inversible.

Réciproquement si A est un corps, alors soit x non nul appartenant à un idéal I, alors I contient $x.A$, donc $x.x^{-1}.A$, donc A.

PROPOSITION 0.10

Dans un anneau principal, les idéaux premiers sont (0) et (p), avec p irréductible.

Démonstration *Soit I un idéal premier et $p \neq 0$ un élément de A tel que $I = (p)$. Supposons que $p = a.b$. Alors $a.b \in (p)$, et donc puisque I est premier, $a \in (p)$ ou $b \in (p)$; on suppose $a \in (p)$. Alors $a = p.a'$. On a alors $p.a'.b = p$, donc $p(1 - a'b) = 0$, or A est intègre, donc $a'.b = 1$, donc b est une unité.*

PROPOSITION 0.11
Dans un anneau principal, pour tout p irréductible, (p) est un idéal maximal.

Démonstration *Soit $I = (p)$, avec p irréductible. Supposons $I \subset J$, avec J inclus dans A. Alors $J = (q)$, et $p = q.a$. Mais p étant irréductible, soit $q = p.x$ avec x unité, soit q est une unité. Dans le premier cas, $J = I$, et dans le deuxième cas, $J = A$.*

On va maintenant étudier la notion d'anneau quotient.

Cette notion n'est étudiée que dans le cas d'anneaux commutatifs.

DÉFINITION 0.10 **anneau quotient**
Étant donné I un idéal de A, on définit une relation d'équivalence $\mathcal{R}_I$ par

$$a\mathcal{R}_I b \iff a - b \in I$$

Alors l'ensemble quotient pour cette relation, muni des opérations induites par les opérations sur I, est un anneau ; on l'appelle **anneau quotient** de A par l'idéal I, et on le note A/I.

Il convient de vérifier que la relation est bien compatible avec les opérations définies sur l'anneau (vérification aisée).

1.3 Décomposition d'un homomorphisme d'anneaux et utilisation des idéaux

Définition 0.11 **Factorisation d'un homomorphisme**
On dit que f homomorphisme d'un anneau A vers un anneau B se factorise par A/I avec I idéal de A si et seulement s'il existe g homomorphisme de A/I dans B tel que $f(x) = g(\overline{x})$.

THÉORÈME 0.12
Soit f un homomorphisme d'anneaux de A vers B. Alors pour tout I idéal inclus dans $Ker\ f$, on définit $x \mapsto \overline{x}$ la projection canonique de A sur A/I, et on a les propriétés suivantes :

•Il existe un unique homomorphisme g de A/I dans B tel que $\forall x\ f(x) = g(\overline{x})$. (factorisation par A/I)

•$Im\ f \simeq A/(Ker\ f)$.

•g est injectif si et seulement si $I = Ker\ f$.

•g est surjectif si et seulement si f est surjectif.

PROPOSITION 0.13 **(Image et image réciproque d'un idéal par un homomorphisme)**
•L'image réciproque d'un idéal par un homomorphisme est un idéal.

- **Si f est un homomorphisme surjectif**, alors l'image d'un idéal par f est un idéal.

PROPOSITION 0.14

Soit I idéal de A. Alors l'application ϕ qui à un idéal J avec $I \subset J \subset A$ associe la projection $\overline{J}$ de J sur A/I est une bijection de l'ensemble des idéaux de A contenant I vers l'ensemble des idéaux de A/I.

Démonstration *$x \mapsto \overline{x}$ étant surjectif, il est clair que ϕ associe bien un idéal à un idéal.*

Pour montrer que ϕ est bijective, on considère l'application ψ qui à un idéal K de A/I associe $\{a; \overline{a} \in K\}$.

PROPOSITION 0.15
Un idéal I d'un anneau A est maximal si et seulement si A/I est un corps.

Démonstration *On utilise le lemme 0.9 et la propriété ci-dessus.*

COROLLAIRE 0.16
Tout idéal maximal est premier.

Démonstration *Supposons que I, idéal maximal, contient $a.b$, avec $a \notin I$ et $b \notin I$.*

Alors la classe de a et la classe de b dans A/I sont non nulles, et leur produit est nul, d'où contradiction.

THÉORÈME 0.17 **Krull**
Pour tout idéal I de A, I différent de A, il existe un idéal maximal de A contenant I.

Application 0.7 Par le théorème de Krull, on peut dire que tout anneau commutatif non nul contient au moins un idéal maximal ; or, cela implique qu'il contient au moins un idéal premier. Tout anneau commutatif non nul contient donc au moins un idéal premier.

[2] signale aussi que le théorème de Krull est possiblement utilisé pour la construction des clôtures algébriques de corps commutatifs.

Démonstration *Cette preuve nécessite l'axiome du choix, via le théorème de Zorn (voir le lemme* **??***).*

•*On considère l'ensemble des idéaux différents de A contenant I idéal de A, ordonné par l'inclusion.*

•*Cet ensemble est inductif. En effet étant donnée une chaîne, on considère la réunion, c'est un idéal différent de A (en effet il ne contient pas 1 par exemple).*

•*On peut donc considérer un élément maximal pour l'inclusion, et conclure que cet idéal est maximal.*

1.4 Anneaux commutatifs

Dans la vie de tous les jours, les anneaux sont généralement supposés commutatifs. On va maintenant étudier des cas particuliers d'anneaux commutatifs, avec des cas de plus en plus riches. Tout d'abord les anneaux euclidiens, puis les anneaux noethériens, puis les anneaux intègres, puis les anneaux factoriels, puis les anneaux principaux. On a les implications (euclidien ⇒ principal) et (principal ⇒ factoriel) et (factoriel ⇒ intègre) et (principal ⇒ noethérien) ; le caractère noethérien passe au quotient ou aux anneaux de polynômes (A noethérien ⇒ $A[X]$ noethérien). On verra aussi que différents théorèmes permettent, avec quelques hypothèses techniques, de passer d'un anneau intègre noethérien à un anneau factoriel. Grosso modo, une fois que l'on obtient un anneau factoriel, on a des représentations à peu près canoniques des éléments de ces anneaux.

1.4.1 Anneaux euclidiens

Cette notion n'est ici étudiée que dans le cas d'anneaux commutatifs. Pour éclaircir les idées, précisions que l'application f citée dans la définition est typiquement le degré pour des anneaux de polynômes. Un intérêt fort des anneaux euclidiens est qu'ils sont tous principaux. Or, les anneaux principaux sont factoriels (voir plus bas).

DÉFINITION 0.12 **euclidien**
Un anneau A commutatif est dit **euclidien** pour une application f de $A \setminus \{0\}$ dans $\mathbb{N}$, si pour tout a dans A et tout b dans $A \setminus \{0\}$ il existe $(q, r) \in A^2$ tels que $a = b.q + r$ et $r = 0$ ou $f(r) < f(b)$.

Un anneau A commutatif est dit **euclidien** s'il existe une application pour laquelle il est euclidien.

PROPOSITION 0.18
Quelques exemples d'anneaux euclidiens :
- $\mathbb{Z}$ est euclidien.
- $\mathbb{K}[X]$ est euclidien.

Démonstration *Considérer respectivement :*

•$f(z) = |z|$

•$f(P) = deg(P)$ *(voir la démonstration de la division euclidienne en* **??***)*

PROPOSITION 0.19
Étant donnée f une application multiplicative (i.e. $f(a.b) = f(a).f(b)$) de $A \setminus \{0\}$ dans $\mathbb{N} \setminus \{0\}$, avec A anneau intègre, on prolonge f multiplicativement sur le corps des fractions de A en posant $f(a/b) = f(a)/f(b)$ (f est maintenant à valeurs dans $\mathbb{Q}$). Alors A est euclidien pour f si et seulement si pour tout x dans le corps des fractions il existe a dans A tel que $f(x - a) < 1$.

Démonstration *La preuve est laissée en exercice.*

PROPOSITION 0.20
Tout anneau euclidien est principal.

Démonstration *Soit A un tel anneau (commutatif, euclidien pour un certain f). Soit I un idéal de A. On se donne P_0 dans $I \setminus \{0\}$ tel que $f(P_0)$ soit minimal*[1]*. On note I' l'idéal engendré par P_0, c'est-à-dire l'ensemble des $P_0.P$ pour $P \in A$.*

Pour tout P dans I, on utilise la définition $P = P_0.Q + R$; alors $P \in I$, $P_0 \in I$, donc $P_0.Q \in I$ (par définition d'un idéal), et donc $R \in I$; or $f(R) < f(P_0)$ si R est non nul, ce qui contredit la définition de P_0. Donc R est nul, et $P \in I'$, d'où $I = I'$. Donc l'anneau est principal.

PROPOSITION 0.21
$\mathbb{Z}[i]$ et $\mathbb{Z}[\sqrt{2}]$ sont euclidiens.

Démonstration *Dans les deux cas on utilise la caractérisation de la proposition 0.19.*
Dans le premier cas on choisit $f(a + i.b) = |a + i.b|^2$ pour a et b dans $\mathbb{Q}$.
Dans le second cas on utilise $f(a + b.\sqrt{2}) = |a^2 - 2.b^2|$ si a et b dans $\mathbb{Z}$.
Ce second choix est particulièrement instructif; $f(a + b.\sqrt{d}) = |a^2 - d.b^2|$ sera souvent utile.

1.4.2 Anneaux noethériens

Comme pour beaucoup de structures algébriques, l'intérêt des anneaux noethériens apparaît lorsqu'on en a besoin : en particulier, les anneaux noethériens n'ont plus qu'à avoir une division euclidienne pour être factoriels. Or les anneaux factoriels sont très utiles, comme on le verra en section 1.4.4.

DÉFINITION 0.13 **Anneau noethérien**
Un anneau commutatif dont tout idéal est de type fini est dit **noethérien**.

PROPOSITION 0.22
Un anneau commutatif est noethérien si et seulement si toute suite croissante d'idéaux est stationnaire à partir d'un certain rang.

Démonstration *Exercice pour le lecteur.*

PROPOSITION 0.23
Un anneau commutatif A est noethérien si et seulement si tout ensemble non vide d'idéaux de A admet un élément maximal pour l'inclusion.

Démonstration *Rappelons juste qu'un élément maximal n'est pas nécessairement le plus grand élément, l'existence d'un élément maximal n'entraîne pas même celle d'un plus grand élément (voir les définitions en partie* ***??****).*

1. Un tel P_0 peut bien être exhibé car f est à valeurs dans $\mathbb{N}$, par définition.

PROPOSITION 0.24
Quelques exemples d'anneaux noethériens :
•Tout anneau quotient d'un anneau noethérien est noethérien.
•Un anneau principal est noethérien.

Démonstration *Les preuves sont comme suit :*
•*La proposition 0.14 montre qu'un idéal du quotient est la projection d'un idéal ; ce dernier étant de type fini, le projeté est de type fini.*
•*Facile, tout idéal d'un anneau principal est engendré par un seul élément, donc par un nombre fini d'éléments.*
⚠ *Attention 0.8* La propriété annoncée pour les anneaux quotients n'est pas vraie pour les sous-anneaux.

THÉORÈME 0.25 **Théorème de Hilbert**
Si A est un anneau noethérien, alors pour tout n $A[X_1, ..., X_n]$ est aussi un anneau noethérien.

Démonstration *Admis (preuve difficile).*
Intuition •Tout corps est un anneau noethérien, donc tout $K[x_1, \ldots, x_n]$ aussi.
•$\mathbb{Z}[x_1, \ldots, x_n]$ est noethérien.

1.4.3 Anneaux intègres

Les anneaux ont besoin d'être intègres pour être factoriels.
On a déjà vu les définitions, mais voici un rappel : un anneau est dit intègre si :
•il est de cardinal > 1
•il est commutatif
•il est sans diviseur de 0

DÉFINITION 0.14 **Définitions dans les anneaux intègres**
a et b dans A anneau intègre sont dits **premiers entre eux** si

$$\forall x \in A \; x|a \text{ et } x|b \to x \text{ est une unité}$$

De même les éléments d'une famille $(a_i)_{i\in[[1,n]]}$ sont dits premiers entre eux si un élément divisant tous les a_i est nécessairement une unité.

COROLLAIRE 0.26 **Théorème de Bezout**
Dans un anneau principal des éléments a_i sont premiers entre eux si et seulement s'il existe une famille λ_i d'éléments de A telle que $\sum \lambda_i a_i$ soit une unité.

PROPOSITION 0.27 **Quotientage par l'indexation**
Soit A un anneau intègre, et ϕ l'application qui à x dans A quotienté par la relation d'association $\mathcal{R}$ associe l'idéal engendré par x. ϕ est un isomorphisme d'ordre entre $A/\mathcal{R}$ muni de la divisibilité et l'ensemble des idéaux principaux de A muni de l'inverse de l'inclusion.

Démonstration

- *Tout d'abord il est clair que ϕ est bien définie, car deux éléments associés engendrent évidemment le même idéal.*
- *L'application est surjective, par définition, puisqu'on considère l'ensemble des idéaux principaux.*
- *Montrons que l'application est injective : si deux éléments a et b engendrent le même idéal alors $b = b'.a$ et $a = a'.b$ et donc $b = b'.a'.b$ et donc b' et a' sont des unités (car A est intègre), et donc $\overline{b} = \overline{a}$.*
- *Montrons qu'il s'agit d'un morphisme d'ordres :*
  - *Si $a|b$ alors $b = a.c$ donc $b.A = a.c.A \subset a.A$ et $(b) \subset (a)$ clairement.*
  - *Si $(b) \subset (a)$ alors $b = a.c$ pour un certain c et donc $a|b$.*

1.4.4 Anneaux factoriels

On l'a vu, beaucoup de notions précédentes visent à montrer le caractère factoriel d'anneaux. Nous allons voir pourquoi cette notion est si utile : dans les anneaux factoriels les éléments ont des représentations à peu près canoniques, un peu dans l'esprit des bases dans les espaces vectoriels ou dans les espaces hilbertiens.

DÉFINITION 0.15 **Anneau factoriel**

Un anneau A est dit **factoriel** si :
•il est intègre
•tout a dans A s'écrit de manière unique à association près et à permutation près $a = a'.p_1.p_2.....p_n$ avec a' unité et p_i irréductible pour tout i.

DÉFINITION 0.16 **Valuation**
Étant donné un élément p irréductible de A un anneau factoriel, on appelle **valuation p-adique de A** pour a dans A le nombre d'occurences d'un élément associé à p dans la décomposition de a sous forme $a = a'.p_1.....p_n$. On note généralement $v_p(A)$ la valuation p-adique de a.

PROPOSITION 0.28
Étant donné A un anneau factoriel, on peut choisir un élément dans chaque classe d'équivalence de A pour la relation d'association $\mathcal{R}$. L'ensemble de ces éléments permet de simplifier la décomposition de $a \in A$ en $a = a'.\prod_{i \in A/\mathcal{R}} p_i^{v_{p_i}(a)}$, le support de $i \mapsto v_{p_i}(a)$ étant fini.

Démonstration *Laissée en exercice.*
Voyons maintenant quelques propriétés intéressantes des anneaux factoriels.

PROPOSITION 0.29
Dans un anneau factoriel un élément est irréductible si et seulement s'il est premier.

Le lemme et le théorème qui suivent se démontrent très facilement, simplement en considérant les décompositions de x, y et éventuellement z pour conclure.

LEMME 0.30 **Lemme d'Euclide**
Si A est un anneau factoriel, alors si p est irréductible et divise $x.y$, alors p divise x ou p divise y.

THÉORÈME 0.31 **Théorème de Gauss**
Si z divise $x.y$ et si z est premier avec x alors z divise y.

Application 0.9 Un exemple d'application (parmi beaucoup d'autres) est le théorème **??** quant au résultant de deux polynômes.

PROPOSITION 0.32
Un anneau intègre noethérien vérifiant le lemme d'Euclide ou le théorème de Gauss est factoriel.

Démonstration *Admis.*
Dans l'exemple ci-dessous on utilise le fait que $\mathbb{Z}$ est factoriel.

Exemple Maple

> ifactor(200!);

$$(2)^{197}(3)^{97}(5)^{49}(7)^{32}(11)^{19}(13)^{16}(17)^{11}(19)^{10}(23)^{8}(29)^{6}(31)^{6}(37)^{5}$$
$$(41)^{4}(43)^{4}(47)^{4}(53)^{3}(59)^{3}(61)^{3}(67)^{2}(71)^{2}(73)^{2}(79)^{2}(83)^{2}(89)^{2}(97)^{2}$$

$$(101)(103)(107)(109)(113)(127)(131)(137)(139)(149)(151)(157)$$

$$(163)(167)(173)(179)(181)(191)(193)(197)(199)$$

1.4.5 Anneaux principaux

On rappelle tout d'abord la définition d'un anneau principal : il s'agit d'un anneau intègre dont tout idéal est principal.

On donne sans démonstration (voir [[]p156]TAU) le résultat important suivant :

PROPOSITION 0.33
Tout anneau principal est factoriel.

On peut préciser aussi que sur le corps des fractions rationnelles à coefficients dans un anneau principal, on dispose de la décomposition en éléments simples (voir le théorème **??**).

1.5 Zoologie des anneaux

On verra ici (i) la nilpotence d'une somme de nilpotents qui commutent (utile pour les endomorphismes ou matrices) et (ii) l'anneau célèbre $\mathbb{Z}/n\mathbb{Z}$ dont on a vu qu'il s'injecte dans tout anneau (théorème 0.3).

1.5.1 Nilpotence (d'une somme de deux éléments nilpotents qui commutent)

DÉFINITION 0.17 **Élément nilpotent**
Un élément a dans un anneau A est dit **nilpotent** s'il existe un entier n tel que $a^n = 0$.

PROPOSITION 0.34
La somme de deux éléments nilpotents qui commutent est nilpotente.

Démonstration *Considérer deux tels éléments a et b, et développer par le binome de Newton (Proposition 0.2) la puissance $(a+b)^n$ avec $n+1$ la somme de leurs indices de nilpotence respectifs.*

1.5.2 $\mathbb{Z}/n\mathbb{Z}$

⊡ **Généralités** Étant donné $m \in \mathbb{N}$ on note $\overline{m}$ la classe de m dans $\mathbb{Z}/n\mathbb{Z}$ (la relation d'équivalence considérée étant la congruence modulo n : x et y sont équivalents si n divise $x - y$).

PROPOSITION 0.35
On a équivalence entre les propriétés suivantes :
- m est premier avec n.
- $\overline{m}$ est générateur du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.
- $\overline{m}$ est inversible dans l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.

Démonstration *Facile, en application du Théorème de Bezout.*

DÉFINITION 0.18 **Fonction d'Euler**
On appelle **fonction d'Euler** la fonction ϕ telle que $\phi(n)$ soit le nombre d'entiers x tels que $1 \leq x \leq n$ et $x \wedge n = 1$.

PROPOSITION 0.36
Quelques cas simples de calcul de $\phi(n)$:
- Si n est premier $\phi(n) = n - 1$ et $\phi(n^r) = n^{r-1}.(n-1)$ si $r > 0$.
- $\phi(n)$ est le nombre d'éléments inversibles de $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.

Démonstration *le premier point est clair ; il suffit de voir qu'un élément est premier avec n^r si et seulement s'il n'est pas divisible par n.*

Le second point est un corollaire de la proposition précédente.

LEMME 0.37 **Lemme Chinois**
Si p et q sont premiers entre eux alors

$$(\mathbb{Z}/pq\mathbb{Z}, +) \simeq (\mathbb{Z}/p\mathbb{Z}, +) \times (\mathbb{Z}/q\mathbb{Z}, +).$$

⊡ **Lemme chinois**

Démonstration *Il s'agit des groupes additifs usuels. L'égalité des cardinaux montre qu'il suffit de trouver un morphisme de groupes injectif. Pour cela on associe à la classe de n dans $\mathbb{Z}/pq\mathbb{Z}$ la classe de n dans $\mathbb{Z}/p\mathbb{Z}$ et la classe de n dans $\mathbb{Z}/q\mathbb{Z}$. Il est clair que si deux entiers ont la même classe modulo pq alors ils ont la même classe modulo p et modulo q, donc l'application est bien définie.*

Le fait que cette application soit un morphisme est clair.

L'application est injective, car si deux entiers ont la même classe modulo p et q, alors ils ont la même classe modulo pq.

COROLLAIRE 0.38
Si $n = \prod_i p_i^{\alpha_i}$, avec les p_i premiers distincts et les $\alpha_i > 0$, alors

$$(\mathbb{Z}/n\mathbb{Z}, +, \times) \simeq \prod_i (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}, +, \times)$$

$$(\mathbb{Z}/n\mathbb{Z})^* \simeq \prod_i (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^*$$

$$\phi(n) = \prod_i \phi(p_i^{\alpha_i}) = n.\Pi_i(1 - 1/p_i)$$

Démonstration *Le premier point découle de l'utilisation récurrente du Lemme Chinois, le deuxième et le troisième sont des conséquences immédiates du premier.*

PROPOSITION 0.39
L'ensemble des automorphismes de $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^*$.

⊡ **Automorphismes de $\mathbb{Z}/n\mathbb{Z}$**

Démonstration *Il suffit de considérer l'application ψ qui à un élément inversible m associe l'automorphisme $x \mapsto m.x$;*

- *il est clair que c'est un morphisme injectif de $(\mathbb{Z}/n\mathbb{Z})^*$ dans $Aut(\mathbb{Z}/n\mathbb{Z})$.*
- *étant donné un automorphisme f de $\mathbb{Z}/n\mathbb{Z}$ on montre facilement qu'il est égal à $\psi(f(1))$.*

COROLLAIRE 0.40
$Aut(\mathbb{Z}/n\mathbb{Z})$ est un groupe abélien d'ordre $\phi(n)$.

⊡ **Forme des groupes** $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ p désigne un nombre premier.

LEMME 0.41
$(\mathbb{Z}/p\mathbb{Z})^* \simeq (\mathbb{Z}/(p-1)\mathbb{Z}, +)$.

Démonstration *$(\mathbb{Z}/p\mathbb{Z})$ est un corps fini (voir le chapitre **??** sur la théorie des groupes).*

On sait (voir Proposition 0.57) que le groupe multiplicatif d'un corps fini est cyclique, donc isomorphe à un certain $(\mathbb{Z}/n\mathbb{Z})$.

Il suffit donc de se rappeler que le cardinal de $(\mathbb{Z}/p\mathbb{Z})^*$ est $p-1$ pour conclure.

LEMME 0.42
Si $k > 0$, alors $(1+p)^{p^k} = 1 + \lambda.p^{k+1}$, avec $\lambda > 0$ et $\lambda \wedge p = 1$.

Démonstration *Par récurrence sur k :*

•$k = 1$

$(1+p)^p = \sum_{i=0}^{p} C_p^i p^i$ donc $(1+p)^p = 1 + p^2 + m.p^3 = 1 + p^2.(1 + m.p)$

•k quelconque

On écrit $(1+p)^{p^{k+1}} = ((1+p)^{p^k})^p = (1 + \lambda.p^{k+1})^p$; il suffit alors de développer en utilisant le binôme de Newton la puissance p-ième en isolant le premier et le dernier terme.

COROLLAIRE 0.43
Si $\alpha \geq 2$, $1+p$ est d'ordre $p^{\alpha-1}$ dans $\mathbb{Z}/p^\alpha\mathbb{Z}$.

Démonstration *il est d'ordre au plus $p^{\alpha-1}$ au vu du lemme précédent.*

En outre $(1+p)^{p^{\alpha-2}} = 1 + \lambda.p^{\alpha-1}$, et donc ne saurait être congru à 1 modulo p^α.

LEMME 0.44
Si m et t sont premiers entre eux, et si a et b commutent, et si a est d'ordre m et b est d'ordre t, alors $a.b$ est d'ordre $m.t$.

Démonstration *•Il est facile de voir que ab est d'ordre au plus $m.t$, puisque a et b commutent.*

•Réciproquement, si $(ab)^n = 1$, alors $a^{n.t}.b^{n.t} = 1$, donc $a^{n.t} = 1$, puisque $b^{n.t} = 1$. Donc t divise l'ordre de ab. De même m divise l'ordre de ab ; donc $m.t$ divise l'ordre de ab, puisque m et t sont premiers entre eux.

PROPOSITION 0.45
Si p premier > 2, $m \geq 2$, alors

$$(\mathbb{Z}/p^\alpha\mathbb{Z})^* \simeq \mathbb{Z}/\phi(p^\alpha)\mathbb{Z} \simeq \mathbb{Z}/p^{\alpha-1}.(p-1)\mathbb{Z}$$

Démonstration *On va utiliser les lemmes précédents.*

•On considère tout d'abord l'application ψ définie par

$$\psi : (\mathbb{Z}/p^\alpha\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*,$$

ψ étant la fonction induite par l'identité (il convient de bien vérifier que ψ est bien définie et est un morphisme de groupes surjectif).

•par le Lemme 0.41 tout élément dont l'image par ψ est non égal à $\overline{1}$ engendre $(\mathbb{Z}/p\mathbb{Z})^*$; donc son ordre est un multiple de $p-1$.

•étant donné x un tel élément, il existe y appartenant au groupe engendré par x tel que y est d'ordre $p-1$.

•On applique alors le Lemme 0.44, $y.(p+1)$ est d'ordre le produit des ordres de y et de $p+1$; or y est d'ordre $p-1$ comme on vient de le voir, et $p+1$ est d'ordre $p^{\alpha-1}$ par le Corollaire 0.43 ; $y.(p+1)$ est donc d'ordre $(p+1).p^{\alpha-1}$; le groupe engendré par y est donc nécessairement $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ tout entier, d'où le résultat.

On vient donc par cette proposition de détailler la forme des $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ dans le cas où $p>2$. Il convient de considérer le cas $p=2$.

LEMME 0.46

$$k>0 \rightarrow 5^{2^k} = 1+\lambda.2^{k+2}$$

avec $\lambda \wedge 2 = 1$ (i.e. λ impair)

Démonstration *Facile, par récurrence.*

PROPOSITION 0.47
$(\mathbb{Z}/2\mathbb{Z})^* = \{1\}$, $(\mathbb{Z}/4\mathbb{Z})^* = \{1,-1\} \simeq \mathbb{Z}/2\mathbb{Z}$, et ensuite (pour $\alpha \leq 3$) $(\mathbb{Z}/2^\alpha\mathbb{Z})^* \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2^{\alpha-2}\mathbb{Z}$.

Démonstration *•On considère le morphisme surjectif ψ induit par l'identité de $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ sur $(\mathbb{Z}/4\mathbb{Z})^* = \{1,-1\} \simeq \mathbb{Z}/2\mathbb{Z}$.*

•Le noyau de ψ est d'ordre $2^{\alpha-2}$.

•5 appartient au noyau de ψ.

•par le Lemme 0.46, 5 est d'ordre $2^{\alpha-2}$ (l'ordre est une puissance de 2, et $5^{2^{\alpha-3}}$ ne peut être congru à 1).

•le noyau de ψ est donc cyclique (au vu des trois affirmations précédentes).

•On a alors la suite exacte (voir chapitre sur la théorie des groupes)

$$1 \rightarrow \mathbb{Z}/2^{\alpha-2} \rightarrow (\mathbb{Z}/2^\alpha\mathbb{Z})^* \xrightarrow{\psi} \mathbb{Z}/2\mathbb{Z} \rightarrow 1.$$

•Le sous-groupe $\{-1,1\}$ de $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ est une section de ψ, et il est distingué puisque notre groupe $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ est abélien. Donc on a un produit direct

$$(\mathbb{Z}/2^\alpha\mathbb{Z})^* \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$$

ce qui conclut la preuve (précisons que le produit direct $A\times B$ est isomorphe au produit direct $B\times A$).

1.5.3 Idéaux étrangers

DÉFINITION 0.19 **étrangers**
Soit A un anneau et c et d deux idéaux bilatères de A. Les anneaux c et d sont dits **étrangers** (ou comaximaux) si $c+d=A$.

Exemple 0.10 Exemples Deux idéaux maximaux distincts sont toujours étrangers.

PROPOSITION 0.48
Si $a_1, \ldots, a_n$, $b_1, \ldots, b_m$ sont des idéaux bilatères de A, et si pour tout $(i,j) \in \{1,\ldots,n\} \times \{1,\ldots,m\}$ a_i et b_j sont étrangers, alors les idéaux $a_1 \times a_2 \times \cdots \times a_n$ et $b_1 \times b_2 \times \cdots \times b_m$ sont étrangers.

Démonstration *On fait d'abord la preuve pour $m = 1$ en utilisant des égalités : $x_i + y_i = 1$ avec $x_i \in a_i$ et $y_i \in b_1$. On multiplie terme à terme. Puis on fait pareil avec $a_1, \ldots, a_n$ et chaque b_i.*

Remarque 0.6 dans $\mathbb{Z}$, a et b sont premiers entre eux si et seulement si (a) et (b) sont étrangers.

1.6 Corps

Les corps sont la troisième des catégories abstraites classiquement vues en algèbre (après groupes et anneaux). Les corps sont pourtant extrêmement anciens ne fût-ce que pour le cas de $\mathbb{R}$; mais leur formalisation est tardive et leur essort date notamment de la résolution d'équations polynomiales. Les nombres complexes forment un autre corps très important $\mathbb{C}$, qui en est la clôture algébrique. Dans la suite $\mathbb{Z} \to \mathbb{Q} \to \mathbb{R} \to \mathbb{C}$, on utilise consécutivement le passage au corps des fractions ($\mathbb{Z} \to \mathbb{Q}$), le passage au complété ($\mathbb{Q} \to \mathbb{R}$), la clôture algébrique ($\mathbb{R} \to \mathbb{C}$). Ainsi, un anneau (sous certaines hypothèses techniques), peut être plongé dans un corps (le corps des fractions rationnelles), et un corps peut être plongé dans sa clôture algébrique. Des corps très différents (finis) existent aussi, quoiqu'ils soient beaucoup plus abstraits ; typiquement $\mathbb{Z}/p\mathbb{Z}$ avec p premier. Un autre exemple important de corps, non commutatif, est le corps des quaternions.

Après une section dédiée aux généralités, on se penchera sur les extensions de corps et sur les corps finis. Les extensions de corps sont importantes lorsque $k \subset K$ avec k et K des corps avec les mêmes lois. K est alors en particulier une k-algèbre. Pour aller plus loin, on pourra se référer à [**?**, 2].

1.6.1 Définitions de base

DÉFINITION 0.20 **corps**
Un anneau $(K, +, .)$ est un **corps** si et seulement si le groupe des unités est $K - \{0\}$.

Un corps est dit **commutatif** si l'anneau sous-jacent est commutatif, c'est-à-dire si la multiplication est commutative.

On appelle **caractéristique** d'un corps k le plus petit $n \in \mathbb{N}$, s'il existe, tel que $0 = 1 + 1 + 1 + \cdots + 1$ (n fois). On dit que la caractéristique est nulle en cas contraire.

Propriétés •Dans un corps, tout élément est inversible.

•Un anneau commutatif intègre dont tout élément est inversible est un corps.

•Un anneau commutatif non nul est un corps si et seulement si ses seuls idéaux sont les idéaux triviaux.

•Un anneau intègre fini est un corps.

1.6.2 Extensions de corps

L'intérêt des extensions de corps (corps en contenant un autre) est qu'on arrive à dire des choses, alors que pour les anneaux inclus dans des anneaux, on en dit peu (noter toutefois les corps de fractions, qui étendent des anneaux à condition qu'ils soient intègres). Concrètement, l'intérêt des extensions de corps est aussi de permettre la résolution d'équations polynomiales. Il faut donc connaître quelques extensions fondamentales (parfois triviales, i.e. égales à k) de tout corps k : les corps de rupture « engendrés » par une racine d'un polynôme donné dans $k[X]$, les corps de décomposition « engendrés » par *toutes* les racines d'un polynôme donné, et la clôture algébrique (contenant toutes les racines de tous les polynômes).

DÉFINITION 0.21 **sous-corps**
Un sous-anneau L de l'anneau sous-jacent à un corps K est un **sous-corps** de K si c'est un corps pour les lois induites.

Si L est un sous-corps de K, on dit que K est un **sur-corps** ou une **extension** de L.

Avec L sous-corps de K, et $A \subset K$, on dit que A **engendre** K sur L si K est le plus petit sous-corps de K contenant A et L. On note alors $K = L(A)$. Si A est fini on note $K = L(a_1, ..., a_n)$. L'extension est dite **monogène** si A contient un seul élément.

Avant de construire un corps « autour » d'un corps (i.e. une extension de corps) on va déjà étendre un anneau intègre en un corps :

THÉORÈME 0.49
Étant donné un anneau intègre A, il existe un unique corps K (à isomorphisme près) contenant un anneau intègre B isomorphe à A et tel que tout sous-corps de K contenant B soit K lui-même. On l'appelle **corps des fractions** de A.

Démonstration *On procède selon les étapes suivantes pour montrer l'existence :*

•*On considère les classes d'équivalences sur $A \times A$ pour la relation $\mathcal{R}$ définie par*

$$(x, y)\mathcal{R}(x', y') \iff xy' = x'y$$

(intuitivement les classes d'équivalence sont les fractions). Appelons K l'ensemble quotient ainsi obtenu.

•*On considère ensuite l'addition sur ces classes, facile à retrouver au vu de la considération sur les fractions ; il s'agit de $(x, y) + (x', y') = (xy' + x'y, yy')$. De même la multiplication est définie par $(a, b).(a', b') = (aa', bb')$. Il est facile de voir que ces lois vérifient toutes les propriétés souhaitées, et qu'elles sont bien définies dans la structure quotient. On trouve un élément $(0, 1)$ neutre pour l'addition, et un élément $(1, 1)$ neutre pour la multiplication.*

•*L'application qui à x associe $(x, 1)$ est un morphisme injectif de A dans K. C'est donc un isomorphisme de A sur son image A'.*

•*Étant donné un sous-corps de K contenant A', il contient nécessairement les quotients d'éléments de A', et donc K tout entier.*

•*Il ne reste plus qu'à vérifier l'unicité de K, à isomorphisme près. Cette tâche est laissée au lecteur.*

Application 0.11 On a les cas suivants de corps de fractions :
– Construction de $\mathbb{Q}$ à partir de $\mathbb{Z}$.
— Construction du corps des fractions rationnelles, à partir de l'anneau des polynômes.

PROPOSITION 0.50
Algèbre linéaire et corps :
•Si L est un sous-corps de K, alors K est un L-espace vectoriel.
•Si la dimension de K en tant que L-espace vectoriel est finie alors on l'appelle **degré** de K pour L et on le note $[K : L]$.
•Si K et L sont finis, alors $|K| = |L|^{[K:L]}$.

Démonstration *Le premier point est clair.*
Le second point est une définition.
Le troisième point est clair.

THÉORÈME 0.51 **Théorème des bases téléscopiques**
Si $M \subset L \subset K$ (tous trois des corps), alors si e_i est une base de K en tant que L-espace vectoriel et si f_j est une base de L en tant que M-espace vectoriel , alors $e_i.f_j$ est une base de K en tant que M-espace vectoriel . Donc $[K : M] = [K : L].[L : M]$.

Démonstration *Facile.*

DÉFINITION 0.22 **Différentes extensions de corps**
Si L est une extension du corps K, alors un élément a de L est dit **algébrique sur** K s'il existe un polynôme P à coefficients dans K tel que $P(a) = 0$. Un nombre réel est souvent dit simplement **algébrique** s'il est algébrique sur $\mathbb{Q}$. L'ensemble des éléments de L algébriques sur K est appelée extension algébrique de K dans L.

Étant donné K un corps et $P \in K[X]$, on appelle **corps de rupture de** P un sur-corps L de K dans lequel P admet une racine a et tel que $L = K(a)$.

Étant donné K un corps et $P \in K[X]$, on appelle **corps de décomposition de** P un sur-corps L de K dans lequel P est scindé et $L = K(Z)$, avec Z l'ensemble des zéros de P dans L.

Étant donné K un corps, on appelle **clôture algébrique** de K une extension de K algébriquement close et dont tous les éléments sont algébriques sur K.

On a existence du corps de décomposition, et existence du corps de rupture lorsque le polynôme est sans racine (s'il n'est pas sans racine, le corps lui-même contient une racine, et il n'est pas besoin de l'étendre !). Dans les deux cas, on a unicité à isomorphisme près. Le théorème de Steinitz (difficile) montre que tout corps admet une clôture algébrique, unique à isomorphisme près.

Démonstration *(de l'existence du corps de rupture) Le corps $K(X)/(P)$ convient (i.e. le quotient de K par l'idéal engendré par P).*

1.6.3 Corps finis

Cette section, très brève, peut être prolongée par la lecture de [3].

Proposition 0.52
Un anneau intègre fini est un corps.

Démonstration *Si un anneau est intègre, l'application $x \mapsto yx$ est bijective pour tout y. En particulier, il existe x tel que $yx = 1$.*

Théorème 0.53
Un corps fini n'est jamais algébriquement clos.

Démonstration *Il suffit de considérer le polynôme $\prod_{k \in K} (X - k) + 1$.*

Théorème 0.54 **Wedderburn**
Tout corps fini est commutatif.

Théorème 0.55 **Corps de Galois**

Quel que soit p premier, quel que soit n dans $\mathbb{N}$ non nul, il existe un unique corps, à isomorphisme près, de cardinal p^n. Tout corps fini est de cette forme.

Les corps finis sont appelés aussi **corps de Galois** (d'ordre q quand le cardinal du corps est q). p est égal à la caractéristique du corps.

Démonstration *Ces résultats, non triviaux, ne seront pas prouvés ici. On pourra consulter [3] pour une preuve compréhensible.*

Enfin deux résultats (non triviaux) donnés sans preuve :

Proposition 0.56
Le groupe des automorphismes d'un corps fini de cardinal p^n est cyclique, d'ordre n, engendré par $x \mapsto x^n$.

Proposition 0.57
Le groupe multiplicatif d'un corps fini est cyclique.

Notons aussi l'existence de résultats sur les extensions de corps finis : toute extension fini d'un corps fini est engendrée par un seul élément.

1.7 Quelques résultats supplémentaires de théorie des nombres

On présentera ici quelques résultats supplémentaires, de bon aloi pour illustrer une leçon : la très classique étude des sous-groupes de $\mathbb{R}$ pour l'addition (1.7.1), représentation p-adique des réels (1.7.2), fractions continues (1.7.3), cryptographie à clé révélée (1.7.4).

1.7.1 Sous-groupes additifs de $\mathbb{R}$

La proposition qui suit n'est pas difficile, mais tellement plus joliment rédigée quand on a vu une fois qu'il fallait introduire $\inf G \cap \mathbb{R}^{+*}$.

PROPOSITION 0.58
Tout sous-groupe G du groupe $(\mathbb{R}, +)$ vérifie l'une et une seule des deux conditions suivantes :
- $\exists x \;\; G = x\mathbb{Z}$
- G est dense dans $\mathbb{R}$.

Démonstration *On considère $\alpha = \inf G \cap R^{+*}$. On distingue les deux cas $\alpha > 0$ et $\alpha = 0$.*

1.7.2 Représentation p-adique des réels

DÉFINITION 0.23 **fraction continue**
On se donne un entier $p > 1$. On appelle représentation p-adique du réel x la suite d'entiers $(c_n)_{n\in\mathbb{N}}$ définie par

$$c_n = \left\{ \begin{array}{l} E(x) \text{ si } n = 0 \\ \frac{1}{p^n}[E(p^n x) - pE(p^{n-1}x)] \text{ sinon} \end{array} \right.$$

($E(y)$ désignant la partie entière de y).

Intuition Le développement p-adique des réels est simplement la façon quotidienne de parler des nombres réels : le développement p-adique de π pour $p = 10$ est simplement $c_0 = 3$, $c_1 = 1$, $c_2 = 4$, $c_3 = 1$,... Les ordinateurs utilisent la même chose en binaire ($p = 2$).

Une propriété importante est

$$x = \sum_{n=0}^{+\infty} c_n p^{-n}$$

THÉORÈME 0.59
Le développement p-adique de $x \in \mathbb{R}$ est périodique à partir d'un certain rang si et seulement si x est rationnel.

Démonstration •*Supposons tout d'abord le développement périodique.*

Alors x est somme des $c_n p^{-n}$ pour $n \in \mathbb{N}$. Vue la périodicité, cette somme se réécrit comme somme d'un rationnel et de $\sum_{n\geq N} \frac{a}{(p^{-k})^n}$, avec a dans $\mathbb{N}$ et $k > 0$, et donc x est somme d'un rationnel et de $\frac{ap^{-kN}}{1-p^{-k}}$, et donc x est rationnel.

•*Réciproquement supposons que x soit rationnel.*

– On peut écrire $x = a/b$ avec a et b dans $\mathbb{N}$ (on se limite au cas $x > 0$, les autres cas étant similaires).

– On définit $x_0 = a$, et par récurrence $x_{n+1} = (x_n - bc_n)p$, avec c_n le quotient dans la division euclidienne de x_n par b.

– On montre facilement par récurrence que $0 \leq x_i < bp$ pour tout i et que les c_i sont le développement p-adique de x.

– les x_i étant bornés, on passe nécessairement deux fois par la même valeur ; à partir de ce moment, le développement est clairement périodique.

1.7.3 Fractions continues

DÉFINITION 0.24 **Fractions continues**
Une **fraction continue** est un objet de la forme suivante :

$$[a_0, a_1, \dots, a_n, \dots] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots}}}$$

Elle est caractérisée par une suite d'entiers qui est finie ou infinie.

On appelle **convergents** d'une fraction continue la suite de numérateurs p_n et de dénominateurs q_n définis par :

- $p_0 = a_0$, $q_0 = 1$
- $p_1 = a_0 a_1 + 1$, $q_1 = 1$
- $\vdots$
- $p_n = a_n p_{n-1} + p_{n-2}$,$q_n = a_n q_{n-1} + q_{n-2}$.

Propriétés

- A tout nombre réel on peut associer un et un seul développement en fraction continue.
- Tout nombre rationnel peut être représenté par une fraction continue finie (ex $\frac{1}{3} = 0 + \frac{1}{2+1}$).
- Seuls les nombres rationnels peuvent être représentés par une fraction continue finie.
- Un nombre est quadratique (i.e. solution d'une équation du second degré à coefficients dans $\mathbb{Z}$) si et seulement si son développement en fraction continue est périodique.
- Une fraction continue est liée à ses convergents par les relations $[a_0, \dots, a_n] = p_n/q_n$ et $[a_0, \dots, a_n, \dots] = \lim_n \frac{p_n}{q_n}$. En outre avec $[a_0, \dots, a_n] = \frac{p_n}{q_n}$, $|[a_0, \dots, a_n] - [a_0, \dots, a_n, \dots]| < 1/q_n^2$.

THÉORÈME 0.60 **Formule d'Euler**
Supposons les a_i tous non nuls.

Alors $1/a_1 - 1/a_2 + 1/a_3 - 1/a_4 + ... + (-1)^n/a_n =$

$$\cfrac{1}{a_1 + \cfrac{a_1^2}{a_2 - a_1 + \cfrac{a_1^2}{a_3 - a_2 + \cfrac{a_3^2}{\ddots + \cfrac{\ddots}{a_{n-1} - a_{n-2} + \cfrac{a_{n-1}^2}{a_n - a_{n-1}}}}}}}.$$

Démonstration *•Pour $n = 1$, le résultat est clair.*
•Au rang 2, un calcul rapide montre que le résultat est encore valable.
•On procède ensuite par récurrence, en supposant l'égalité vraie pour $n-1$ et les rangs inférieurs.
•Dans l'égalité pour $n-1$, on remplace a_n par $\frac{a_n . a_{n+1}}{a_{n+1} - a_n}$.
•Le résultat en découle tout seul.

1.7.4 Cryptographie à clé révélée : RSA

Nous nous limiterons ici à une brève introduction. On pourra consulter [4] pour plus d'informations.

Précisons que l'on parle aussi parfois de clé 'publique' ; il s'agit de la même notion que la clé révélée.

L'objectif de la **cryptographie** est de permettre de communiquer par des messages codés, qui ne pourront être lus que par leur destinataire.

Pour cela, un « superviseur » donne à chaque receveur potentiel un « décodeur » et une « clé ». La clé, comme son nom ne l'indique peut-être pas, est quelque chose qui peut être diffusé à tout le monde.

Pour envoyer un message M crypté à un individu I, il suffit de passer le message M par la moulinette de la clé correspondante à I. Cela n'est pas difficile, puisque I diffuse abondamment sa clé, à tous ses correspondants éventuels. Lorsque I reçoit un message, il peut alors utiliser son décodeur, qu'il est seul à posséder, pour transformer le message crypté en le message original.

La difficulté est que, formellement, il est toujours possible de reconstruire le message initial à partir du message crypté, pourvu que vous ayez la clé. Pour cela, il suffit de tester tous les messages possibles, l'un après l'autre (ils sont bien en bijection avec $\mathbb{N}$, comme on peut s'en convaincre facilement en considérant l'ordre lexicographique sur les messages possibles), et de les passer par la moulinette de la clé jusqu'à ce que l'on retrouve le message crypté. Mais il reste un espoir de fabriquer une cryptographie efficace, car bien sûr, cette méthode prendrait un temps énorme. La cryptographie est ainsi basée sur l'hypothèse de base que certaines tâches, faciles à faire dans un sens (le sens du cryptage par une clé), sont difficiles à faire dans l'autre (décryptage à l'aide d'une clé).

On note bien que la difficulté réside dans le fait que la fonction « clé » est publique. Si on cache la clé, il est très facile de réaliser des cryptographies parfaites. Par exemple, on peut utiliser le protocole suivant pour que A envoie un message à B :

– A signale à B qu'il veut lui envoyer un message, que l'on supposera constitué uniquement de 0 et de 1 (par un codage quelconque on peut facilement se ramener à cela), et de longueur 1000.

– B fournit à A une liste L de 1000 chiffres 0 ou 1, 0 et 1 étant équiprobables.

– le protocole recommence à l'étape précédente jusqu'à ce que la liste de chiffres soit passée sans être interceptée ; on tire au sort une nouvelle liste de 1000 chiffres à chaque nouvel essai.

– A transforme le message M en un message M', par $M' = M + L$ dans $\mathbb{Z}/2\mathbb{Z}$.

– A envoit M' à B ; si M' est intercepté, il ne sera pas décodable, puisque L n'est pas connu.

– B décode M' par $M = M' + L$ dans $\mathbb{Z}/2\mathbb{Z}$.

Aucune interception ne permet de décoder le message ; mais les étapes 2 et 3 peuvent prendre du temps ou n'être pas réalisables. Il est indispensable de changer de liste L à chaque nouveau message, ou du moins régulièrement - sinon, en considérant les fréquences des 0 et des 1, un observateur des différents M' pourrait finir par reconstituer L.

L'algorithme **RSA**, du nom de ses inventeurs, Rivest, Shamir et Adleman, est basé sur la difficulté de la factorisation d'un nombre entier en nombres premiers.

Supposons que A souhaite envoyer des messages cryptés RSA à B. Alors B se donne deux grands nombres premiers p et q. Maple permet aisément de construire de tels nombres, par exemple ; il suffit par exemple de tirer des nombres au sort et de recommencer jusqu'à ce qu'ils soient premiers, grâce à un algorithme permettant de dire si oui ou non un nombre est premier. En fait les algorithmes utilisés pour cela sont généralement probabilistes, c'est-à-dire qu'ils ont une probabilité non nulle de se tromper ; mais les erreurs sont extrêmement rares. La fonction Maple `isprime` permet de tester

la primalité d'un nombre ; par exemple, `isprime(12345678901234567890123456)` renvoit `false`, donc `12345678901234567890123456` n'est pas premier.

`nextprime(12345678901234567890123456)`
renvoit `12345678901234567890123651`,

qui est donc le nombre premier le plus petit plus grand que celui-ci. On constate donc que Maple permet très rapidement de trouver de grands nombres premiers ; les exemples ici fournis ne sont pas du tout à la limite du faisable, on peut aller largement au delà.

Ces deux nombres premiers seront notés p et q. La première partie de la clé publique, notée c, sera le produit de p et q. A utilise alors un nombre d (d est la seconde partie de la clé publique, qui peut donc être fournie par B éventuellement, si A n'a pas eu l'occasion d'accéder de manière sûre à p et q), premier avec $\phi(c) = (p-1)(q-1)$, où ϕ est la fonction d'Euler, c'est-à-dire le nombre de nombres premiers avec c qui sont plus petits que c, donc $(p-1)(q-1)$. Il est facile de choisir un nombre qui soit premier avec un autre : il suffit d'en piocher un au hasard, et de recommencer jusqu'à ce que l'algorithme de Bezout confirme que ces nombres sont premiers entre eux. On peut aussi déterminer facilement d^{-1}, inverse de d dans $(\mathbb{Z}/c\mathbb{Z})^* \simeq \mathbb{Z}/\phi(c)\mathbb{Z}$ (il y a isomorphisme car $(\mathbb{Z}/c\mathbb{Z})^* \simeq (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$ par le Corollaire 0.38 et isomorphisme entre $(\mathbb{Z}/p\mathbb{Z})^*$ et $\mathbb{Z}/(p-1)\mathbb{Z}$ (resp. $(\mathbb{Z}/q\mathbb{Z})^*$ et $\mathbb{Z}/(q-1)\mathbb{Z}$) par le Lemme 0.41) : il suffit d'utiliser l'algorithme de Bezout.

Cryptage :

– On suppose le message suffisamment court pour être codable par un élément inversible de $\mathbb{Z}/c\mathbb{Z}$, ce qui est possible en remplaçant le message par des tranches successives suffisamment petites (si on a un alphabet de taille α, il suffit de prendre des tranches de longueur l avec $\alpha^l < \phi(c)$). Cette méthode de codage n'a pas à être compliquée ni à être cachée. Il suffit donc d'avoir une injection de $[1, \alpha^l]$ dans $(\mathbb{Z}/c\mathbb{Z})^*$.

– chaque message de A est donc remplacé (par A) par un élément n inversible dans $\mathbb{Z}/c\mathbb{Z}$.

– A envoie alors à B le nombre $e = n^d$ dans $\mathbb{Z}/c\mathbb{Z}$.

Décryptage :

– B, qui dispose de d et de d^{-1}, effectue simplement le calcul de $e^{d^{-1}}$, qui lui donne n, et donc le message initial.

D'autres systèmes de cryptographie à clé publique font intervenir des structures plus complexes que $\mathbb{Z}/n\mathbb{Z}$, comme par exemple les courbes elliptiques.

Au total :

— Information accessible à B : p, q, $c = pq$, d, d^{-1} (pour $\mathbb{Z}/c\mathbb{Z}$), e (version codée du message, fournie par A).

— Information accessible à A : n, c, d, $e = n^d$ dans $\mathbb{Z}/c\mathbb{Z}$.

— Information accessible à tout l'univers : c, d, e. c et d permettent théoriquement de calculer d^{-1} dans $\mathbb{Z}/d\mathbb{Z}$, mais ce calcul est énorme ; alors qu'en disposant de q et p ce calcul est facile, grâce à notre théorème de Bezout.

Références

[1] B. Chazelle, *The Discrepancy Method*, Cambridge University Press, 2000.

[2] Wikipédia, *L'encyclopédie Libre, Wikipédia*, Wikipédia Fondation.

[3] D. Perrin, *Cours d'algèbre*, Ellipses 1996.

[4] F. Combes *Algèbre et géométrie*, Bréal, 1998.