La matière pour intra 2 de jeudi prochain est toute la matière couverte jusqu'à mardi passé dans le cours et le TP d'hier. Donc est recapitulatif.

(Sauf quand je l'ai explicitement écrit dans les notes de cours. Par exemple le th. de Fermat ou les preuves des propriétés de $\mathbb{N}$; les propriétés soi-mêmes sont supposées connues.)

En particulier, ce que je ferai aujourd'hui fait partie de l'examen final, mais pas de l'intra 2.

Mardi prochain je vais essayer de vous aider à la préparation à l'intra 2. En particulier vous pouvez poser vos questions en classe (ou en avance par courriel).

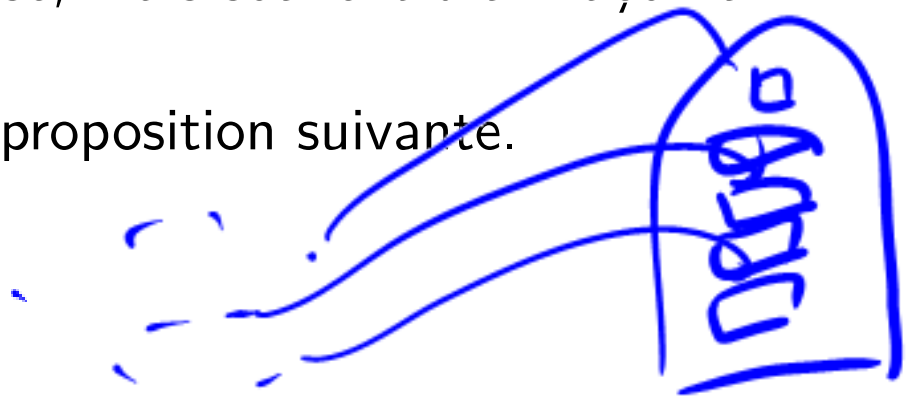
# *Principe des tiroirs de Dirichlet, ou le principe des nids de pigeon*

Considérons un principe très simple.

## Proposition (Principe des tiroirs de Dirichlet)

*Si $m+1$ objets ou plus sont rangés dans $m$ tiroirs, alors il y aura au moins un tiroir qui contient deux objets ou plus.*

Ce principe est régulièrement utilisé, mais souvent d'un façon un peu surprenant.
Une version mathématique est la proposition suivante.

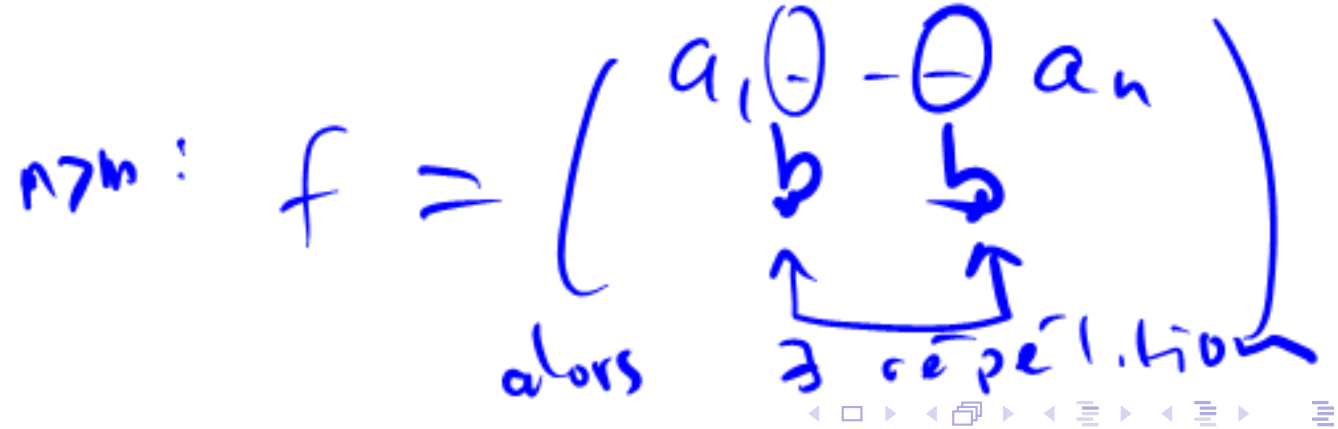


## Proposition

*Soit $f : A \to B$ une fonction entre deux ensembles finis. Posons $n = |A|$ et $m = |B|$.*

*(i) Si $n > m$ alors il existe un $b \in B$ tel que $|f^{-1}(b)| \geq 2$.*

*(ii) Plus généralement, si pour un nombre naturel $r$ on a $n > rm$ alors il existe un $b \in B$ tel que $|f^{-1}(b)| \geq r + 1$.*



Démonstration.

(i) est le cas spécial de (ii) où $r = 1$.

(ii) On a en général

$$|A| = \sum_{b \in B} |f^{-1}(b)|,$$

parce que $A = \bigcup_{b \in B} f^{-1}(b)$ est une union disjointe : $f^{-1}(b) \cap f^{-1}(b') = \emptyset$ et $a \in f^{-1}(f(a))$.

Supposons par contre que $|f^{-1}(b)| \leq r$ pour chaque $b \in B$. Alors

$$n = |A| = \sum_{b \in B} |f^{-1}(b)| \leq |B| r = mr,$$

ce qui est en contradiction avec l'hypothèse $n > rm$. Donc en effet il existe un $b \in B$ tel que $|f^{-1}(b)| \geq r + 1$. □

## Corollaire (Principe des tiroirs de Dirichlet)

*Si $m+1$ objets ou plus sont rangés dans $m$ tiroirs, alors il y aura au moins un tiroir qui contient deux objets ou plus.*

## Démonstration.

Soit $A$ l'ensemble des objets et $B$ l'ensemble des tiroirs. Si l'objet $x$ est rangé dans le tiroir $t$ on écrit $f(x) = t$. Ça donne une fonction $f : A \to B$.

On a $|A| > m$ et $|B| = m$. Donc, par la prop. avant, il existe un $t \in B$ tel que $|f^{-1}(t)| > 2$.

Traduction : dans ce tiroir $t$ on a rangé au moins 2 objets. □

Ex :
On suppose qu'un groupe de pigeons s'envole vers un ensemble de nids pour s'y percher. S'il y a plus de pigeons que de nids, alors il doit y avoir au moins un nid dans lequel se trouvent au moins deux pigeons.

Ex :
Dans un groupe avec au moins 367 personnes, il doit y avoir au moins deux personnes qui ont la même date d'anniversaire.

Exemple :
Dans un groupe avec au moins 241 personnes, il doit y avoir au moins vingt-et-un personnes qui ont dans le même mois leurs anniversaires.

Démonstration.
Soit $A$ l'ensemble des personnes dans ce groupe et $B$ l'ensemble des 12 mois. Si la personne $P$ dans ce groupe est née dans le mois $M$ on écrit $f(P) = M$. C'est une fonction $f : A \to B$. Ici $|A| = 241$ et $|B| = 12$ et $241 > 20 \cdot 12$. Donc il existe un mois $M$ tel que $|f^{-1}(M)| \geq 21$.
C.-à-d., dans ce mois $M$ au moins 21 personnes dans ce groupe a son anniversaire. □

Exemple :
Soit $n > 1$ et $E$ une collection d'au moins $n + 1$ nombres entiers différents. Il existe deux nombres différents dans $E$, disons $a$ et $b$, tels que leur différence $a - b$ est divisible par $n$.

Par exemple : $n = 7$ et l'ensemble de 8 entiers est

$$E = \{123-4567, -345438, 3^7-5^9, 23, 4545^3-1, 93*992, -1000, -238\}$$

La différence de deux des nombres différents dans $E$ est divisible par 7 .

(Mais quels ?)

(Trouver une fonction .....)

Démonstration.

Soit $B = \{m \in \mathbb{N} | 0 \leq m < n\}$. Soit $a \in E$. Il existe un unique $r \in B$ qui est le reste de $a$ après division par $n$ ; posons $f(a) = r$. Ça donne une fonction $f : E \to B$. Ici $|E| > n$ et $|B| = n$. Donc il existe un $r \in B$ tel que $|f^{-1}(r)| \geq 2$.

C.-à-d., il existe deux nombres dans $E$, disons $a$ et $b$, qui ont le même reste $r$ après division par $n$. Donc leur différence $a - b$ est divisible par $n$. □

En général vrai ou faux :

Soit $n > 1$ et $E$ une collection d'au moins $n + 1$ nombres entiers différents. Il existe deux nombres différents dans $E$, disons $a$ et $b$, tels que leur somme $a + b$ est divisible par $n$ ?

La preuve ne fonctionne plus, mais ça ne veut pas dire que c'est faux.

Trouver un contre-exemple ? Avec $n = 2$ pu $n = 3$ ?

$n = 3$ $\quad E = \{1, 4, 7, 10\}$

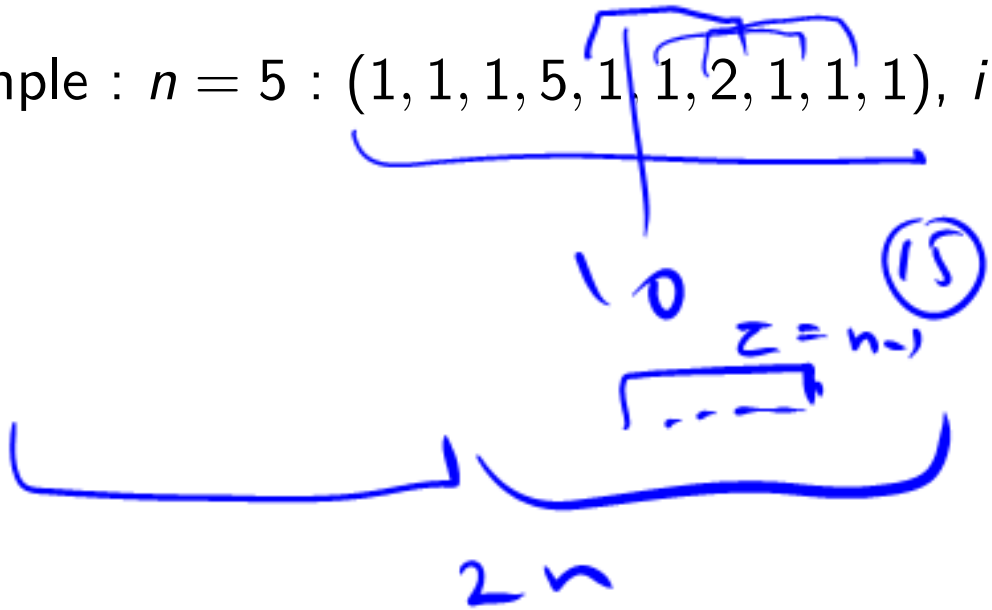
$a, b \in E$ $\quad \forall a \quad a \equiv_3 1$ ici

$a + b \equiv_3 2$

Exemple :

Soit $(a_1, a_2, \ldots, a_{2n})$ une suite de $2n$ nombres naturels (c[redacted]) positifs, et supposons que leurs somme est $\leq 3n$. Alors il existe $i < j$ tel que $a_{i+1} + a_{i+2} + \ldots + a_j = n - 1$.

Exemple : $n = 5$ : $(1, 1, 1, 5, 1, 1, 2, 1, 1, 1)$, $i = 4$ $j = 7$.



(Trouver la fonction, ou les objets/tiroirs, ou les pigeons/nids ....)

**Démonstration.**

Posons $s_i = a_1 + a_2 + \ldots + a_i$. Donc $0 < s_1 < s_2 < \ldots < s_{2n} \leq 3n$. Posons $t_i = s_i + (n-1)$, alors $n-1 < t_1 < t_2 < \ldots < t_{2n} < 4n$. Il y a seulement $4n-1$ "nids" (valeurs entre 1 et $4n-1$) pour les $4n$ "pigeons" (les $s_i$'s et $t_i$'s) : il faut avoir deux "pigeons" sur un même "nid" : il existe un $s_j$ et un $t_i$ tels que $s_j = t_i$. Ou $s_j = s_i + (n-1)$, ou

$$s_j - s_i = a_{i+1} + a_{i+2} + \ldots + a_j = n-1.$$

Exemple :
Soit $E$ un ensemble d'au moins $n+1$ entiers positifs, inférieurs ou égals à $2n$. Il existe un entier dans $E$, disons $a$, qui divise un des autres éléments de $E$, disons $b$ : c.-à-d. $a|b$.

Démonstration.
Chaque nombre $m \in E$ s'écrit uniquement comme $m = 2^e q$, où $e \geq 0$ et $q$ impair (et $0 < q < 2n$). Soit $B$ la collection des nombres positifs impairs, plus petit que $2n$ et $f : E \to B$ la fonction définie par $f(m) = q$. On a $|E| > n$ et $|B| = n$. Donc il existe un $q \in B$ tel que $|f^{-1}(q)| \geq 2$. C.-à-d., il y a deux nombres de la forme $m_1 = 2^{e_1} q$, $m_2 = 2^{e_2} q$ dans $E$. On peut supposer que $e_1 < e_2$. Donc $m_1 | m_2$. ∎

$e_1 < e_2$ $\quad 2^{e_1} | 2^{e_2}$ $\quad 2^{e_1} q \mid 2^{e_2} q$ $\quad m_1 | m_2$

# *Autre principe des tiroirs de Dirichlet.*

Il y a un autre principe qui peut être illustré par les tiroirs de Dirichlet.

**Proposition (Autre principe des tiroirs de Dirichlet)**

*Quelques objets sont rangés dans m tiroirs, tel que chaque tiroir contient exactement n objets. Alors on a rangé nm objets.*

Évident, n'est-ce pas ? !

## Proposition

*Soit $f : A \to B$ une fonction entre deux ensembles finis, tels que pour chaque $b \in B$ on a $|f^{-1}(b)| = n$ Alors $|A| = |B| \cdot n$.*

## Démonstration.

Cette fonction $f$ définit une relation d'équivalence sur $A$ dont chacun des $m = |B|$ classes d'équivalence a $n$ éléments : On a en général

$$|A| = \sum_{b \in B} |f^{-1}(b)|,$$

parce que $A = \bigcup_{b \in B} f^{-1}(b)$ est une union disjointe (une partition). Donc $|A| = |B|n$. □

Démonstration de l'autre principe des tiroirs.

Soit $A$ l'ensemble des objets et $B$ l'ensemble des tiroirs. Si l'objet $x$ est rangé dans le tiroir $t$ on écrit $f(x) = t$. Ça donne une fonction $f : A \to B$. Dans chaque tiroir on a rangé $n$ objets, donc $|f^{-1}(t)| = n$ pour chaque tiroir $t \in B$. On a $m = |B|$. Par la prop. $|A| = mn$, c.-à-d., on a rangé $mn$ objets. $\square$

En conséquence, nous retrouvons

## Corollaire

*Soient $E$ et $F$ deux ensembles finis. Alors $|E \times F| = |E| \times |F|$.*

## Démonstration.

Posons $A = E \times F$ et $f : A \to E$ la fonction définie par $f((x, y)) = x$.
Si $x_0 \in E$, alors $f^{-1}(x_0) = \{(x_0, y) | \ y \in F\}$ est en bijection avec $F$.
Donc $|f^{-1}(x_0)| = |F|$.
Alors par l'autre principe des tiroirs : $|A| = |E| \cdot |F|$. En effet. ☒

Par induction on $m$ on montre (comme la preuve suivante) :

**Corollaire**

*Soit $E$ un ensemble fini et $m \geq 1$. Alors $|E^m| = |E|^m$.*
*C.-à-d., le nombre des suites $(x_1, \ldots, x_m)$, où chaque $x_i \in E$, est $|E|^m$.*

**Corollaire**

*Soit $E$ et $F$ deux ensembles finis. $|E| = m, |F| = n$. Il y a $n^m$ fonctions de $E$ dans $F$.*

**Démonstration.**

Nous avions déjà montré que Fonctions$(E, F)$ est en bijection avec $F^{|E|}$. On conclut. □

## Corollaire

*Soit $E$ un ensemble fini avec $m$ éléments. Le nombre des suites $(x_1, \ldots, x_n)$ où chaque $x_i \in E$ et où tous les $x_i$'s sont différents est $m(m-1)(m-2)\cdots(m-n+1)$.*

*En particulier si $n > m$ il n'existe pas de telles suites.*

## Démonstration.

Preuve par induction sur $n \geq 1$.

Début : Si $n = 1$ c'est trivial.

Étape d'induction : Supposons le résultat est vrai pour $n \geq 1$.

Si $n \geq m$ alors il n'y a pas de telles suites de longueur $n+1$.

Supposons $n < m$.

Soit $A$ l'ensemble des suites $(x_1, \ldots, x_{n+1})$ où chaque $x_i \in E$ et où tous les $x_i$'s sont différents, et $B$ l'ensemble des suites $(y_1, \ldots, y_n)$ où chaque $y_i \in E$ et où tous les $y_i$'s sont différents.

Définissons $f : A \to B$ par $f((x_1, \ldots, x_{n+1})) = (x_1, \ldots, x_n)$.

Soit $b = (y_1, \ldots, y_n) \in B$, alors

$f^{-1}(b) = \{(y_1, \ldots, y_n, x) |\ x \in E - \{y_1, \ldots, y_n\}\}$. Donc

$|f^{-1}(b)| = |E| - n = m - n$

Par la prop. $|A| = |B|(m-n)$ et par induction

$|B| = m(m-1)(m-2)\ldots(m-n+1)$. Donc

$|A| = m(m-1)(m-2)\ldots(m-n+1)(m-n)$.

Donc le résultat est vrai par induction.

## Corollaire

*Soit $E$ et $F$ deux ensembles finis, $|E| = m, |F| = n$.*
*Il y a $n(n-1)(n-2)\cdots(n-m+1)$ fonctions injectives de $E$ dans $F$.*

## Démonstration.

Soit $E = \{x_1, x_2 \ldots, x_m\}$ une enumération fixée des éléments de $E$.
Soit $A$ la collection des suites $(y_1, \ldots, y_m)$ où chaque $y_i \in F$ et où tous les $y_i$'s sont différents.
Soit $B$ la collection de tous les fonctions injectives de $E$ dans $F$.
Soit $a = (y_1, \ldots, y_m) \in A$, et $F_a$ la fonction injective

$$F_a = \begin{pmatrix} x_1 & x_2 & \cdots & x_m \\ y_1 & y_2 & \cdots & y_m \end{pmatrix} \in B$$


Alors $F : A \to B$ définie par $F(a) = F_a$ est bijective.
On conclut $|A| = |B| = n(n-1)(n-2)\cdots(n-m+1)$. □

# *Principe du produit*

L'autre principe des tiroirs est aussi à l'origin d'un principe de comptage de base.

## Proposition

*On suppose qu'une procédure peut être divisée en deux tâches. S'il existe $m$ façons de faire la première tâche et puis $n$ façons d'accomplir la deuxième tâche lorsque la première est terminée, alors il y a $m \cdot n$ façons d'effectuer la procédure.*

## Démonstration du principe du produit.

Soit $B$ l'ensemble des façons de faire la première tâche et $A$ l'ensemble des façons de faire les deux tâches.
La fonction $f : A \to B$ associe à "une façon de faire les deux tâches" : "la première tâche".
Pour une façon donnée de faire la première tâche, il y a toujours $n$ façons d'accomplir la deuxième tâche.
Il suit que les préimages de notre fonction $f$ a toujours $n$ éléments.
Puis on conlut $|A| = |B| \cdot n = mn$. □

# *Principe de la somme*

Il y a aussi un principe de comptage de base additive.

## Proposition

*Si on peut accomplir une tâche de $m$ façons et une deuxième tâche de $n$ façons, et si on ne peut pas effectuer ces tâches simultanément, alors il y a $m + n$ façons d'exécuter l'une ou l'autre de ces tâches.*

La version ensembliste du principe de la somme est (i) de la proposition suivante, que nous connaissons déjà :

## Proposition

*(i) Si on a deux ensembles finis $A$ et $B$ tels que $A \cap B = \emptyset$ alors $|A \cup B| = |A| + |B|$*
*(ii) Supposons on a $r$ ensembles $A_1, A_2, \ldots, A_r$ où $A_i \cap A_j = \emptyset$ si $i \neq j$. Alors*

$$|A_1 \cup A_2 \cup \ldots \cup A_r| = |A_1| + |A_2| + \ldots + |A_r|.$$

## Démonstration du principe de la somme.

Soit $A$ l'ensemble des façons de faire la première tâche et $B$ l'ensemble des façons de faire la deuxième tâche.
"On ne peut pas choisir simultanément" veut dire que $A \cap B$ est vide. Choisir un élément de $A$ ou un élément de $B$ est la même chose qu'exécuter un des deux tâches.
Donc on veut savoir $|A \cup B|$. Par le principe précédent, c'est égal à $|A| + |B|$. □

Avec ces deux principes de comptage on peut briser des problèmes de comptage en sous-problèmes.

Comme une proposition logique peut être composé de propositions plus simples en utilisant $\vee, \wedge, \neg$.

Dans un café on peut acheter 6 sortes de muffin, 7 sortes de boisson chaud et 5 sortes de boisson froid. Combien de façons de choisir un boisson et un muffin ?

Il y a deux tâches : choisir un boisson et puis choisir un muffin.
Première tâche est choisir un boisson, c.-à-d., choisir un boisson chaud ou un boisson froid. Selon le principe de la somme :
$7 + 5 = 12$ façons de choisir un boisson.
N'importe le choix du boisson, il y aura toujours 6 façons de choisir le muffin. Donc par le principe du produit : en total
$(7 + 5) \cdot 6 = 72$ façons de choisir un boisson et un muffin.

# Compter

Si on a une collection d'objets, on veut souvent faire quelque chose avec ça.
Disons : énumerer les objets systématiquement ou les compter, ou les classifier selon un certain principe et puis énumerer ou compter les objets dans les classes différents.
On le fait par exemple pour le besoin d'estimer une probabilité que quelque chose arrivera.

Nous allons donner quelques cas typiques de comptage et un peu comment on peut reconnaître ces cas et les appliquer.

Souvent il y a des différences subtiles entre une analyse d'une situation pratique donnée et une autre analyse un peu semblable mais différente ; mais pas tous les deux sont bonnes.
Une raison est que dans la vraie vie certains hypothèses sont cachées, il faut les découvrir en posant des questions !

Ou on peut aussi avoir deux méthodes différentes pour compter la même collection, et tous les deux correctes ! Utile !

La clef pour avoir du succès est de reformuler les vraies problèmes en termes de constructions avec des ensembles et des fonctions.

Dans la vraie vie, selon Alexandre Dumas :
*Cherchez la femme, pardieu ! cherchez la femme !*

Pour la modélisation discrète :
*Cherchez l'ensemble, pardieu ! et cherchez la fonction !*

Exemple : Description d'un "jeu" entre deux joueurs $A$ et $B$.

Chacun lance un dé ordinaire de six côtés. Supposons que celui de $A$ a valeur $a$ et celui de $B$ a valeur $b$.
Joueur $A$ gagne si $a > b$ et $B$ doit payer \$4 à $A$.
Joueur $B$ gagne si $a \leq b$ et $A$ doit payer \$3 à $B$.

Puis on répète beaucoup de fois. C'est plus facile pour $B$ de gagner une partie, mais il gagnerait moins d'argent.

Qui a l'avantage à long terme ?

Nous allons énumérer tous les résultats $(a, b)$ d'une lance de dé de chaque joueur.

$$\begin{array}{cccccc}
(1,1) & (1,2) & (1,3) & (1,4) & (1,5) & (1,6) \\
(2,1) & (2,2) & (2,3) & (2,4) & (2,5) & (2,6) \\
(3,1) & (3,2) & (3,3) & (3,4) & (3,5) & (3,6) \\
(4,1) & (4,2) & (4,3) & (4,4) & (4,5) & (4,6) \\
(5,1) & (5,2) & (5,3) & (5,4) & (5,5) & (5,6) \\
(6,1) & (6,2) & (6,3) & (6,4) & (6,5) & (6,6)
\end{array}$$

Il y a 6 possibilités pour chaque dé, et en total $6 \cdot 6 = 36$, comme on voit. Chaque cas à la même "probabilité" de $\frac{1}{36}$.

Les cas favorables pour $B$ sont

$$\begin{array}{cccccc} (1,1) & (1,2) & (1,3) & (1,4) & (1,5) & (1,6) \\ & (2,2) & (2,3) & (2,4) & (2,5) & (2,6) \\ & & (3,3) & (3,4) & (3,5) & (3,6) \\ & & & (4,4) & (4,5) & (4,6) \\ & & & & (5,5) & (5,6) \\ & & & & & (6,6) \end{array}$$

Donc en total il y a 21 cas favorable pour $B$. Donc la "probabilité" que $B$ gagne une partie est $\frac{21}{36} = 0,583333...$.
Il y a $36 - 21 = 15$ cas favorable pour $A$. La "probabiilité" que $A$ gagne une partie est $\frac{15}{36} = 0,416666...$.

Si on joue beaucoup de parties, disons 1000, on prévoit que $B$ va gagner environ $58,33\%$ des parties et $A$ environ $41,67\%$ des parties.

Donc $B$ gagne environ $583,3 \cdot \$3 = \$1750$ et il perd seulement environ $416,7 \cdot \$4 = \$1667$.
L'avantage est pour $B$ à long terme.

Dans la formulation de ce problème il n'y avait pas d'ensemble.

Mais dans l'analyse nous avons utilisé l'ensemble des cas possibles (qui est un produit cartésien de deux ensembles de 6 éléments chacun) et une partition en deux sous-ensembles (les cas favorables pour $B$, respectivement pour $A$).

Et les fractions des tailles des sous-ensembles par rapport à l'ensemble total nous donnait les deux "probabilités" qui nous servaient après.