Algèbre - Chapitre 9

Arithmétique et dénombrement

I Arithmétique dans $\mathbb{Z}$

1) Divisibilité

a) Généralités

Rappel : Ensembles de nombres entiers

On note $\mathbb{N}$ l'ensemble des nombres entiers naturels, c'est à dire l'ensemble des entiers positifs ou nuls.
On note $\mathbb{Z}$ l'ensemble des nombres entiers relatifs, c'est à dire l'ensemble des entiers positifs ou négatifs (ou nul).

Définition :

Soient a et b deux entiers relatifs.
On dit que b divise a et on note $b|a$ si et seulement si

$$\exists q \in \mathbb{Z}, a = bq$$

On dit alors que b est un **diviseur** de a, et que a est un **multiple** de b.

Exemples :

- 3 divise -12 puisque $-12 = 3 \times (-4)$.
- 1 et -1 divisent tous les entiers : $\forall n \in \mathbb{Z}$, on peut écrire $n = 1 \times n$ et $n = (-1) \times (-n)$.
- Tous les entiers divisent 0 :

Notation

On note $\mathcal{D}(a)$ l'ensemble des diviseurs positifs de a.
On note $a\mathbb{Z}$ l'ensemble des multiples de $\mathbb{Z}$.

Exemples :

- $\mathcal{D}(4) =$ et $\mathcal{D}(-4) =$
- $\mathcal{D}(0) =$
- L'ensemble des multiples de 2 est $2\mathbb{Z}$: l'ensemble des nombres paires.

Remarques :

- L'ensemble des diviseurs de a est le même que l'ensemble des diviseurs de $-a$: c'est la raison pour laquelle on s'intéressera aux diviseurs positifs.
- Pour tout $n > 0$, si $d|n$, alors $d \leq n$.

b) Division euclidienne sur $\mathbb{Z}$

Theorème 1 :
Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Alors il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tels que

$$a = bq + r \text{ avec } 0 \leq r < |b|$$

- q est appelé **quotient de la division euclidienne** de a par b,
- r est appelé **reste de la division euclidienne**.

Remarques :
- si a et b sont des entiers naturels, alors $q \in N$ également.
- On a immédiatement que $b|a$ si et seulement si le reste de la division euclidienne de a par b est nul.

▷ *Preuve* :

◁

2) PGCD et PPCM

a) Définition

Définition :
Soient a et b deux entiers non tous nuls.
On appelle **PGCD** de a et b le plus grand diviseur commun à a et à b. On le note parfois $a \wedge b$.
On appelle **PPCM** de a et b le plus petit multiple strictement positif commun à a et b. On le note parfois $a \vee b$.

Remarques :
- L'ensemble des diviseurs communs à a et b est majoré par $|a|$ et par $|b|$, et l'ensemble des diviseurs est fini. Donc il admet bien un plus grand élément.
- L'ensemble des multiples positifs admet bien un plus petit élément, puisque c'est une partie de $\mathbb{N}$ minorée par $\min(|a|, |b|)$. Il y a donc bien un plus petit élément.
- Comme 1 divise tous les entiers, on a toujours $1 \leq a \wedge b$.
- Comme $|ab|$ est un multiple commun à a et b, on a $a \vee b \leq |ab|$.
- si a est non nul et $b = 0$, on a immédiatement $a \wedge b = |a|$

b) Algorithme d'Euclide

Propriété 1 :
Soient a et b deux entiers avec $b \neq 0$.
Si $a = bq + r$ avec q, r entiers, alors $a \wedge b = b \wedge r$

▷ *Preuve* :

◁

Méthode : **Algorithme d'Euclide**

Soient a et b deux entiers, avec b non nul.
Tant que b est non nul, on effectue les opérations suivantes :

1. On effectue la division euclidienne :
$$a = bq + r$$
2. On remplace (a, b) par (b, r)

L'algorithme s'arrête forcément car le reste est positif, et plus petit strictement que $|b|$. Ainsi, les valeurs successives de b sont strictement décroissantes et positives à partir de la première itération. L'entier b finira donc par valoir 0.

Exemple
Déterminez le PGCD de 782 et 221 :

3) Nombres premiers

a) Définition

Définition :

Un entier naturel différent de 1 est un **nombre premier** si et seulement si il n'admet que deux diviseurs : 1 et lui même.

Proposition 1 :

Tout nombre entier peut s'écrire comme un produit de premier (éventuellement : produit avec un seul élément).

▷ *Preuve* :

◁

Propriété 2 :

L'ensemble des nombres premiers est infini.

▷ *Preuve* :

◁

b) Décomposition primaire dans $\mathbb{N}$

Theorème 2 :

Soit $n \in \mathbb{N}^*$, alors il existe $p_1, p_2, \ldots, p_r$ r nombres premiers distincts, et $\alpha_1, \alpha_2, \ldots, \alpha_r$ r entiers non nuls tels que

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$$

De plus, cette écriture est unique à l'ordre des facteurs près.

▷ *Preuve* :
On admet. L'existence provient de la proposition précédente, l'unicité est plus difficile à montrer.
◁

c) Application à la recherche de PGCD et PPCM

Proposition 2 :

Soient $n \in \mathbb{N}$ de décomposition primaire

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$$

Alors les diviseurs de n sont tous les nombres d qui s'écrivent

$$d = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}$$

où pour tout i, β_i est un entier tels que $0 \leq \beta_i \leq \alpha_i$

▷ *Preuve* : On donne ici juste l'idée :

- Tous les nombres de la forme proposés sont des diviseurs.
- Si d est un diviseur de n, alors $n = dc$ avec c un entier. d et c admettent une décomposition primaire, et le produit de cette décomposition primaire doit donner celle de n.
  Comme la décomposition primaire est unique, d est forcément constitué des mêmes nombres premier, éventuellement avec des puissances nulles, et avec des puissances inférieures à celles de n.

◁

Méthode : PPCM et PGCD à partir de la décomposition

Soient a et b deux entiers, de décomposition primaire respectives

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} \text{ et } b = q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s}$$

On suppose que a et b ont t nombres premiers en commun dans leur décomposition. Quitte à renumeroter les nombres, supposons qu'ils ont en communs $p_1, p_2, \dots, p_t$.
Ainsi :

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t} \dots p_{t+1}^{\alpha_{t+1}} \dots p_r^{\alpha_r} \text{ et } b = p_1^{\beta_1} p_2^{\beta_2} \dots p_t^{\beta_t} \dots q_{t+1}^{\beta_{t+1}} \dots q_s^{\beta_s}$$

Alors le PCGD de a et b est donné par

$$a \wedge b = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_t^{\gamma_t} \text{ avec } \forall k \in [\![1, t]\!], \gamma_k = \min(\alpha_k, \beta_k)$$

et le PPCM de a et b est donné par :

$$a \vee b = p_1^{\delta_1} p_2^{\delta_2} \dots p_t^{\delta_t} p_{t+1}^{\alpha_{t+1}} \dots p_r^{\alpha_r} q_{t+1}^{\beta_{t+1}} \dots q_s^{\beta_s} \text{ avec } \forall k \in [\![1, t]\!], \delta_k = \max(\alpha_k, \beta_k)$$

Exemple :
Prenons $a = 5400$ et $b = 1260$
On a

$$a = 2 \times 3^3 \times 4 \times 5^2 \text{ et } b = 3^2 \times 4 \times 5 \times 7$$

II Dénombrement

1) Cardinal

a) Généralités :

Définition :

Soit E un ensemble.
On dit que E est un ensemble fini si et seulement si il existe $n \in \mathbb{N}$ tel qu'il existe une bijection entre E et $[\![1;n]\!]$.
Le nombre n est unique, et est appelé **cardinal** de E, noté $card(E)$ ou $|E|$.

Au secours ! **UNE BIJECTION ?**

La définition peut sembler effrayante, mais elle signifie concrètement qu'on peut numéroter les éléments de E : à chaque élément de E, on associe un entier différent.

Ainsi, dire que E est de cardinal fini permet d'écrire que $E = \{e_1, e_2, \dots e_n\}$ avec tous les e_i distincts.

Le cardinal est tout simplement le nombre d'éléments....

Exemples :

- $E = \{1, 4, 6\}$ est de cardinal .
- $E = [\![0, n]\!]$ est de cardinal
- $E = \{2, 6, -2, 2, 4\}$ est de cardinal
- Si E est l'ensemble des lettres de l'alphabet romain : $card(E) =$
- $card(\emptyset) =$

Remarque :
Une telle écriture n'est pas possible avec des intervalles réels par exemple.

Proposition 3 :

Soit $A \in \mathscr{P}(E)$ (c'est à dire $A \subset E$) où E est un ensemble fini. Alors $card(A) \leq card(E)$.
En outre, si $A \subset E$, et $card(A) = card(E)$, alors $A = E$.

▷ *Preuve* : on admet, c'est intuitivement évident.... ◁

? Le saviez-vous ? — CANTOR VS KRONECKER

Le dénombrement tel que présenté en PCSI est limité au cas du cardinal fini et des entiers. Mais la théorie des ensembles propose de parler de cardinal d'ensembles infinis.
En définissant le cardinal à travers des bijections, Cantor a montré, vers la moitié du XIXème siècle, qu'il y avait "autant" d'entiers naturels que d'entiers relatifs... ou que de nombres rationnels (les fractions). En revanche, $\mathbb{R}$ contient infiniment plus d'éléments : il y aurait donc plusieurs infinis (et même une infinité d'infinis...) !
Une véritable révolution à l'époque qui l'opposa à un grand professeur de mathématiques reconnu, Leopold Kronecker, dont il était un des étudiants...

L'opposition entre les deux mathématiciens est sujette à beaucoup de légendes (comme celle attribuant au jeune Cantor un tag d'insultes contre Kronecker, gravé sur une table de l'université de Berlin) : Kronecker refusait totalement l'avancée notable de Cantor dans ce domaine. Professeur très influent à Berlin, il s'est ainsi opposé à ce que son ancien étudiant obtienne une chaire dans la prestigieuse université....
Tout ceci n'a pas empêché Cantor d'être reconnu comme un génie des mathématiques et un des fondateurs des mathématiques modernes.

b) Méthode élémentaire : arbre des possibilités

Une situation qui se produit très souvent en dénombrement est le comptage via un arbre : cela consiste à décomposer une situation en plusieurs sous situations.
Prenons un exemple : dans un restaurant, le menu "découverte" propose le choix entre 3 entrées, 4 plats principaux et 2 desserts. Combien de repas peut-on faire avec ce menu ?
Faisons un arbre :

On compte alors le nombre de branches à la fin : chaque branche correspond à un repas différent (on dit qu'on a effectué une partition des cas).
On obtient : branches, c'est à dire repas différents.

Remarque :
Très rapidement, on n'essaiera plus de dessiner l'arbre de comptage, car les cas sont vite trop nombreux pour être représentés. Néanmoins, gardez en tête cette représentation pour vous

rappeler qu'il faut multiplier....

2) Opérations sur les ensembles et cardinal :

a) Union

Définition : (rappel)

$A \cup B$ désigne l'ensemble constitué des éléments appartenant à A ou à B, ou au deux.

En maths, l'union est toujours au sens large : A ou B ne veut jamais dire “soit A, soit B”.
Exemple : si $A = \{1, 2, 3\}$ et $B = \{2, 3, 5\}$, 2 est bien un élément de A ou B. De même, 1 est un élément de A ou de B.

Proposition 4 :

Soit A et B deux sous ensembles de E. Alors

$$card(A \cup B) =$$

En particulier, si A et B sont disjoints (ie $A \cap B = \emptyset$), alors

$$card(A \cup B) =$$

▷ *Preuve* : On admet. Le dessin ci dessous donne l'idée, la formaliser est un peu compliqué...

◁

Méthode : SI ON A PLUS DE DEUX ENSEMBLES :

Deux cas :

1. Si les ensembles sont disjoints deux à deux, il suffit de faire la somme des cardinaux.
2. Sinon, il faut "faire des groupes" pour calculer avec la formule

Par exemple $card(A \cup B \cup C) = card((A \cup B) \cup C)$. En appliquant la formule aux deux ensembles $(A \cup B)$ et C on obtient :

On peut d'ailleurs retenir cette formule pour 3 ensembles

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

Au secours ! QUE FAIT-ON DES INTERSECTIONS ?

De manière générale, on ne peux rien dire sur le cardinal de $A \cap B$. Tout juste peut-on écrire

$$card(A \cap B) \leq min(card(A), card(B))$$

Il faut donc, pour calculer $card(A \cap B)$, étudier cas par cas ce qu'il se passe....

b) Complémentaire et différence

Définition : (rappels)

- Soient E un ensemble et $A \subset E$. On appelle complémentaire de A et on note $\bar{A}$ ou A^c l'ensemble des éléments de E qui ne sont pas dans A.
- Soient E un ensemble, $A \subset E$ et $B \subset E$. On appelle différence de A et de B l'ensemble noté $A \setminus B$ constitués des éléments de A qui ne sont pas dans B.
  (En fait, $A \setminus B = A \cap \bar{B}$.)

Propriété 3 :
Soient E un ensemble, $A \subset E$ et $B \subset E$. Alors :

- $card(\bar{A}) = card(E) - card(A)$
- si $B \subset A$, $card(A \setminus B) = card(A) - card(B)$

▷ *Preuve* :

◁

Attention :
Pour la différence, l'hypothèse $B \subset A$ est primordiale !
Par exemple :

c) Produit cartésien

On rappelle les définitions suivantes :

Définition :

- si E et F sont deux ensembles, $E \times F$ désigne l'ensemble des couples formés d'un éléments de E et d'un élément de F, autrement dit

$$E \times F = \{(x, y), x \in E \text{ et } y \in F\}$$

- Pour $p \in \mathbb{N}$, on définit E^p comme l'ensemble des p uplets constitués de p éléments de E, c'est à dire $E^p = \underbrace{E \times E \times ... \times E}_{p \text{ éléments}}$
  En dénombrement et probabilité, on parlera plutôt de p listes d'éléments de E.

A noter : PARENTHÈSES OU ACCOLADES ?
Pour les p listes et les produits cartésiens en général, l'ordre est important. On marque cet ordre en utilisant des parenthèses :
Le couple $(1, 2)$ est différent du couple $(2, 1)$.
En revanche, les accolades désignent l'ensemble des valeurs. Ainsi, $\{1, 2\}$ et $\{2, 1\}$ désigne le même ensemble...

A retenir : parenthèses si l'ordre est important, accolades si l'ordre est indifférent.

Proposition 5 :
Soient E et F deux ensembles finis. Alors $card(E \times F) = card(E) \times card(F)$

▷ *Preuve* :

◁

Corolaire 1 :
Soit $p \in \mathbb{N}$:

(i) Soient $E_1, E_2, \ldots, E_p$ p ensembles finis, alors

$$card(E_1 \times E_2 \times \ldots \times E_p) = card(E_1)card(E_2)\ldots card(E_p)$$

(ii) Soit E un ensemble fini de cardinal n et soit $p \in E$.
Alors il y a n^p $p-$listes d'éléments de E.

▷ *Preuve* :

(i) par récurrence à partir de la proposition précédente.

(ii) les $p-$listes sont les élements de E^p et d'après (i), $card(E^p) = card(E)^p$.

◁

Exemple :
On retourne au restaurant précédent. En notant E l'ensemble des entrées, P l'ensemble des plats et D l'ensemble des desserts, un repas est un élément d'un ensemble R avec

$$R =$$

Il y a donc $card(R)$ repas possibles, et $card(R)$

Méthode :
Lors des problèmes de dénombrement, il ne faut pas hésiter si besoin à introduire d'autres ensembles que ceux proposés dans l'énoncé afin de faire apparaître des ensembles manipulables (union/réunion ou produit cartésien d'ensembles connus...)

3) Applications et cardinal

a) Injection, bijection et surjection :

Proposition 6 :

Soient E et F deux ensembles finis et $f : E \to F$ une application.

- Si f est injective, alors $|E| \quad |F|$
- Si f est surjective, alors $|E| \quad |F|$
- Si f est bijective, alors $|E| \quad |F|$

▷ *Preuve* :

◁

Proposition 7 :

Soient E et F deux ensembles de même cardinal et $f : E \to F$.
Si $|E| = |F|$, alors les assertions suivantes sont équivalentes :

(i) f est injective

(ii) f est bijective

(iii) f est surjective

▷ *Preuve* : (idée) on reprend la preuve précédente en observant à chaque fois que l'on obtient $card(f(E)) = F$ et donc que $f(E) = F$. ◁

Exemple :
On range 5 cravates dans 4 tiroirs, au hasard. Alors il y a forcément un tiroir qui contient deux cravates....

b) Ensemble des applications

Rappel :

Soient E et F deux ensembles. On note F^E l'ensemble des applications de E dans F.

Proposition 8 :

Soient E et F deux ensembles finis non vides. Alors l'ensemble F^E des applications de E dans F est un ensemble fini et on a $card(F^E) = card(F)^{card(E)}$

▷ *Preuve* : Notons $n = |E|$ et $p = |F|$.
Pour construire une application de E dans F, on va choisir pour chaque élément de E son image dans F
Ainsi, chaque élément de E a p possibilités d'image. Comme on a n éléments dans E, on a donc au final $p \times p \times \ldots \times p = p^n$ possibilités.
Il y a donc bien $|F|^{|E|}$ applications possibles entre E et F. ◁

III Listes et combinaisons

1) Listes sans répétition

a) Définition

Exemple :
Lors d'une course hippique, dix chevaux sont partants. Combien de tiercés sont possibles à l'arrivée ?

Ce genre de situation arrivant fréquemment, on pose la définition suivante :

Définition :

Soit un ensemble fini E et $p \in \mathbb{N}$, $p \geq 1$. On appelle p-**listes sans répétition** de E toute p-liste $(e_1, e_2, \ldots, e_p)$ d'éléments de E deux à deux distincts.

Exemples :

- un tiercé est une 3-liste sans répétition.
- Soit $E = \{1, 2, 3, 4, 5, 6\}$: (1,2,3,4),(4,3,2,1) et (1,4,3,2) sont trois listes différentes de 4 éléments de E. $(1, 3, 3)$ n'est pas une liste sans répétition d'éléments de E (mais c'est quand même une $3-$liste.)

Theorème 3 :
Soit E un ensemble fini de cardinal $n \in \mathbb{N}$ et soit $p \in \mathbb{N}$, avec $1 \leq p \leq n$. Le nombre de p-listes de E sans répétition est

$$\frac{n!}{(n-p)!} = \underbrace{n(n-1)\dots(n-p+1)}_{p \text{ facteurs}}$$

▷ *Preuve* :

◁

Remarque : Évidemment, si $p > n$, il n'y a pas de p listes sans répétition possible...

Exemple :
On a vu qu'il y a $|F|^{|E|}$ applications de E dans F... Mais combien y a-t-il d'applications injectives ?

b) Cas particulier : permutations

Définition :

Soit E un ensemble fini et $n = card(E)$.
On appelle **permutation** toute liste de E contenant exactement une fois chaque élément de E. Ainsi, les permutations sont les $n-$listes sans répétition de E.

Exemple :
Les permutations de $E = \{1, 2, 3\}$ sont

Comme donner une permutation d'un ensemble E de cardinal n revient à donner n-liste sans répétition, on a donc directement la formule :

Proposition 9 :

Soit E un ensemble à n éléments. Le nombre de permutations de E est

2) Parties à p éléments (combinaison) :

a) Parties d'un ensemble :

Définition : (rappel)

Soit E un ensemble. On appelle **partie de** E tout sous ensemble de E, et on note $\mathcal{P}(E)$ l'ensemble des parties. Ainsi $A \in \mathcal{P}(E)$ signifie $A \subset E$

Proposition 10 :

Soit E un ensemble fini et $n = card(E)$. Alors $card(\mathcal{P}(E)) = 2^n$.

▷ *Preuve* :

◁

b) Parties à p éléments :

Problème :
On veut faire une équipe de volley (soit 6 joueurs) à partir des 36 élèves de la classe. Cela revient à choisir un sous ensemble de 6 élèves : c'est donc une partie à 6 éléments dans un ensemble constitué de 36 éléments.

Remarque :
L'ordre n'intervient pas ici : on n'est donc pas sur des p listes. Ainsi, l'équipe

$$\{\text{Victor, Louise, Mathilde, Manon, Antoine, Théo}\}$$

est la même que

$$\{\text{Victor, Manon, Theo, Mathilde, Louis, Antoine}\}.$$

Il s'agit bien de sous ensembles, où l'ordre des éléments n'importe pas.

Combien d'équipes est-il possible de faire ?

Définition :

Pour tout $p \in \mathbb{N}$, on appelle p-**combinaison** toute partie à p éléments.

Exemple : Une équipe de volley est une 6-combinaison.

Theorème 4 :

Soit E un ensemble fini à n éléments. Le nombre de partie de p éléments dans E est :

(i) 0 si $p > n$ ou si $p < 0$

(ii) si $0 \leq p \leq n$:

$$\binom{n}{p} = \frac{n!}{p!(n-p)!} = \frac{\overbrace{n \times (n-1) \times \ldots \times (n-p+1)}^{p \text{ termes}}}{p!}$$

$$\text{ou encore : } \binom{n}{p} = \frac{\text{"nombre de } p \text{ listes sans répétition"}}{p!}$$

▷ *Preuve* :

- Le (i) traduit le fait qu'on ne peut pas faire un sous ensemble de p éléments si $p > cardE$

◦ Pour le (ii), commençons par compter les $p-$listes où il n'y a pas de répétitions :

Or plusieurs $p - listes$ correspondent à une même combinaison à p éléments (puisque l'ordre n'a pas d'importance pour les ensembles) : en fait, toutes les permutations d'une liste traduisent le même ensemble.
Il y a $p!$ ordres possibles pour un même ensemble (même preuve que l'exemple de l'équipe), donc on a $p!$ fois trop de représentants, d'où la division par $p!$ et la formule

$$\frac{n!}{p!(n-p)!} = \binom{n}{p}.$$

◁

Astuce... **"P PARMI N"**

Quand on parle du coefficient binomial $\binom{n}{p}$, on lit "p parmi n" : cela correspond bien à la définition de partie à p éléments. On compte le nombre de façons de prendre p éléments parmi les n élements de l'ensemble.

3) Interprétation combinatoire des formules autour des coefficients binomiaux :

a) Propriétés immédiates :

Propriété 4 :
Soit $n \in \mathbb{N}$, soit $p \in \mathbb{N}$ avec $0 \leq p \leq n$:

$$\text{(i)} \binom{n}{0} = 1 \qquad \text{(ii)} \binom{n}{n} = 1 \qquad \text{(iii)} \binom{n}{p} = \binom{n}{n-p}$$

b) Formule du triangle de Pascal

Proposition 11 :

Soit $n \in \mathbb{N}$ et $p \in [\![0, n]\!]$. Alors

$$\binom{n}{p} + \binom{n}{p+1} = \binom{n+1}{p+1}$$

c) Binôme de Newton :

Theorème 5 :

Soient a et b deux complexes et $n \in \mathbb{N}$.

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