Introduction à la Cryptologie

Chapitre 8 : Anneaux et corps

Michael Eisermann (Institut Fourier, UJF Grenoble)

Année 2008-2009
IF / IMAG, Master 1, S1-S2

document mis à jour le 7 juillet 2009

www-fourier.ujf-grenoble.fr/~eiserm/cours # crypto

Objectifs de ce chapitre

La cryptologie est en grande partie fondée sur des structures algébriques.

Dans les chapitres précédents nous avons étudié les groupes (abéliens).

Dans ce chapitre nous continuons à développer nos outils algébriques :

- Le vocabulaire des anneaux et des corps :
  sous-anneaux, sous-corps, morphismes, idéaux, ...
- L'anneau quotient A/I d'un anneau A par un idéal I.

Les anneaux suivants nous intéressent tout particulièrement :

- L'anneau $\mathbb{Z}$ des nombres entiers, et ses quotients.
- L'anneau $\mathbb{K}[X]$ des polynômes sur un corps $\mathbb{K}$, et ses quotients.

En cryptologie ce sont des objets fondamentaux et omniprésents.

Nous nous en servirons dans toute la suite : les chapitres suivants seront consacrés à l'arithmétique des polynômes et à la construction des corps finis.

Sommaire

Anneaux et corps

Soit A un ensemble muni de deux opérations $+, \cdot \colon A \times A \to A$.
On dit que $(A, +, \cdot)$ est un ***corps*** s'il vérifie aux axiomes suivants :

D'abord on exige que $(A, +)$ soit un groupe abélien :

(A1 : associativité) $\forall a, b, c \in A \colon\ (a+b)+c = a+(b+c)$

(A2 : commutativité) $\forall a, b \in A \colon\ a+b = b+a$

(A3 : élément neutre) $\exists 0 \in A\ \forall a \in A \colon\ 0+a = a$

(A4 : élément opposé) $\forall a \in A\ \exists b \in A \colon\ a+b = 0$

Ensuite on exige que la multiplication soit distributive sur l'addition :

(D : distributivité) $\forall a, b, c \in A \colon\ a \cdot (b+c) = (a \cdot b) + (a \cdot c)$

Finalement on exige que $(A^*, \cdot)$ soit un groupe abélien, où $A^* = A \smallsetminus \{0\}$:

(M1 : associativité) $\forall a, b, c \in A \colon\ (a \cdot b) \cdot c = a \cdot (b \cdot c)$

(M2 : commutativité) $\forall a, b \in A \colon\ a \cdot b = b \cdot a$

(M3 : élément neutre) $\exists 1 \in A^*\ \forall a \in A \colon\ 1 \cdot a = a$

(M4 : élément inverse) $\forall a \in A^*\ \exists b \in A \colon\ a \cdot b = 1$

Pour un ***anneau*** $(A, +, \cdot)$ on n'exige que (A1–A4), (D) et (M1).
Un anneau est ***commutatif*** s'il vérifie (M2), et ***unitaire*** s'il vérifie (M3) :

Dans la suite nous dirons « anneau » pour « anneau commutatif unitaire ».

Exemples simples

Pour chacun des exemples déterminer quels axiomes sont satisfaits :

1. Les nombres naturels $\mathbb{N}$, entiers $\mathbb{Z}$, rationnels $\mathbb{Q}$, réels $\mathbb{R}$, complexes $\mathbb{C}$.
2. Le sous-groupe $2\mathbb{Z} \subset \mathbb{Z}$ muni de la multiplication usuelle (par restriction)
3. Le quotient $\mathbb{Z}/_m$ muni de l'addition et de la multiplication induites.
4. Si $A_1, \dots, A_n$ sont des anneaux, on munit $A_1 \times \dots \times A_n$ des opérations

$$(a_1, \dots, a_n) + (b_1, \dots, b_n) := (a_1 + b_1, \dots, a_n + b_n),$$
$$(a_1, \dots, a_n) \cdot (b_1, \dots, b_n) := (a_1 b_1, \dots, a_n b_n).$$

   Si $A_1, \dots, A_n$ sont des corps, est-ce que $A_1 \times \dots \times A_n$ est un corps ?
5. Soit A un anneau et soit Ω un ensemble. On peut munir l'ensemble A^Ω des fonctions $\Omega \to A$ de l'addition et de la multiplication point par point. De même pour l'ensemble $A^{(\Omega)}$ des fonctions $\Omega \to A$ à support fini.
6. Pour tout ensemble Ω on peut considérer $(\mathscr{P}(\Omega), \Delta, \cap)$ où $\mathscr{P}(\Omega)$ est l'ensemble des parties de Ω et $A \mathbin{\Delta} B = (A \cup B) \smallsetminus (A \cap B)$.
7. Les matrices $\mathrm{Mat}(2 \times 2, \mathbb{C})$ avec les opérations usuelles :

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11} + a_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix}$$
$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}$$

   De même pour $\mathrm{Mat}(n \times n, A)$ sur un anneau A.

Exemples sophistiqués

7 Un corps non commutatif ? Les quaternions de Hamilton (1843)...

On considère $\mathbb{H} = \{a1 + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$ comme un espace vectoriel sur $\mathbb{R}$ qui a pour base $1, i, j, k$. On définit la multiplication sur la base par $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$, puis par extension linéaire sur tout $\mathbb{H}$. Visiblement le produit n'est pas commutatif... Est-ce que $(\mathbb{H}, +, \cdot)$ est un corps non commutatif ?

$$\mathbb{H} = \left\{ \begin{pmatrix} a+ib & -c-id \\ c-id & a-ib \end{pmatrix} \;\middle|\; a, b, c, d \in \mathbb{R} \right\} \subset \mathrm{Mat}(2 \times 2, \mathbb{C}).$$

8 Un corps de cardinal 4 ? La découverte de Galois (1830)...

On sait que $\mathbb{Z}/_2$ est un corps de cardinal 2 ; de même $\mathbb{Z}/_3$ est un corps de cardinal 3 ; mais $\mathbb{Z}/_4$ de cardinal 4 n'est pas un corps. Existe-t-il un corps de cardinal 4 ? Essayons $\mathbb{F}_4 = \{0, 1, x, y\}$ avec les opérations suivantes :

$+$	0	1	x	y
0	0	1	x	y
1	1	0	y	x
x	x	y	0	1
y	y	x	1	0

$\cdot$	0	1	x	y
0	0	0	0	0
1	0	1	x	y
x	0	x	y	1
y	0	y	1	x

En dépit d'outils, c'est pour le moment une question de brute force.
Un des objectifs de ce cours et de construire tous les corps finis.

Remarques

Convention de notation : on écrit $ab + cd$ au lieu de $(a \cdot b) + (c \cdot d)$.

Dans tout groupe l'élément 0, étant neutre pour l'addition, est unique.
De même, l'élément opposé de a est unique, et on le note $-a$.
Dans tout anneau on a $0a = (0+0)a = 0a + 0a$, d'où $0 = 0a$.

Dans tout anneau l'élément 1, étant neutre pour la multiplication, est unique :
si $1' \in A$ vérifie $1'a = a1' = a$ pour tout $a \in A$, alors $1' = 1 \cdot 1' = 1$.
On trouve $(-1)a + a = (-1)a + 1a = (-1+1)a = 0a = 0$, d'où $(-1)a = -a$.

Dans tout corps, l'élément inverse de a est unique :
si $ab = ab' = 1$, alors $b = 1b = (b'a)b = b'(ab) = b'1 = b'$.
L'unicité nous permet d'écrire sans univoque a^{-1} pour l'inverse de a.

L'exemple trivial $(\{0\}, +, \cdot)$ est l'anneau nul où $1 = 0$ (anneau non unitaire).
Inversement, si $1 = 0$, alors $a = 1a = 0a = 0$ donc $A = \{0\}$.

Diviseurs de zéro

Définition (diviseurs de zéros)

Soit A un anneau. On note $A^* = A \smallsetminus \{0\}$ les éléments non nuls.

On dit que $a \in A^*$ est un ***diviseur de zéro*** s'il existe $b \in A^*$ tel que $ab = 0$.

L'anneau A est ***intègre*** s'il n'a pas de diviseurs de zéro.

Remarque

Un corps est un anneau intègre car il n'a jamais de diviseurs de zéro :

Si $ab = 0$ et $a \neq 0$ alors $b = 1b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0$.

Exemples

L'anneau $\mathbb{Z}/_6$ a des diviseurs de zéro : $\bar{2} \cdot \bar{3} = \bar{0}$.

L'anneau $\mathbb{Z}/_7$ est un corps et n'a donc pas de diviseurs de zéro.

L'anneau $\mathbb{Z}$ est intègre mais ce n'est pas un corps.

Exercice

Pour $m \in \mathbb{Z}$, $m \geq 2$, nous avons $\mathbb{Z}/_m$ intègre $\Leftrightarrow$ m premier $\Leftrightarrow$ $\mathbb{Z}/_m$ un corps.

Éléments inversibles

Définition (éléments inversibles)

Un élément $a \in A$ est ***inversible*** dans A s'il existe $b \in A$ tel que $ab = 1$.

Dans ce cas b est unique et on l'appelle ***l'inverse*** de a, noté a^{-1}.

On définit $A^\times := \{a \in A \mid a \text{ est inversible dans } A\}$.

Exemples

Dans l'anneau $\mathbb{Z}$ nous avons $\mathbb{Z}^\times = \{-1, +1\} \subsetneq \mathbb{Z}^*$.

Dans l'anneau $\mathbb{Z}/_m$ nous avons $\mathbb{Z}/_m^\times = \{\bar{a} \mid a \in \mathbb{Z} \text{ et } \operatorname{pgcd}(a, m) = 1\}$.

Remarque

Un élément inversible n'est jamais un diviseur de zéro.

Un anneau est un corps si et seulement si $A^\times = A^*$.

Exercice

Un anneau fini intègre est un corps.

Le groupe des éléments inversibles

Proposition

Soit $(A, +, \cdot)$ *un anneau (commutatif). Alors* $(A^\times, \cdot)$ *est un groupe (abélien).*

Démonstration.
Si $a, b \in A^\times$, alors $ab \in A^\times$ car $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}b = 1$.
Ceci permet de définir la multiplication $\cdot\colon A^\times \times A^\times \to A^\times$ par restriction.
Cette multiplication est associative (et commutative si l'anneau l'est).
L'élément 1 est inversible, donc $1 \in A^\times$, et il sert d'élément neutre.
Si $a \in A^\times$ alors $a^{-1} \in A^\times$ par définition, et $aa^{-1} = 1$. □

Exemples

Dans $\mathbb{Z}$ nous avons $\mathbb{Z}^\times = \{-1, +1\} \subsetneq \mathbb{Z}^*$. Dans $\mathbb{Q}$ nous avons $\mathbb{Q}^\times = \mathbb{Q}^*$.

Dans $\mathbb{Z}/_m$ nous avons $\mathbb{Z}/_m^\times = \{\bar{a} \mid a \in \mathbb{Z}$ et $\operatorname{pgcd}(a, m) = 1\}$.
Ici l'inverse se calcule par l'algorithme d'Euclide-Bézout.
Nous avons analysé sa structure par le théorème des restes chinois.

Pour l'anneau $A = \operatorname{Mat}(n \times n, \mathbb{K})$ des matrices sur un corps $\mathbb{K}$ nous obtenons le groupe $A^\times = \operatorname{GL}(n; \mathbb{K}) = \{A \in \operatorname{Mat} \mid \det(A) \in \mathbb{K}^\times\}$ des matrices inversibles. Ici l'inverse se calcule par l'algorithme de Gauss.

Anneaux et corps : extensions quadratiques

Les exemples suivants sont une source d'inspiration inépuisable.

Exercice (entiers de Gauss)

On considère le corps des nombres complexes $\mathbb{C} = \mathbb{R} + i\mathbb{R}$ où $i^2 = -1$.
L'ensemble $\mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\}$ est-il un corps ? (sous-corps de $\mathbb{C}$)
L'ensemble $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ est-il un anneau ? (sous-anneau de $\mathbb{C}$)

Exercice (extensions quadratiques)

En généralisant l'exemple précédent on fixe un entier $c \in \mathbb{Z}$ quelconque.
L'ensemble $\mathbb{Q}[\sqrt{c}] = \{a + b\sqrt{c} \mid a, b \in \mathbb{Q}\}$ est-il un (sous-)corps ?
L'ensemble $\mathbb{Z}[\sqrt{c}] = \{a + b\sqrt{c} \mid a, b \in \mathbb{Z}\}$ est-il un (sous-)anneau ?

Exercice (norme et éléments inversibles)

On fixe $c \in \mathbb{Z}$, ici $c < 0$ pour simplifier. Nous écrivons $\sqrt{c} = i\sqrt{d}$ où $d = |c|$.
On définit $N \colon \mathbb{Z}[i\sqrt{d}] \to \mathbb{N}$ par $N(a + ib\sqrt{d}) := |a + ib\sqrt{d}|^2 = a^2 + b^2 d$.

A-t-on mutiplicativité $N(xy) = N(x)N(y)$ pour tout $x, y \in \mathbb{Z}[i\sqrt{d}]$?
Montrer que $x \in \mathbb{Z}[i\sqrt{d}]$ est inversible si et seulement si $N(x) = 1$.
Expliciter ainsi les groupes $\mathbb{Z}[i]^\times$ puis $\mathbb{Z}[i\sqrt{d}]^\times$ pour $d \in \mathbb{N}$, $d \geq 2$.

Morphismes d'anneaux

Définition (morphisme d'anneaux)

Soient A, B deux anneaux.
Une application $\phi\colon A \to B$ est un ***morphisme d'anneaux*** si

- $\phi(x + y) = \phi(x) + \phi(y)$, morphisme des groupes additifs,
- $\phi(1_A) = 1_B$ et $\phi(xy) = \phi(x)\phi(y)$ pour tout $x, y \in A$.

C'est un mono- / épi- / isomorphisme s'il est injectif / surjectif / bijectif.

Exemple (théorème des restes chinois)

L'application quotient $\pi\colon \mathbb{Z} \to \mathbb{Z}/_m$ est un morphisme d'anneaux.

Pour $m, n \in \mathbb{Z}$ il existe un unique morphisme d'anneaux $\mathbb{Z}/_{mn} \to \mathbb{Z}/_m \times \mathbb{Z}/_n$.
C'est un isomorphisme d'anneaux si et seulement si $\operatorname{pgcd}(m, n) = 1$.
Dans ce cas ϕ induit un isomorphisme de groupes $\mathbb{Z}/_{mn}^\times \xrightarrow{\sim} \mathbb{Z}/_m^\times \times \mathbb{Z}/_n^\times$.
Nous l'avons utilisé pour l'indicatrice d'Euler et le cryptosystème RSA.

Remarque (exercice)

Si $\phi\colon A \to B$ est un isomorphisme d'anneaux, alors l'application inverse $\phi^{-1}\colon B \to A$ est aussi un (iso)morphisme d'anneaux. Tout morphisme d'anneaux $A \to B$ induit un morphisme de groupes $A^\times \to B^\times$.

Morphismes de corps

Définition

Soient A, B deux corps. Alors tout morphisme d'anneaux $\phi\colon A \to B$ est appelé ***morphisme de corps***.

Proposition

Tout morphisme de corps est injectif.

Démonstration. Soit $\phi\colon A \to B$ un morphisme de corps.
Pour $a \in A^* = A^\times$ on a $\phi(a)\phi(a^{-1}) = \phi(aa^{-1}) = \phi(1_A) = 1_B$.
On en déduit que $\phi(a) \neq 0$ et que $\phi(a)^{-1} = \phi(a^{-1})$.
En particulier $\ker(\phi) = \{0\}$ est ϕ est injectif. $\square$

Remarque

Un morphisme de corps n'a en général aucune raison d'être surjectif :
les inclusions $\mathbb{Q} \hookrightarrow \mathbb{R}$ et $\mathbb{R} \hookrightarrow \mathbb{C}$ sont injectives mais non surjectives.

Caractéristique d'un anneau ou d'un corps

Remarque (exercice de révision)

Soit $\mathbb{Z}$ l'anneau des nombres entiers et soit A un anneau quelconque.
Il existe un unique morphisme d'anneaux $\phi\colon \mathbb{Z} \to A$, à savoir $\phi(n) = n \cdot 1_A$.
Le noyau $\ker(\phi)$ est donc un sous-groupe de $\mathbb{Z}$.
Nous en déduisons que $\ker(\phi) = m\mathbb{Z}$ pour un certain $m \in \mathbb{Z}$, $m \geq 0$.
Par passage au quotient nous obtenons $\bar{\phi}\colon \mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} \operatorname{im}(\phi) \subset A$.

Définition

Le générateur $m \geq 0$ de l'exemple précédent tel que $\ker(\mathbb{Z} \to A) = m\mathbb{Z}$ est appelé la ***caractéristique*** de l'anneau A, notée $\operatorname{car}(A) = m$.

Exemples

Nous avons $\operatorname{car}(\mathbb{Z}/_m) = m$ pour tout $m \in \mathbb{N}$, ainsi que $\operatorname{car}(\mathbb{Z}) = \operatorname{car}(\mathbb{Q}) = 0$.
À noter que $\operatorname{car}(A) = 0$ si et seulement si le morphisme $\mathbb{Z} \to A$ est injectif.

Remarque

Si A est intègre, alors ou $\operatorname{car}(A) = 0$ ou $\operatorname{car}(A)$ est un nombre premier.
Si K est un corps, alors ou $\mathbb{Q} \subset K$ ou $\mathbb{Z}/_p \subset K$ (léger abus de notation).

Exercice

Soit A un anneau de caractéristique p où p est un nombre premier.
Alors $\mathfrak{f}\colon A \to A$, $\mathfrak{f}(a) = a^p$ est un morphisme d'anneaux.

Que faut-il montrer ?
Quant à l'addition il faut montrer que $\mathfrak{f}(a+b) = \mathfrak{f}(a) + \mathfrak{f}(b)$ pour tout $a, b \in A$.
Quant à la multiplication il faut montrer que $\mathfrak{f}(1) = 1$ et $\mathfrak{f}(ab) = \mathfrak{f}(a)\mathfrak{f}(b)$.

Solution. On a toujours $\mathfrak{f}(1) = 1^p = 1$ et $\mathfrak{f}(ab) = (ab)^p = a^p b^p = \mathfrak{f}(a)\mathfrak{f}(b)$.
Ici nous n'utilisons que l'associativité et la commutativité de la multiplication.

Pour p premier nous avons déjà montré que $p \mid \binom{p}{k}$ pourvu que $0 < k < p$.
Comme A est de caractéristique p nous avons $p \cdot 1_A = 0_A$ dans A, d'où
$\mathfrak{f}(a+b) = (a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} = a^p + b^p = \mathfrak{f}(a) + \mathfrak{f}(b)$. ☺

Sous-anneaux

Définition (sous-anneau)

Soit A un anneau. Un ***sous-anneau*** de A est une partie $B \subset A$ telle que

- B est un sous-groupe de $(A, +)$,
- $1 \in B$ et $xy \in B$ pour tout $x, y \in B$.

Ainsi $(B, +, \cdot)$ est un anneau et $B \hookrightarrow A$ est un morphisme d'anneaux.

Exemples

Par exemple, $\mathbb{Z}$ est un sous-anneau du corps $\mathbb{Q}$ (ou de $\mathbb{R}$).
Par contre, $2\mathbb{Z}$ n'est pas un sous-anneau de $\mathbb{Z}$ car $1 \neq 2\mathbb{Z}$.

Proposition

Soit $\phi \colon A \to A'$ un morphisme d'anneaux.
Si B est un sous-anneau de A, alors $\phi(B)$ est un sous-anneau de A'.
En particulier l'image $\operatorname{im}(\phi) = \phi(A)$ est un sous-anneau de A'.

Exemples

Bien sûr $A \subset A$ est un sous-anneau de A ; c'est le plus grand.
De même $\operatorname{im}(\mathbb{Z} \to A)$ est un sous-anneau de A ; c'est le plus petit.

Sous-corps

Définition (sous-corps)

Un ***sous-corps*** est un sous-anneau qui est un corps. Plus explicitement :

Soit A un corps (ou un anneau). Un sous-corps $K \subset A$ est un sous-anneau tel que tout élément non nul $x \in K$ admette un inverse dans K.

Exemples

$\mathbb{Z}$ est un sous-anneau de $\mathbb{R}$ mais non un sous-corps.
$\mathbb{Q}$ est un sous-corps de $\mathbb{R}$, ainsi que $\mathbb{R}$ est un sous-corps de $\mathbb{C}$.

Exercice (caractérisation des sous-corps)

Soit A un corps. Une partie $K \subset A$ est un sous-corps si $0, 1 \in K$ et pour tout a, b dans K on a aussi $a + b$ et $a - b$ et ab et ab^{-1} (pourvu que $b \neq 0$) dans K. Une moitié de ces exigences est redondante : laquelle ?

Exercice (révision des espaces vectoriels)

Soit E un anneau et soit $K \subset E$ un corps. On a l'addition $+\colon E \times E \to E$ et la multiplication $\cdot\colon K \times E \to E$ des éléments de E par des éléments de K. Montrer que cette structure satisfait aux axiomes d'un espace vectoriel.

Ainsi un anneau E est un espace vectoriel sur tout sous-corps K.

Sous-anneaux et sous-corps engendrés

Proposition (exercice)

Soit $(A_i)_{i\in I}$ *une famille de sous-anneaux* A_i *d'un anneau* B*.*
Alors leur intersection $A := \bigcap_{i\in I} A_i$ *est un sous-anneau de* B*.* □

Définition (sous-anneau engendré)

Soit B un anneau, $A \subset B$ un sous-anneau, et $S \subset B$ un sous-ensemble.
On note $A[S]$ le plus petit sous-anneau de B contenant à la fois A et S :
c'est l'intersection de tous les sous-anneaux de B contenant A et S.

Proposition (exercice)

Soit $(K_i)_{i\in I}$ *une famille de sous-corps* K_i *d'un anneau* A*.*
Alors leur intersection $K := \bigcap_{i\in I} K_i$ *est un sous-corps de* A*.* □

Définition (sous-corps engendré)

Soit L un corps, $K \subset L$ un sous-corps, et $S \subset L$ un sous-ensemble.
On note $K(S)$ le plus petit sous-corps de L contenant à la fois K et S :
c'est l'intersection de tous les sous-corps de L contenant K et S.

Exercice

Dans $\mathbb{C}$ expliciter le sous-anneau $\mathbb{Z}[i]$ et le sous-corps $\mathbb{Q}(i)$ où $i^2 = -1$.
Déterminer la dimension de $\mathbb{Q}(i)$ comme espace vectoriel sur $\mathbb{Q}$.

Exercice

Dans $\mathbb{C}$ expliciter le sous-anneau $\mathbb{Z}[\sqrt{c}]$ où $c \in \mathbb{Z}$ et le sous-corps $\mathbb{Q}(\sqrt{c})$.
Déterminer la dimension de $\mathbb{Q}(\sqrt{c})$ comme espace vectoriel sur $\mathbb{Q}$.

Exercice

Dans $\mathbb{R}$ expliciter le sous-anneau $\mathbb{Q}[e]$ et le sous-corps $\mathbb{Q}(e)$ où $e = \sum_{k=0}^{\infty} \frac{1}{k!}$.
Déterminer la dimension de $\mathbb{Q}[e]$ comme espace vectoriel sur $\mathbb{Q}$.

Nous admettons ici que $e = \sum_{k=0}^{\infty} \frac{1}{k!}$ est transcendant sur $\mathbb{Q}$,
c'est-à-dire que $a_0 + a_1 e + \cdots + a_n e^n \neq 0$ si $(a_0, a_1, \ldots, a_n) \neq 0$.

Corps des fractions : définition

Tout sous-anneau d'un corps est intègre : $ab = 0$ implique $a = 0$ ou $b = 0$.
Étant donné un anneau intègre, pouvons-nous le plonger dans un corps ?

Définition

On appelle ***corps des fractions*** de A toute paire (K, κ) tel que

- K est un corps et $\kappa \colon A \to K$ est un monomorphisme d'anneaux.
- Tout $x \in K$ s'écrit comme $\kappa(a)\kappa(b)^{-1}$ où $a, b \in A$, $b \neq 0$.

Proposition (propriété universelle)

Soit (K, κ) un corps des fractions d'un anneau A.
Soit $\lambda \colon A \to L$ un monomorphisme dans un corps L.
Alors il existe un unique morphisme de corps $\phi \colon K \to L$ tel que $\lambda = \phi \circ \kappa$.

Démonstration. Si $\kappa(a)\kappa(b)^{-1} = \kappa(c)\kappa(d)^{-1}$ alors $\kappa(a)\kappa(d) = \kappa(b)\kappa(c)$, d'où $\kappa(ad) = \kappa(bc)$ puis $ad = bc$ car κ est un monomorphisme.
Ainsi $\lambda(ad) = \lambda(bc)$ puis $\lambda(a)\lambda(d) = \lambda(b)\lambda(c)$ d'où $\lambda(a)\lambda(b)^{-1} = \lambda(c)\lambda(d)^{-1}$.
On peut donc définie ϕ par $\kappa(a)\kappa(b)^{-1} \mapsto \lambda(a)\lambda(b)^{-1}$ où $a, b \in A$, $b \neq 0$.
On vérifie ensuite que ϕ est un morphisme de corps. □

Corollaire (unicité)

Deux corps des fractions d'un anneau A sont canoniquement isomorphes.

Corps des fractions : construction

Proposition (existence)

Pour tout anneaux intègre A il existe un corps des fractions (K, κ).

Démonstration. On veut construire les fractions $\frac{a}{b}$ pour $a, b \in A$, $b \neq 0$.
En s'inspirant de cette idée, on considère $F = A \times A^*$ avec les opérations

$$(a, b) + (c, d) := (ad + bc, bd) \qquad \text{et} \qquad (a, b) \cdot (c, d) := (ac, bd).$$

On constate que $(F, +, \cdot)$ n'est pas un anneau. (Pourquoi ?)

Afin de sortir de cette impasse, on définit la relation $(a, b) \sim (c, d)$ si $ad = bc$.
On vérifie d'abord qu'il s'agit d'une relation d'équivalence, ensuite que les opérations $+$ et $\cdot$ sont bien définies sur le quotient $K = F/_{\sim}$, et finalement que $(K, +, \cdot)$ est un corps. (Le détailler ! Où utilise-t-on l'intégrité de A ?)

La classe d'équivalence de (a, b) est notée $\frac{a}{b}$. L'application $\kappa \colon A \to K$ donnée par $a \mapsto \frac{a}{1}$ est un homomorphisme d'anneaux et il est injectif. Tout élément $x \in K$ s'écrit comme $x = \frac{a}{b} = \frac{a}{1}\frac{1}{b} = \kappa(a)\kappa(b)^{-1}$ où $a, b \in A$, $b \neq 0$. $\square$

Remarque (le corps des fractions comme extension)

On peut identifier l'anneau A avec son image $\kappa(A)$ dans le corps K.
Ainsi A devient un sous-anneau de son corps des fractions K.

Idéaux

Remarque

Pour tout morphisme d'anneaux $\phi\colon A \to B$ le noyau $I = \ker(\phi)$ vérifie

(1) I est un sous-groupe de $(A, +)$.

(2) Pour tout $a \in A$ et $b \in I$ on a $ab \in I$.

Démonstration. Pour (2) on voit que $\phi(ab) = \phi(a)\phi(b) = \phi(a) \cdot 0 = 0$. □

Définition

Un ***idéal*** d'un anneau A est un sous-ensemble $I \subset A$ satisfaisant (1) et (2).

Exemples

Évidemment $\{0\}$ et A sont des idéaux de A, dits ***idéaux triviaux***.
Nous savons que $m\mathbb{Z}$ est un idéal de $\mathbb{Z}$, et tout idéal de $\mathbb{Z}$ est de cette forme.

Exercice (correspondance des idéaux)

Soit $\phi\colon A \to B$ un épimorphisme d'anneaux. Soit $\mathscr{I}$ l'ensemble des idéaux de A contenant $\ker(\phi)$. Soit $\mathscr{J}$ l'ensemble des idéaux de B. Alors

$$\Phi\colon \mathscr{I} \to \mathscr{J}, I \mapsto \phi(I), \qquad \text{et} \qquad \Psi\colon \mathscr{J} \to \mathscr{I}, J \mapsto \phi^{-1}(J),$$

sont bien définies et des bijections mutuellement inverses.

Construction de l'anneau quotient

Proposition

*Soit I un idéal d'un anneau A. Alors sur le quotient A/I il existe une unique structure d'anneau telle que $\pi\colon A \to A/I$ soit un morphisme d'anneaux. Ainsi on appelle A/I **l'anneau quotient** de A par I.*

Pour $I = A$ on obtient l'anneau nul $A/I = \{\bar{0}\}$ qui n'est pas unitaire ($\bar{1} = \bar{0}$).
Si l'anneau A est unitaire ($1 \neq 0$) et si l'idéal I est propre ($I \subsetneq A$),
alors l'anneau quotient A/I est à nouveau unitaire ($\bar{1} \neq \bar{0}$).

Démonstration. Le groupe $(A, +)$ est abélien et $I \subset A$ est un sous-groupe. Sur le quotient A/I il existe donc une unique structure de groupe telle que l'application quotient $\pi\colon A \to A/I$ soit un morphisme de groupes.

Si π est un morphisme d'anneau, alors $\pi(x)\pi(y) = \pi(xy)$.
Ceci prouve l'unicité de la multiplication sur A/I.

Pour montrer son existence, il faut vérifier que le produit $\pi(x)\pi(y) := \pi(xy)$ ne dépend que $\pi(x), \pi(y) \in A/I$ et non des représentants $x, y \in A$.
Si $\pi(x) = \pi(x')$ et $\pi(y) = \pi(y')$ alors $x' = x + a$ et $y' = y + b$ avec $a, b \in I$.
Nous trouvons $x'y' - xy = (x + a)(y + b) - xy = xb + ay + ab \in I$.
Ceci prouve que $\pi(x'y') = \pi(xy)$, le produit est donc bien défini.

Finalement, on vérifie aisément que $(A/I, +, \cdot)$ ainsi construit satisfait aux axiomes d'un anneau et que $\pi\colon A \to A/I$ est un morphisme de groupe. $\square$

Passage à l'anneau quotient

Proposition

Soit A un anneau, soit $I \subset A$ un idéal, et soit $\phi\colon A \to B$ un morphisme d'anneaux. Les deux conditions suivantes sont équivalentes :

1. *Il existe un morphisme d'anneaux $\bar{\phi}\colon A/I \to B$ tel que $\phi = \bar{\phi} \circ \pi$.*
2. $I \subset \ker(\phi)$

Dans ce cas on dit que ϕ ***passe au quotient*** *; le morphisme $\bar{\phi}$ est unique, et on l'appelle le morphisme* ***induit*** *par passage au quotient.*

Démonstration. «⇒» Si $a \in I$ alors $\pi(a) = 0$, donc $\phi(a) = \bar{\phi} \circ \pi(a) = 0$.

«⇐» Supposons que $I \subset \ker(\phi)$, et construisons $\bar{\phi}$ tel que $\phi = \bar{\phi} \circ \pi$
Cette exigence entraîne que $\bar{\phi}(\mathfrak{cl}(a)) = \phi(a)$. Montrons que c'est bien défini.
Si $\mathfrak{cl}(a) = \mathfrak{cl}(b)$, alors $a - b \in I$, donc $a - b \in \ker(\phi)$, puis $\phi(a) = \phi(b)$.
On peut donc définir $\bar{\phi}\colon A/I \to A$ par $\bar{\phi}(\mathfrak{cl}(a)) := \phi(a)$.
On a $\phi = \bar{\phi} \circ \pi$ par construction. C'est un morphisme d'anneaux :

$$\begin{aligned}
\bar{\phi}(\mathfrak{cl}(a) + \mathfrak{cl}(b)) &= \bar{\phi}(\mathfrak{cl}(a+b)) = \phi(a+b) = \phi(a) + \phi(a) = \bar{\phi}(\mathfrak{cl}(a)) + \bar{\phi}(\mathfrak{cl}(b)),\\
\bar{\phi}(\mathfrak{cl}(a)\mathfrak{cl}(b)) &= \bar{\phi}(\mathfrak{cl}(ab)) = \phi(ab) = \phi(a)\phi(a) = \bar{\phi}(\mathfrak{cl}(a))\bar{\phi}(\mathfrak{cl}(b)),\\
\bar{\phi}(\mathfrak{cl}(1_A)) &= \phi(1_A) = 1_B.
\end{aligned}$$

Ceci prouve la proposition. □

Factorisation canonique des morphismes

Corollaire

Tout morphisme d'anneaux $\phi\colon A \to B$ *induit un isomorphisme d'anneaux* $\bar\phi\colon A/\ker(\phi) \xrightarrow{\sim} \operatorname{im}(\phi)$.

Démonstration. D'abord ϕ induit un morphisme surjectif $\tilde\phi\colon A \to \operatorname{im}(\phi)$.
Par passage au quotient $\tilde\phi$ induit un morphisme $\bar\phi\colon A/\ker(\phi) \to \operatorname{im}(\phi)$.
Si $\bar\phi(\bar x) = \bar\phi(\bar y)$ alors $\phi(x) = \phi(y)$, donc $x - y \in \ker(\phi)$, d'où $\bar x = \bar y$. $\square$

Exemple

Pour tout anneau A il existe un unique morphisme d'anneaux $\phi\colon \mathbb{Z} \to A$.
Nous en déduisons que $\ker(\phi) = m\mathbb{Z}$ pour un certain $m \in \mathbb{Z}$, $m \geq 0$.
Par passage au quotient nous obtenons $\bar\phi\colon \mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} \operatorname{im}(\phi) \subset A$.

Autrement dit, tout anneau A contient une copie de $\mathbb{Z}/m\mathbb{Z}$ comme sous-anneau où l'entier $m = \operatorname{car}(A)$ est la caractéristique de A.

Idéaux engendrés

Proposition (exercice)

Soit $(I_\lambda)_{\lambda\in\Lambda}$ est une famille d'idéaux I_λ d'un anneau A.
Alors leur intersection $I = \bigcap_{\lambda\in\Lambda} I_\lambda$ est un idéal de A.

Définition

Soit A un anneau et soit $S \subset A$ un sous-ensemble.
On note $(S) \subset A$ le plus petit idéal de A contenant S :
c'est l'intersection de tous les idéaux de A contenant S.

Remarque (exercice)

Plus explicitement, pour tout $S \subset A$ nous avons

$$(S) = \{\, a_1 s_1 + \cdots + a_n s_n \mid n \geq 0, a_1, \ldots, a_n \in A, s_1, \ldots, s_n \in S \,\}.$$

Notons des cas particuliers : Pour un singleton $S = \{s\}$ on écrit

$$(S) = (s) = sA = As = \{as \mid a \in A\}.$$

Pour une famille finie $S = \{s_1, \ldots, s_n\}$ on écrit

$$(S) = (s_1, \ldots, s_n) = As_1 + \cdots + As_n.$$

Idéaux engendrés : exemples et applications

Exemple

Dans l'anneau $\mathbb{Z}$ tout idéal est de la forme (m) pour un $m \in \mathbb{N}$.
Pour tout $a, b \in \mathbb{Z}$ on a $(a, b) = (m)$ où $m = \operatorname{pgcd}(a, b)$ par Bézout.

Proposition

Un anneau A est un corps si et seulement si ses seuls idéaux sont $\{0\}$ et A.

Démonstration. «$\Rightarrow$» Soit A un corps et soit $I \subset A$ un idéal.
Si $I \neq \{0\}$ alors il existe $x \in I \setminus \{0\}$.
Pour tout $a \in A$ on a donc $a = (ax^{-1}) \cdot x \in I$, donc $I = A$.

«$\Leftarrow$» Supposons que $\{0\}$ et A sont les seuls idéaux de A.
Pour $a \in A^*$ on a $\{0\} \neq (a)$, donc $(a) = A$.
Il existe donc $b \in A$ tel que $ab = 1$, d'où a est inversible. $\square$

Corollaire

Tout morphisme $\phi\colon K \to A$ d'un corps dans un anneau unitaire est injectif.

Démonstration. Le noyau $I = \ker(\phi)$ est un idéal de K.
Puisque $\phi(1_K) = 1_A \neq 0_A$, nous avons $1_K \notin I$, donc $I \neq K$.
Notre hypothèse implique que $I = \{0\}$, donc ϕ est injectif. $\square$

Idéaux d'un quotient

Proposition

Soit $I \subset A$ un idéal et soit $\pi\colon A \to A/I$ le morphisme quotient.
Soit $\mathscr{X}$ l'ensemble des idéaux de A contenant I.
Soit $\mathscr{Y}$ l'ensemble des idéaux du quotient A/I.
Alors les applications

$$\Phi\colon \mathscr{X} \to \mathscr{Y}, X \mapsto \pi(X), \qquad \textit{et} \qquad \Psi\colon \mathscr{Y} \to \mathscr{X}, Y \mapsto \pi^{-1}(Y),$$

sont bien définies et des bijections mutuellement inverses.

Exercice

Prouver la proposition. Expliciter les idéaux de $\mathbb{Z}/12\mathbb{Z}$ et leurs inclusions.
Expliciter les quotients de $\mathbb{Z}/12\mathbb{Z}$ et leurs morphismes quotients.

Idéaux premiers et maximaux

Définition

Soit A un anneau et soit $I \subset A$ un idéal.

- On dit que I est ***premier*** si l'anneau quotient A/I est intègre.
- On dit que I est ***maximal*** si l'anneau quotient A/I est un corps.

Rappelons que A/I est intègre si $\bar{x} \neq 0$ et $\bar{y} \neq 0$ entraîne $\bar{x} \cdot \bar{y} \neq 0$.
Par contraposé, ceci veut dire : si $\bar{x} \cdot \bar{y} = 0$, alors $\bar{x} = 0$ ou $\bar{y} = 0$
Pour l'idéal $I \subsetneq A$ ceci veut dire : si $xy \in I$, alors $x \in I$ ou $y \in I$.

Remarques

L'idéal (0) est premier si et seulement si A est intègre.
L'idéal $(1) = A$ n'est jamais premier car $A/A = \{\bar{0}\}$ n'est pas intègre.
Tout corps est intègre, donc tout idéal maximal est premier.

Si A/I est un corps, alors ses seuls idéaux sont $\{\bar{0}\}$ et A/I.
Les seuls idéaux de A contenant I sont donc I et A. Par conséquent :

Proposition

Un idéal $I \subsetneq A$ est maximal si pour tout idéal J de A vérifiant $I \subset J \subset A$ on a ou $J = I$ ou $J = A$. □

L'anneau des fonctions polynomiales

Exercice (l'anneau des fonctions $C^\infty(\mathbb{R}, \mathbb{R})$)

L'ensemble $\mathbb{C}^\infty(\mathbb{R}, \mathbb{R})$ des fonctions $\mathbb{R} \to \mathbb{R}$ infiniment dérivables est un anneau pour l'addition et la multiplication des fonctions (point par point).
Il contient $\mathbb{R}$ comme sous-corps des fonctions constantes. L'anneau $\mathbb{C}^\infty(\mathbb{R}, \mathbb{R})$ n'est pas intègre : si f, g sont à supports disjoints, alors $gf = 0$.

Exercice (l'anneau des fonctions polynomiales)

La fonction identité définie par $X \colon \mathbb{R} \to \mathbb{R}$, $x \mapsto x$, appartient à $C^\infty(\mathbb{R}, \mathbb{R})$.
Le sous-anneau $\mathbb{R}[X]$ est formé des fonctions polynomiales $f = \sum_{k=0}^{n} a_k X^k$.
Évidemment les coefficients $a_0, \dots, a_n \in \mathbb{R}$ déterminent la fonction f, et réciproquement les coefficients sont déterminés par f, car $a_k = \frac{1}{k!} f^{(k)}(0)$.

On définit le degré par $\deg f := \sup\{k \in \mathbb{N} \mid a_k \neq 0\}$. Montrer qu'il vérifie $\deg(f + g) \leq \sup\{\deg f, \deg g\}$ et $\deg(fg) = \deg(f) + \deg(g)$.
En déduire le groupe $\mathbb{R}[X]^\times$ des éléments inversibles.

L'anneau des fonctions polynomiales en deux variables

Exercice (l'anneau des fonctions $C^\infty(\mathbb{R}^2, \mathbb{R})$)

L'ensemble $\mathbb{C}^\infty(\mathbb{R}^2, \mathbb{R})$ des fonctions $\mathbb{R}^2 \to \mathbb{R}$ infiniment dérivables est un anneau pour l'addition et la multiplication des fonctions (point par point). Il contient $\mathbb{R}$ comme sous-corps des fonctions constantes.

Exercice (l'anneau des fonctions polynomiales en deux variables)

$C^\infty(\mathbb{R}^2, \mathbb{R})$ contient $X, Y \colon \mathbb{R}^2 \to \mathbb{R}$, $X(x,y) = x$ et $Y(x,y) = y$.
Le sous-anneau $\mathbb{R}[X,Y]$ est formé des fonctions $f = \sum_{k,\ell} a_{k,\ell} X^k Y^\ell$.

Les coefficients $a_{k,\ell} \in \mathbb{R}$ sont déterminés par f, car $a_{k,\ell} = \frac{1}{k!} \frac{1}{\ell!} \frac{\partial^{k+\ell} f}{\partial x^k \partial y^\ell}(0)$.

On définit le degré total par $\deg f := \sup\{k + \ell \mid a_{k,\ell} \neq 0\}$. Montrer qu'il vérifie $\deg(f+g) \leq \sup\{\deg f, \deg g\}$ et $\deg(fg) = \deg(f) + \deg(g)$.
En déduire le groupe $\mathbb{R}[X,Y]^\times$ des éléments inversibles.

L'anneau des fonctions trigonométriques

Exercice (l'anneau des fonctions trigonométriques)

Les fonctions $\cos, \sin \colon \mathbb{R} \to \mathbb{R}$ appartiennent à l'anneau $\mathbb{C}^\infty(\mathbb{R}, \mathbb{R})$.

Le sous-anneau $\mathbb{R}[\cos]$ est formé des fonctions $f = \sum_{k=0}^{n} \bar{a}_k \cos^k$, $\bar{a}_k \in \mathbb{R}$. En linéarisant, on peut réécrire f comme $f(x) = \sum_{k=0}^{n} a_k \cos(kx)$, $a_k \in \mathbb{R}$. Dans une telle écriture les coefficients a_k sont uniquement déterminés par la fonction f, car $a_0 = \frac{1}{2\pi} \int_0^{2\pi} f(x)dx$ et $a_k = \frac{1}{\pi} \int_0^{2\pi} f(x) \cos(kx)dx$ pour $k \geq 1$.

Le sous-anneau $\mathbb{R}[\cos, \sin]$ est formé des fonctions $f = \sum_{k,\ell} a_{k,\ell} \cos^k \sin^\ell$. Malheureusement une telle écriture n'est pas unique, car $\cos^2 + \sin^2 = 1$.

Montrer que le sous-anneau $\mathbb{R}[\cos, \sin]$ est formé des fonctions $f(x) = a_0 + \sum_{k=1}^{n} a_k \cos(kx) + b_k \sin(kx)$ où $a_k, b_k \in \mathbb{R}$, et qu'ici les coefficients sont uniquement déterminés par f.

On peut donc définir $\deg f := \sup\{k \in \mathbb{N} \mid a_k \neq 0$ ou $b_k \neq 0\}$. Montrer qu'il vérifie $\deg(f + g) \leq \sup\{\deg f, \deg g\}$ et $\deg(fg) = \deg(f) + \deg(g)$. En déduire le groupe $\mathbb{R}[\cos, \sin]^\times$ des éléments inversibles.