



Table des matières

I	Anneaux, sous-anneaux, corps	2
I.1	Structure d'anneau	2
I.2	Calculs dans un anneau	2
I.3	Eléments remarquables dans un anneau	4
I.4	Sous-anneaux	5
I.5	Structure de corps	6
II	Arithmétique élémentaire	7
II.1	Bases de numération dans \mathbb{N}	7
II.2	Divisibilité dans \mathbb{Z}	11
II.3	Pgcd de deux entiers relatifs	12
II.4	Entiers premiers entre eux	15
II.5	Résolution dans \mathbb{Z} de l'équation $ax+by=c$	16
II.6	Ppcm de deux entiers relatifs	18
II.7	Extension au cas de plusieurs entiers relatifs	19
II.8	Nombres premiers	20

I Anneaux, sous-anneaux, corps

I.1 Structure d'anneau

Définition

Soit A un ensemble muni de deux lois de composition, notées $+$ et \times .

On dit que $(A, +, \times)$ est un *anneau* si :

- $(A, +)$ est un groupe commutatif (son neutre est en général noté 0).
- La loi \times est associative et distributive par rapport à l'addition.
- Il existe un élément neutre pour le produit \times (en général noté 1).

Si de plus la loi \times est commutative, on dit que $(A, +, \times)$ est un *anneau commutatif*.

Exemples

– $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des anneaux commutatifs.

– Si E est un ensemble, $(\mathcal{P}(E), \Delta, \cap)$ est un anneau commutatif.

– Soient $(A, +, \times)$ un anneau et X un ensemble non vide.

Soit $\mathcal{F}(X, A)$ l'ensemble des applications de X vers A .

$\mathcal{F}(X, A)$, muni des lois $+$ et \times déduites de celles de A , est un anneau.

- Le neutre pour l'addition est l'application constante égale à 0 .
- Celui du produit est l'application constante égale à 1 .

En particulier $\mathcal{F}(\mathbb{R}, \mathbb{R})$ et $\mathcal{F}(\mathbb{N}, \mathbb{R})$ (suites réelles) sont des anneaux.

– Soit A l'ensemble des applications de \mathbb{C} dans \mathbb{C} , de la forme $z \rightarrow \alpha z + \beta \bar{z}$.

$(A, +, \circ)$ est un anneau non commutatif (le produit est la loi de composition).

Anneau nul

Soit $(A, +, \times)$ un anneau de neutres 0 (pour la loi $+$) et 1 (pour la loi \times).

Il est possible que les deux éléments 0 et 1 de A soient identiques.

Mais dans ce cas A se réduit à $\{0\}$ (anneau nul, sans grand intérêt).

Anneau produit

Soit $(A, +, \times)$ un anneau.

On définit des lois $+$ et \times sur $A \times A$ en posant :

$$\begin{cases} (a, b) + (c, d) = (a + c, b + d). \\ (a, b)(c, d) = (ac, bd). \end{cases}$$

On vérifie que $(A \times A, +, \times)$ est un anneau :

$$\begin{cases} \text{Le neutre additif est } (0, 0). \\ \text{Le neutre multiplicatif est } (1, 1). \end{cases}$$

On peut généraliser à A^n , pour tout n de \mathbb{N}^* . Par exemple $(\mathbb{R}^n, +, \times)$ est un anneau.

I.2 Calculs dans un anneau

Règles de calcul

Soit $(A, +, \times)$ un anneau (on note 0 le neutre pour $+$, et 1 le neutre pour \times).

Rappelons qu'on note $a - b$ plutôt que $a + (-b)$.

Pour tout (a, b, c) de A^3 , et tout entier relatif m , on a :

$$\begin{cases} a0 = 0a = 0, & (-a)b = a(-b) = -(ab) \\ (-a)(-b) = ab, & a(b - c) = ab - ac \\ (a - b)c = ac - bc, & a(mb) = (ma)b = m(ab) \end{cases}$$

Sommes et produits. Développements

Soit $(A, +, \times)$ un anneau.

Pour toute famille finie a_m, a_{m+1}, \dots, a_n d'éléments de A , on pose :

$$a_m + \dots + a_n = \sum_{k=m}^n a_k \quad \text{et} \quad a_m \times \dots \times a_n = \prod_{k=m}^n a_k$$

Si $m > n$, on pose encore $\sum_{k=m}^n a_k = 0$ et $\prod_{k=m}^n a_k = 1$.

On vérifie les égalités, pour tout b de A :

$$b \left[\sum_{k=m}^n a_k \right] = \sum_{k=m}^n (ba_k) \quad \text{et} \quad \left[\sum_{k=m}^n a_k \right] b = \sum_{k=m}^n (a_k b)$$

Plus généralement (notations analogues) :

$$\left[\sum_{j=m}^n a_j \right] \left[\sum_{k=p}^q b_k \right] = \sum_{j=m}^n \left[a_j \sum_{k=p}^q b_k \right] = \sum_{j=m}^n \sum_{k=p}^q a_j b_k$$

Si a et b commutent, alors, pour tout n de \mathbb{N} :

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

En particulier :

$$\forall q \in A, \forall n \in \mathbb{N}^*, 1 - q^n = (1 - q) \sum_{k=0}^{n-1} q^k = (1 - q)(1 + q + q^2 + \dots + q^{n-1})$$

On en déduit que si $q^n = 0$, $1 - q$ est inversible et

$$(1 - q)^{-1} = 1 + q + \dots + q^{n-1}$$

Si a et b commutent, on a la formule du binôme :

$$\forall n \in \mathbb{N}, (a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$$

I.3 Eléments remarquables dans un anneau

Proposition (*Groupe des éléments inversibles*)

- || Soit A un anneau non nul.
- || On note A^* l'ensemble des éléments de A inversibles pour le produit.
- || A^* est un groupe pour la loi \times .

Remarques

- On note que $A^* \subset A - \{0\}$.
Il peut y avoir inclusion stricte. Par exemple, $\mathbb{Z}^* = \{-1, 1\}$.
- Dans l'anneau $(\mathcal{F}(\mathbb{R}), +, \times)$ des fonctions de \mathbb{R} dans \mathbb{R} , les fonctions qui sont inversibles pour le produit sont celles qui ne s'annulent jamais.
L'inverse d'une telle fonction f est $\frac{1}{f}$.
On ne confondra pas avec la bijection inverse pour la composition des applications.

Définition (*Diviseurs de zéro*)

- || Soit A un anneau non réduit à $\{0\}$. Soit a un élément non nul de A .
- || On dit que a est un *diviseur de zéro* s'il existe b dans A , non nul, tel que $ab = 0$ ou $ba = 0$.

Exemples et remarques

- Dans $(A^2, +, \times)$ les couples $(a, 0)$ et $(0, a)$, où $a \neq 0$, sont des diviseurs de zéro.
- a est un diviseur de zéro $\Leftrightarrow a$ est non simplifiable pour le produit.
- Si a est inversible, il est simplifiable, et n'est donc pas un diviseur de zéro.
En prenant la contraposée : si a est un diviseur de zéro, il n'est pas inversible.
- Ces deux notions ne sont cependant pas équivalentes.
Par exemple 2 n'est pas inversible dans l'anneau $(\mathbb{Z}, +, \times)$, et pourtant ce n'est pas un diviseur de zéro (il est simplifiable).

Définition (*Anneau intègre*)

- || On dit qu'un anneau $(A, +, \times)$ est *intègre* s'il est commutatif et sans diviseur de zéro.
- || Un anneau intègre est donc un anneau commutatif A dans lequel $ab = 0 \Rightarrow a = 0$ ou $b = 0$.

Exemples

- $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des anneaux intègres.
- Si $(A, +, \times)$ est non nul, les anneaux $(A^n, +, \times)$ ($n \geq 2$) ne sont pas intègres.
- Soit E un ensemble contenant au moins deux éléments.
L'anneau commutatif $(\mathcal{P}(E), \Delta, \cap)$ n'est pas intègre : $\forall X \subset E, X \cap \overline{X} = \emptyset$.

Définition (*Eléments nilpotents*)

- || Soit A un anneau non réduit à $\{0\}$. Soit a un élément non nul de A .
- || On dit que a est *nilpotent* s'il existe un entier naturel n tel que $a^n = 0$.
- || Avec ces notations, $\forall p \geq n, a^p = 0$.
- || Le plus petit entier n tel que $a^n = 0$ est appelé *indice de nilpotence* de a .



Propriétés et exemples

- Si a est nilpotent, alors a est un diviseur de 0. Il n'est donc pas inversible.
- Si a et b commutent et sont nilpotents, $a + b$ est nul ou nilpotent.
- Soit $(A, +, \circ)$ l'anneau des applications $z \rightarrow \alpha z + \beta \bar{z}$, avec $(\alpha, \beta) \in \mathbb{C}^2$.
L'application $f : z \rightarrow iz + \bar{z}$ est nilpotente, car $f \circ f = 0$ (application nulle).

I.4 Sous-anneaux

Définition

Soit $(A, +, \times)$ un anneau (on note 1 le neutre pour le produit). Soit B une partie de A .

On dit que B est un *sous-anneau* de $(A, +, \times)$ si :

- $1 \in B$
- $\forall (a, b) \in B^2, a + b \in B$ (stabilité pour la loi $+$)
- $\forall (a, b) \in B^2, ab \in B$ (stabilité pour la loi \times)
- Muni des lois induites, $(B, +, \times)$ possède lui-même muni d'une structure d'anneau.

Proposition (Caractérisation d'un sous-anneau)

B est un sous-anneau de $(A, +, \times)$ si et seulement si :

- $1 \in B$ • $\forall (a, b) \in B^2, a - b \in B$ • $\forall (a, b) \in B^2, ab \in B$

Exemples

- Dans $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$, chacun est un sous-anneau du suivant.
- Le seul sous-anneau de $(\mathbb{Z}, +, \times)$ est $(\mathbb{Z}, +, \times)$ lui-même.
- Soit D l'ensemble $\{m10^{-n}, m \in \mathbb{Z}, n \in \mathbb{N}\}$ de tous les nombres décimaux.
 D est un sous-anneau de $(\mathbb{Q}, +, \times)$.
- L'ensemble $\{r + s\sqrt{2}, (r, s) \in \mathbb{Q}^2\}$ est un sous-anneau de $(\mathbb{R}, +, \times)$.

Définition (Morphismes d'anneaux)

Soient $(A, +, \times)$ et $(B, +, \times)$ deux anneaux.

On note 1_A et 1_B les neutres multiplicatifs. On note 0_A et 0_B les neutres additifs.

On dit qu'une application f de A vers B est un *morphisme d'anneaux* si :

- $f(1_A) = 1_B$
- $\forall (a, b) \in A^2, f(a + b) = f(a) + f(b)$
- $\forall (a, b) \in A^2, f(ab) = f(a)f(b)$

Remarques

- En particulier, f est un morphisme de groupes, de $(A, +)$ vers $(B, +)$.
- On note encore $\ker(f) = \{a \in A, f(a) = 0_B\}$. $\forall (a, b) \in A^2, f(a) = f(b) \Leftrightarrow b - a \in \ker(f)$.
- Le morphisme f est injectif $\Leftrightarrow \ker(f) = \{0_A\}$.

I.5 Structure de corps

Définition

Soit K un ensemble muni de deux lois $+$ et \times .

On dit que $(K, +, \times)$ est un *corps* si :

- $(K, +, \times)$ est un anneau commutatif non réduit à $\{0\}$.
- $K^* = K - \{0\}$, c'est-à-dire tout élément non nul de K est inversible pour le produit.

Exemples et remarques

- $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des corps, mais pas $(\mathbb{Z}, +, \times)$.
- Dans un corps, tous les éléments non nuls sont simplifiables.
Il n'y a donc pas de diviseur de 0, et à fortiori pas d'élément nilpotent.
- Un corps est un cas particulier d'anneau intègre ($xy = 0$ implique $x = 0$ ou $y = 0$).
- Si $(K, +, \times)$ est un corps, $(K^2, +, \times)$ n'est pas un corps (idem avec K^n , si $n \geq 2$).

Définition (Sous-corps)

Soit $(K, +, \times)$ un corps.

On dit qu'une partie L de K est un *sous-corps* de $(K, +, \times)$ si :

- L est un sous anneau de $(K, +, \times)$
- $\forall x \in L$, avec $x \neq 0$, $x^{-1} \in L$.
- Muni des lois induites, $(L, +, \times)$ possède alors lui-même une structure de corps.

Proposition (Caractérisation des sous-corps)

L est un *sous-corps* de $(K, +, \times) \Leftrightarrow$:

- $1 \in L$
- $\forall (x, y) \in L^2, x - y \in L$
- $\forall (x, y) \in L^2$, avec $y \neq 0$, $xy^{-1} \in L$.

Remarques et exemples

- Si L est un sous-corps de $(K, +, \times)$, on dit que K est une *extension* de $(L, +, \times)$.
- Dans $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$, chacun est un sous-corps du suivant.
- Le seul sous-corps de $(\mathbb{Q}, +, \times)$ est lui-même.
- L'ensemble $\{r + s\sqrt{2}, (r, s) \in \mathbb{Q}^2\}$ est un sous-corps de $(\mathbb{R}, +, \times)$.

Définition (Morphisme de corps)

Soient $(K, +, \times)$ et $(L, +, \times)$ deux corps.

On dit qu'une application f de K dans L est un *morphisme de corps* si f est un morphisme de l'anneau $(K, +, \times)$ dans l'anneau $(L, +, \times)$, c'est-à-dire si :

- $f(1_K) = 1_L$
- $\forall (x, y) \in K^2, f(x + y) = f(x) + f(y)$
- $\forall (x, y) \in K^2, f(xy) = f(x)f(y)$

Si de plus f est bijective, on dit que f est un *isomorphisme de corps*.

Proposition (*Corps des fractions d'un anneau intègre*)

Soit $(A, +, \times)$ un anneau intègre.

Il existe un corps $(K, +, \times)$, unique à un isomorphisme près, tel que $(A, +, \times)$ est un sous-anneau de K , et tel que $K = \{ab^{-1}, (a, b) \in A^2, b \neq 0\}$.

On dit que K est le *corps des fractions* de l'anneau intègre A .

Remarques et exemples

- Dire que K est unique à un isomorphisme près, c'est dire que si K et K' répondent à la question, alors il existe un isomorphisme f de corps de $(K, +, \times)$ sur $(K', +, \times)$.
- $(\mathbb{Q}, +, \times)$ est le corps des fractions de l'anneau intègre $(\mathbb{Z}, +, \times)$.
- C'est la proposition précédente qui permet de construire le corps $(K(X), +, \times)$ des fractions rationnelles à coefficients dans K , à partir de l'anneau intègre $(K[X], +, \times)$ des polynômes à coefficients dans K .

II Arithmétique élémentaire

II.1 Bases de numération dans \mathbb{N}

Proposition (*Numération en base b*)

Soit b un entier supérieur ou égal à 2.

Tout entier $n \geq 1$ s'écrit de manière unique $n = c_p b^p + c_{p-1} b^{p-1} + \dots + c_1 b + c_0 = \sum_{k=0}^p c_k b^k$, avec : $p \in \mathbb{N}, \forall k \in \{0, \dots, p\}, c_k \in \llbracket 0, \dots, b-1 \rrbracket$ et $c_p \neq 0$.

On pose alors $n = \overline{c_p c_{p-1} \dots c_1 c_0}$ et on parle de l'écriture de n en base b .

On dit que $c_p, c_{p-1}, \dots, c_1, c_0$ sont les *chiffres* de la représentation de n en base b .

Exemples

- On utilise le plus souvent les bases $b = 2$ (numérotation *binnaire*, les chiffres sont 0 et 1), $b = 8$ (numérotation *octale*, les chiffres sont 0, 1, ..., 7), $b = 10$ (numérotation *décimale*, les chiffres sont 0, 1, ..., 9), ou $b = 16$ (numérotation *hexadécimale*, les chiffres sont 0, 1, ..., 9 puis A, B, C, D, E, F qui remplacent respectivement 10, 11, 12, 13, 14, 15).
- L'entier $n = 2001$ (en numération décimale) s'écrit $n = \overline{11111010001}$ en numération binaire, $n = \overline{3721}$ en numération octale, et $n = \overline{7D1}$ en numération hexadécimale.

Interprétation et calcul des chiffres en base b

- Si $n = \overline{c_p c_{p-1} \dots c_1 c_0}$, alors c_0 est le reste dans la division euclidienne de n par la base b , et $q = \overline{c_p c_{p-1} \dots c_1}$ est le quotient dans cette division.

Les chiffres c_0, c_1, \dots, c_p sont donc les restes obtenus successivement dans des divisions répétées par b (jusqu'à obtenir un quotient nul, c_p étant le reste dans cette dernière division).

L'écriture de b en base b est $\overline{10}$. Celle de b^m est $\overline{10 \dots 0}$ (le chiffre 1 suivi par m chiffres 0).

- Si $n = \overline{c_p c_{p-1} \dots c_1 c_0}$ et si $1 \leq m \leq p$, les entiers $\overline{c_p c_{p-1} \dots c_m}$ et $\overline{c_{m-1} \dots c_1 c_0}$ représentent respectivement le quotient et le reste dans la division de n par b^m .

Comparaison de deux nombres écrits en base b

- Soient $n = \overline{c_p c_{p-1} \dots c_1 c_0}$ et $m = \overline{d_q d_{q-1} \dots d_1 d_0}$, avec la convention $c_p \neq 0$ et $d_q \neq 0$.
Si $p \neq q$, alors n et m sont dans le même ordre que p et q .
Si $p = q$, alors n et m sont dans le même ordre que les $(p+1)$ -uplets $(c_p, c_{p-1}, \dots, c_1, c_0)$ et $(d_p, d_{p-1}, \dots, d_1, d_0)$ classés suivant l'ordre lexicographique (c'est-à-dire départagés par la première inégalité entre chiffres de même rang, dans une lecture de gauche à droite.)
- Les entiers qui s'écrivent $n = \overline{c_{p-1} \dots c_1 c_0}$ (c'est-à-dire avec p chiffres) sont compris entre $b^{p-1} = 10 \dots 0$ (le chiffre 1 suivi de $p-1$ fois le chiffre 0) et $b^p - 1 = \alpha \alpha \dots \alpha$ (p fois le chiffre noté ici α et correspondant à la valeur $b-1$.)

Somme de deux nombres écrits en base b

- Soient x et y deux entiers naturels non nuls.
Quitte à rajouter en tête des chiffres égaux à 0, on peut supposer que les écritures en base b des entiers x et y ont la même longueur.

Si $x = \overline{x_p \dots x_1 x_0} = \sum_{k=0}^p x_k b^k$ et $y = \overline{y_p \dots y_1 y_0} = \sum_{k=0}^p y_k b^k$, on a $z = x + y = \sum_{k=0}^p (x_k + y_k) b^k$.

Dans cette écriture, les entiers $x_k + y_k$ sont compris entre 0 et $2b-2$. Ils peuvent être supérieurs à $b-1$ et ne représentent donc pas en général les chiffres z_k de $z = x + y$.

Pour obtenir cette représentation, il faut utiliser et reporter une retenue de 1 à chaque fois que la somme intermédiaire obtenue est supérieure ou égale à b .

La procédure Maple suivante additionne deux entiers représentés par les listes X et Y de leurs chiffres (aucun test n'est effectué sur la validité des arguments). On place dans x la plus longue des deux listes (l'autre est complétée par des 0) et on forme la somme dans la liste x :

```

somme:=proc(X,Y) global base; local x,y,n,r,k;
  if nops(X)>=nops(Y) then x:=X: y:=Y else x:=Y: y:=X fi;
  n:=nops(x): y:=[0$n-nops(y),op(y)]; r:=0;
  for k from n to 1 by -1 do
    x[k]:=x[k]+y[k]+r;
    if x[k]>=base then x[k]:=x[k]-base: r:=1 else r:=0 fi;
  od;
  if r=1 then [1,op(x)] else x fi;
end:
    
```

Produit de deux nombres écrits en base b

- Le produit de $n = \overline{c_p c_{p-1} \dots c_1 c_0}$ par la base b s'écrit $\overline{c_p c_{p-1} \dots c_1 c_0 0}$. Plus généralement le produit par b^m s'obtient en ajoutant m fois le chiffre 0 à la droite de la représentation de n .
- Soient x et y deux entiers naturels non nuls, écrits en base b :

Si $x = \overline{x_p \dots x_1 x_0} = \sum_{j=0}^p x_j b^j$ et $y = \overline{y_q \dots y_1 y_0} = \sum_{k=0}^q y_k b^k$ (avec $x_p \neq 0$ et $y_q \neq 0$).

Alors le produit $z = xy$ peut s'écrire $z = \sum_{j=0}^p x_j b^j y = \sum_{j=0}^p \left(\sum_{k=0}^q x_j y_k b^{k+j} \right)$.

Notons $t_j = \sum_{k=0}^q x_j y_k b^{k+j}$ le produit de y par $x_j b^j$.