DEVOIR SURVEILLÉ 3

(durée : 4 h 00)

Rédigez vos réponses dans un français correct. Terminez chaque résolution d'exercice par une conclusion $\boxed{\text{encadrée}}$ *ou* *soulignée*. *Laissez une marge au correcteur.*

Les exercices sont indépendants et peuvent être traités dans n'importe quel ordre. Dans un exercice avec plusieurs questions, on pourra, si besoin est, admettre le résultat d'une question pour répondre aux suivantes.

La calculatrice n'est pas autorisée.

EXERCICE 1

Lemme des mariages

Soient F et G deux ensembles tels que F est fini et non vide. On considère une fonction $\varphi : F \longrightarrow \mathscr{P}(G)$. Pour toute partie A de F, on pose $\varphi[A] = \bigcup_{x\in A} \varphi(x)$. On souhaite démontrer le *théorème de Hall* :

$$\begin{pmatrix} \text{il existe une injection } m \text{ de } F \text{ dans } G \\ \text{telle que } \forall x \in F,\ m(x) \in \varphi(x) \end{pmatrix} \iff \Big(\forall A \in \mathscr{P}(F),\ \ \operatorname{card}\varphi[A] \geqslant \operatorname{card} A\Big).$$

1. Démontrer l'implication directe $\Longrightarrow$.
2. Nous allons maintenant démontrer l'implication réciproque $\Longleftarrow$. On suppose par conséquent que $\forall A \in \mathscr{P}(F),\ \operatorname{card}\varphi[A] \geqslant \operatorname{card} A$.
   a) Soit $x_0 \in F$. Démontrer que $\varphi(x_0) \neq \varnothing$.
   b) On suppose que $\forall A \in \mathscr{P}(F)\setminus\{\varnothing, F\},\ \operatorname{card}\varphi[A] > \operatorname{card} A$. On fixe $x_0 \in F$ et $y_0 \in \varphi(x_0)$. On considère
   $$\psi \left\{ \begin{array}{ccc} F \setminus \{x_0\} & \longrightarrow & \mathscr{P}(G \setminus \{y_0\}) \\ x & \longmapsto & \varphi(x) \setminus \{y_0\} \end{array} \right.$$
   Démontrer que $\forall A \in \mathscr{P}(F \setminus \{x_0\}),\ \operatorname{card}\psi[A] \geqslant \operatorname{card} A$.
   c) On suppose qu'il existe $A_0 \in \mathscr{P}(F) \setminus \{\varnothing, F\}$ tel que $\operatorname{card}\varphi[A_0] = \operatorname{card} A_0$. On pose
   $$\theta \left\{ \begin{array}{ccc} F \setminus A_0 & \longrightarrow & \mathscr{P}(G \setminus \varphi[A_0]) \\ x & \longmapsto & \varphi(x) \setminus \varphi[A_0] \end{array} \right.$$
   α] Démontrer que $\forall A \in \mathscr{P}(F \setminus A_0),\ \operatorname{card}\theta[A] + \operatorname{card} A_0 = \operatorname{card}\varphi[A \cup A_0]$.
   β] Démontrer que $\forall A \in \mathscr{P}(F \setminus A_0),\ \operatorname{card}\theta[A] \geqslant \operatorname{card} A$.
   d) Démontrer qu'il existe une injection m de F dans G telle que $\forall x \in F,\ m(x) \in \varphi(x)$.
3. Le théorème de Hall est aussi appelé *le lemme des mariages*. Expliquer pourquoi.
4. On distribue un jeu de 52 cartes en treize paquets de 4 cartes chacun. Démontrer qu'il est toujours possible d'ordonner ces paquets de sorte que le premier paquet contienne un as, le second un 2, le troisième un 3, et ainsi de suite jusqu'au treizième paquet qui contient un roi.

EXERCICE 2

Moyenne quadratique de la discrépance

Soit Ω un ensemble fini. Pour toutes parties A et X de Ω, on appelle *discrépance* entre A et X l'entier naturel $\Delta(A, X)$ défini par

$$\Delta(A, X) = |\operatorname{card}(A \cap X) - \operatorname{card}(A \cap \overline{X})|.$$

1. Soient A et X deux parties de Ω et a un élément de Ω.
   a) $\alpha]$ Calculer $\Delta(\varnothing, X)$, $\Delta(\{a\}, X)$ et $\Delta(A, \varnothing)$.
      $\beta]$ Démontrer que $\Delta(A, X)$ est un entier de l'intervalle $[\![0; \operatorname{card} A]\!]$, de même parité que $\operatorname{card} A$.
   b) Démontrer que $\Delta(A, X) = \Delta(A, A \cap X)$.
   c) Démontrer que $\Delta(A, X) = \Delta(A, A \setminus X)$. Que vaut $\Delta(A, A)$?
2. Soit A une partie de Ω.
   a) Démontrer que
   $$\frac{1}{\operatorname{card} \mathscr{P}(A)} \sum_{X \in \mathscr{P}(A)} \operatorname{card} X = \frac{\operatorname{card} A}{2}$$
   et
   $$\frac{1}{\operatorname{card} \mathscr{P}(A)} \sum_{X \in \mathscr{P}(A)} (\operatorname{card} X)^2 = \frac{(\operatorname{card} A)(\operatorname{card} A + 1)}{4}.$$
   b) En déduire que
   $$\frac{1}{\operatorname{card} \mathscr{P}(A)} \sum_{X \in \mathscr{P}(A)} \Delta(A, X)^2 = \operatorname{card} A.$$
3. Soit A une partie de Ω.
   a) Démontrer que l'application
   $$\varphi \begin{cases} \mathscr{P}(\Omega) & \longrightarrow & \mathscr{P}(A) \times \mathscr{P}(\overline{A}) \\ X & \longmapsto & (X \cap A, X \cap \overline{A}) \end{cases}$$
   est une bijection.
   b) Démontrer que
   $$\frac{1}{\operatorname{card} \mathscr{P}(\Omega)} \sum_{X \in \mathscr{P}(\Omega)} \Delta(A, X)^2 = \operatorname{card} A.$$
4. Soit $(A_1, \ldots, A_p)$ une partition de Ω. Pour toute partie X de Ω, on appelle *discrépance* entre $(A_1, \ldots, A_p)$ et X l'entier naturel $\Delta(A_1, \ldots, A_p, X)$ défini par
   $$\Delta(A_1, \ldots, A_p, X) = \sqrt{\sum_{k=1}^{p} \Delta(A_k, X)^2}.$$
   Démontrer que
   $$\frac{1}{\operatorname{card} \mathscr{P}(\Omega)} \sum_{X \in \mathscr{P}(\Omega)} \Delta(A_1, \ldots, A_p, X)^2 = \operatorname{card} \Omega.$$

EXERCICE 3

Anneau quotient

Soit A un anneau commutatif. Une partie X de A est appelée un *idéel* de A lorsqu'il existe un élément x de A et un idéal I de A tel que $X = x + I$ (c'est-à-dire $X = \{x + i : i \in I\}$).

1. a) Parmi les propositions suivantes, reconnaître (en justifiant) les idéels :
   - ▷ $\varnothing$;
   - ▷ les idéaux de A ;
   - ▷ les singletons de A ;
   - ▷ les sous-anneaux de A.

   b) Quels sont les idéels de $\mathbb{Z}$?

2. Soit X un idéel de A. On considère un élément x de A et un idéal I de A tel que $X = x + I$.

   a) Démontrer que $x \in X$. Réciproquement, démontrer que, si $y \in X$, alors $X = y + I$.

   b) On suppose qu'il existe un élément y de A et un idéal J de A tel que $X = y + J$. Démontrer que $x - y \in I$ et $J = I$.

   ► On dit que I est la *direction* de X.

3. Démontrer qu'un idéel est un idéal si, et seulement si, il contient 0_A.

4. a) Démontrer qu'une intersection (quelconque) d'idéels de A est ou bien vide ou bien un idéel de A.

   b) Démontrer qu'une somme de deux idéels de A est un idéel de A.

5. Soit $\varphi : A \longrightarrow A'$ un morphisme d'anneaux commutatifs.

   a) α] Soit X un idéel de A. Démontrer que $\varphi(X)$ est un idéel de l'anneau $\varphi(A)$.

      β] Soit X' un idéel de A'. Démontrer que $\varphi^{-1}(X')$ est ou bien vide ou bien un idéel de A.

   b) Pour tout $x' \in A'$, on pose $\text{Ben}(\varphi, x') = \{a \in A : \varphi(a) = x'\} = \varphi^{-1}(\{x'\})$.

      α] Reconnaître $\text{Ben}(\varphi, 0_{A'})$.

      β] Justifier que, pour tout $x' \in A'$, $\text{Ben}(\varphi, x')$ est ou bien vide ou bien un idéel de A dont on précisera la direction.

      γ] Démontrer que φ est injectif si, et seulement si, il existe un élément x' de A' tel que $\text{Ben}(\varphi, x')$ est un singleton.

6. Soit I un idéal de A. Sur A, on définit la relation de *congruence modulo* I, notée $\equiv [I]$, par $\forall a, b \in A,\ (a \equiv b\ [I]) \Leftrightarrow (b - a \in I)$.

   a) Vérifier que $\equiv [I]$ est un relation d'équivalence sur A.

   b) Soit $x \in A$. Démontrer que la classe d'équivalence de x modulo la relation $\equiv [I]$ est l'idéel $x + I$.

   ► On note $A/_I$ l'ensemble quotient de A par la relation d'équivalence $\equiv [I]$. La question précédente nous dit que $A/_I = \{x + I : x \in A\}$, c'est-à-dire que $A/_I$ est l'ensemble des idéels de A dont la direction est I.

   Sur $A/_I$, on considère l'addition et la multiplication définies, pour tous éléments $x + I$ et $y + I$ de $A/_I$, par

   $$(x + I) + (y + I) = (x + y) + I \qquad \text{et} \qquad (x + I)(y + I) = xy + I.$$

   c) Justifier que l'addition et la multiplication sur $A/_I$ sont bien définies et démontrer que $A/_I$, muni de ces lois, est un anneau commutatif.

   d) On dit que I est un idéal *maximal* lorsque $I \neq A$ et I n'est inclus que dans deux idéaux : lui-même et A.

   Démontrer que $A/_I$ est un corps si, et seulement si, I est maximal.

CORRECTION DU DS 3

(durée : 4 h 00)

EXERCICE 1

Soient F, G deux ensembles tels que F est fini et non vide. On considère une fonction $\varphi : F \longrightarrow \mathscr{P}(G)$. Pour toute partie A de F, on pose $\varphi[A] = \bigcup_{x\in A}\varphi(x)$. On souhaite démontrer qu'il existe une injection m de F dans G telle que $\forall x \in F,\ m(x) \in \varphi(x)$ si, et seulement si, $\forall A \in \mathscr{P}(F),\ \operatorname{card}\varphi[A] \geqslant \operatorname{card} A$. C'est le théorème de Hall.

1. *Démontrer l'implication directe $\Longrightarrow$.*

   Supposons qu'il existe une injection m de F dans G telle que $\forall x \in F,\ m(x) \in \varphi(x)$. Démontrons que $\forall A \in \mathscr{P}(F),\ \operatorname{card}\varphi[A] \geqslant \operatorname{card} A$.
   Soit $A \in \mathscr{P}(F)$.
   Comme $m(x) \in \varphi(x)$ pour tout $x \in F$, on sait a fortiori que $\forall x \in A,\ m(x) \in \varphi(x)$. Il s'ensuit que $m(A) \subset \varphi[A]$.
   Or m est injective donc $\operatorname{card} m(A) = \operatorname{card} A$. Cela implique que $\operatorname{card}\varphi[A] \geqslant \operatorname{card} A$.
   En conclusion,

   $$\boxed{\text{la condition } (\forall A \in \mathscr{P}(F),\ \operatorname{card}\varphi[A] \geqslant \operatorname{card} A) \text{ est nécessaire à l'existence d'une injection } m \text{ de } F \text{ dans } G \text{ telle que } \forall x \in F,\ m(x) \in \varphi(x).}$$

2. *Démontrons l'implication réciproque $\Longleftarrow$. On suppose que $\forall A \in \mathscr{P}(F),\ \operatorname{card}\varphi[A] \geqslant \operatorname{card} A$.*

   a) *Soit $x_0 \in F$. Démontrer que $\varphi(x_0) \neq \varnothing$.*

   En appliquant l'hypothèse $\forall A \in \mathscr{P}(F),\ \operatorname{card}\varphi[A] \geqslant \operatorname{card} A$ avec $A = \{x_0\}$, on obtient $\operatorname{card}\varphi[\{x_0\}] \geqslant 1$. Or $\varphi[\{x_0\}] = \varphi(x_0)$, donc $\operatorname{card}\varphi(x_0) \geqslant 1$, c'est-à-dire

   $$\boxed{\varphi(x_0) \neq \varnothing.}$$

   b) *On suppose que $\forall A \in \mathscr{P}(F) \setminus \{\varnothing, F\},\ \operatorname{card}\varphi[A] > \operatorname{card} A$. On fixe $x_0 \in F$ et $y_0 \in \varphi(x_0)$. On considère $\psi : F \setminus \{x_0\} \to \mathscr{P}(G \setminus \{y_0\})$ telle que $\forall x \in F \setminus \{x_0\},\ \psi(x) = \varphi(x) \setminus \{y_0\}$. Démontrer que $\forall A \in \mathscr{P}(F \setminus \{x_0\}),\ \operatorname{card}\psi[A] \geqslant \operatorname{card} A$.*

   Soit $A \in \mathscr{P}(F \setminus \{x_0\})$. Alors $A \in \mathscr{P}(F) \setminus \{F\}$, ce qui permet d'utiliser l'hypothèse de cette question pour affirmer que $\operatorname{card}\varphi[A] > \operatorname{card} A$. Or

   $$\psi[A] = \bigcup_{x\in A}\psi(x) = \bigcup_{x\in A}\left(\varphi(x) \setminus \{y_0\}\right) = \Big(\bigcup_{x\in A}\varphi(x)\Big) \setminus \{y_0\} = \varphi[A] \setminus \{y_0\},$$

   donc

   $$\operatorname{card}\psi[A] \geqslant \operatorname{card}\varphi[A] - 1,$$

   ce qui donne

   $$\operatorname{card}\psi[A] > \operatorname{card} A - 1$$

   ou encore

   $$\operatorname{card}\psi[A] \geqslant \operatorname{card} A.$$

   On a ainsi démontré que

   $$\boxed{\forall A \in \mathscr{P}(F \setminus \{x_0\}), \qquad \operatorname{card}\psi[A] \geqslant \operatorname{card} A.}$$

c) *On suppose qu'il existe* $A_0 \in \mathscr{P}(F) \setminus \{\varnothing, F\}$ *tel que* $\operatorname{card} \varphi[A_0] = \operatorname{card} A_0$. *On considère* $\theta : F \setminus A_0 \to \mathscr{P}(G \setminus \varphi[A_0])$ *telle que* $\forall x \in F \setminus A_0,\ \theta(x) = \varphi(x) \setminus \varphi[A_0]$.

α] *Démontrer que* $\forall A \in \mathscr{P}(F \setminus A_0),\ \operatorname{card} \theta[A] + \operatorname{card} A_0 = \operatorname{card} \varphi[A \cup A_0]$.

Soit $A \in \mathscr{P}(F \setminus A_0)$. On a

$$\begin{aligned}
\operatorname{card} \theta[A] + \operatorname{card} A_0 &= \operatorname{card} \theta[A] + \operatorname{card} \varphi[A_0] && \text{car } \operatorname{card} \varphi[A_0] = \operatorname{card} A_0 \\
&= \operatorname{card}(\theta[A] \cup \varphi[A_0]) && \text{car } \theta[A] \text{ et } \varphi[A_0] \text{ sont disjoints} \\
& && \text{puisque } \theta[A] \in \mathscr{P}(G \setminus \varphi[A_0]) \\
&= \operatorname{card}\Big[\Big(\bigcup_{x \in A} \theta(x)\Big) \cup \varphi[A_0]\Big] \\
&= \operatorname{card}\Big[\Big(\bigcup_{x \in A} \varphi(x) \setminus \varphi[A_0]\Big) \cup \varphi[A_0]\Big] \\
&= \operatorname{card}\Big[\Big(\bigcup_{x \in A} \varphi(x)\Big) \cup \varphi[A_0]\Big] \\
&= \operatorname{card}\Big[\Big(\bigcup_{x \in A} \varphi(x)\Big) \cup \Big(\bigcup_{x \in A_0} \varphi(x)\Big)\Big] \\
&= \operatorname{card}\Big[\bigcup_{x \in A \cup A_0} \varphi(x)\Big] \\
&= \operatorname{card} \varphi[A \cup A_0].
\end{aligned}$$

Donc

$$\boxed{\forall A \in \mathscr{P}(F \setminus A_0), \qquad \operatorname{card} \theta[A] + \operatorname{card} A_0 = \operatorname{card} \varphi[A \cup A_0].}$$

β] *Démontrer que* $\forall A \in \mathscr{P}(F \setminus A_0),\ \operatorname{card} \theta[A] \geqslant \operatorname{card} A$.

Soit $A \in \mathscr{P}(F \setminus A_0)$. En appliquant l'hypothèse $\forall A \in \mathscr{P}(F),\ \operatorname{card} \varphi[A] \geqslant \operatorname{card} A$ à la partie $A \cup A_0$, on obtient

$$\operatorname{card} \varphi[A \cup A_0] \geqslant \operatorname{card}(A \cup A_0).$$

Comme A et A_0 sont disjoints, il s'ensuit que

$$\operatorname{card} \varphi[A \cup A_0] \geqslant \operatorname{card} A + \operatorname{card} A_0.$$

En tenant compte de cette inégalité dans le résultat de la question précédente, on obtient

$$\operatorname{card} \theta[A] + \operatorname{card} A_0 \geqslant \operatorname{card} A + \operatorname{card} A_0,$$

ce qui donne

$$\operatorname{card} \theta[A] \geqslant \operatorname{card} A.$$

En conclusion, on a

$$\boxed{\forall A \in \mathscr{P}(F \setminus A_0), \qquad \operatorname{card} \theta[A] \geqslant \operatorname{card} A.}$$

d) *Démontrer qu'il existe une injection* m *de* F *dans* G *telle que* $\forall x \in F,\ m(x) \in \varphi(x)$.

On procède par récurrence forte sur le cardinal n de F. Pour $n \in \mathbb{N}^*$, on note $\mathscr{P}(n)$ l'assertion « pour tout ensemble F de cardinal n, tout ensemble G et toute application $\varphi : F \longrightarrow \mathscr{P}(G)$ telle que $\forall A \in \mathscr{P}(F),\ \operatorname{card} \varphi[A] \geqslant \operatorname{card} A$, il existe une injection m de F dans G telle que $\forall x \in F,\ m(x) \in \varphi(x)$ ».

<u>Initialisation</u>

Supposons que F est un singleton, c'est-à-dire $F = \{x_0\}$. Prenons G un ensemble quelconque et $\varphi : F = \{x_0\} \longrightarrow \mathscr{P}(G)$ telle que $\forall A \in \mathscr{P}(F),\ \operatorname{card} \varphi[A] \geqslant \operatorname{card} A$. On a vu, à la question a), que $\varphi(x_0) \neq \varnothing$. Cela permet d'introduire y_0, un élément de $\varphi(x_0)$. On définit alors $m : F = \{x_0\} \longrightarrow G$ en posant $m(x_0) = y_0$. C'est clairement une injection. Donc $\mathscr{P}(1)$ est vraie.

<u>Hérédité</u>

Fixons $n \in \mathbb{N}^*$ tel que $\mathscr{P}(1), \mathscr{P}(2), \ldots, \mathscr{P}(n)$ sont vraies et démontrons $\mathscr{P}(n+1)$. Soit F un ensemble de cardinal $n+1$, G un ensemble quelconque et $\varphi : F \longrightarrow \mathscr{P}(G)$ telle que $\forall A \in \mathscr{P}(F),\ \operatorname{card} \varphi[A] \geqslant \operatorname{card} A$. On distingue deux cas :

▷ Premier cas : $\forall A \in \mathscr{P}(F) \setminus \{\varnothing, F\},\ \operatorname{card}\varphi[A] > \operatorname{card} A$
Comme à la question b), on fixe $x_0 \in A$ et $y_0 \in \varphi(x_0)$ puis on introduit l'application $\psi : F \setminus \{x_0\} \longrightarrow \mathscr{P}(G \setminus \{y_0\})$ telle que $\forall x \in F \setminus \{x_0\},\ \psi(x) = \varphi(x) \setminus \{y_0\}$. On a vu que ψ vérifie alors la condition $\forall A \in \mathscr{P}(F \setminus \{x_0\}),\ \operatorname{card}\psi[A] \geqslant \operatorname{card} A$.
Comme $\operatorname{card}(F \setminus \{x_0\}) = n$, on peut utiliser l'hypothèse de récurrence $\mathscr{P}(n)$ pour affirmer l'existence d'une injection m de $F\setminus\{x_0\}$ dans $G\setminus\{y_0\}$ telle que $\forall x \in F\setminus\{x_0\},\ m(x) \in \psi(x)$.
On prolonge alors m à F tout entier en posant $m(x_0) = y_0$ (abusivement, on continue d'appeler m ce prolongement). On obtient une injection m de F dans G.
Si $x \in F \setminus \{x_0\}$, on a $m(x) \in \psi(x)$ et donc $m(x) \in \varphi(x)$ puisque $\psi(x) \subset \varphi(x)$.
Si $x = x_0$, on a $m(x) = y_0 \in \varphi(x_0)$ par définition de y_0.
L'application m est donc une injection de F dans G telle que $\forall x \in F,\ m(x) \in \varphi(x)$.
Dans ce cas, $\mathscr{P}(n+1)$ est donc vraie.

▷ Second cas : $\exists A_0 \in \mathscr{P}(F) \setminus \{\varnothing, F\},\ \operatorname{card}\varphi[A] = \operatorname{card} A$
Comme à la question c), on introduit l'application $\theta : F \setminus A_0 \longrightarrow \mathscr{P}(G \setminus \varphi[A_0])$ définie par $\forall x \in F \setminus A_0,\ \theta(x) = \varphi(x) \setminus \varphi[A_0]$. On a démontré que θ vérifie alors la condition $\forall A \in \mathscr{P}(F \setminus A_0),\ \operatorname{card}\theta[A] \geqslant \operatorname{card} A$.
Comme $\operatorname{card}(F \setminus A_0) = n - \operatorname{card} A_0 \in [\![1; n]\!]$, on peut utiliser l'hypothèse de récurrence $\mathscr{P}(n - \operatorname{card} A_0)$ pour affirmer l'existence d'une injection m de $F \setminus A_0$ dans $G \setminus \varphi[A_0]$ telle que $\forall x \in F \setminus A_0,\ m(x) \in \theta(x)$.
Par ailleurs, on considère λ, la restriction de φ à A_0 au départ et $\varphi[A_0]$ à l'arrivée. Si $A \in \mathscr{P}(A_0)$, alors $\operatorname{card}\lambda[A] = \operatorname{card}\varphi[A] \geqslant \operatorname{card} A$, ce qui démontre que λ satisfait la condition $\forall A \in \mathscr{P}(A_0),\ \operatorname{card}\lambda[A] \geqslant \operatorname{card} A$.
Comme $\operatorname{card}(A_0) \in [\![1; n]\!]$, on peut utiliser l'hypothèse de récurrence $\mathscr{P}(\operatorname{card} A_0)$ pour affirmer l'existence d'une injection ℓ de A_0 dans $\varphi[A_0]$ telle que $\forall x \in A_0,\ \ell(x) \in \lambda(x)$.
On prolonge alors m à F tout entier en posant $m(a) = \ell(a)$ pour tout $a \in A_0$ (abusivement, on continue d'appeler m ce prolongement). On obtient une injection m de F dans G.
Si $x \in F \setminus A_0$, on a $m(x) \in \theta(x)$ et donc $m(x) \in \varphi(x)$ puisque $\theta(x) \subset \varphi(x)$.
Si $x \in A_0$, on a $m(x) = \ell(x) \in \lambda(x) = \varphi(x)$ puisque λ est la restriction de φ sur A_0.
L'application m est donc une injection de F dans G telle que $\forall x \in F,\ m(x) \in \varphi(x)$.
Dans ce cas, $\mathscr{P}(n+1)$ est donc vraie.

Dans tous les cas, on a donc démontré que $\mathscr{P}(n+1)$ est vraie.

<u>Hérédité</u>

D'après le principe de récurrence, $\mathscr{P}(n)$ est vraie pour tout $n \in \mathbb{N}^*$. Autrement dit,

> la condition ($\forall A \in \mathscr{P}(F),\ \operatorname{card}\varphi[A] \geqslant \operatorname{card} A$) est suffisante à l'existence d'une injection m de F dans G telle que $\forall x \in F,\ m(x) \in \varphi(x)$.

3. *Le théorème de Hall est aussi appelé le lemme des mariages. Expliquer pourquoi.*

Voici l'interprétation cupidonesque de ce théorème. On suppose que F désigne un ensemble de filles, que G est un ensemble de garçons et que φ est le nom de l'application qui à chaque fille associe l'ensemble des garçons qui lui plaisent. Le sens réciproque du théorème de Hall nous dit que

> si pour chaque sous-ensemble de filles, le nombre de garçons qui leur plaisent est plus grand que le nombre de filles de ce sous-ensemble, alors il est possible de marier chaque fille à un garçon qui lui plait.

Bien sûr, on peut échanger le rôle des filles et des garçons !

Remarque culturelle :

Le lemme des mariages (une variante pour être honnête) est utilisé pour attribuer les places des écoles d'ingénieurs aux différents candidats des concours. Notons G l'ensemble des places disponibles et F l'ensemble des candidats. Pour toute place $x \in G$, $\varphi(x)$ est la liste des candidats admissibles visant cette place. On retrouve la situation du lemme des mariages. Ainsi, chaque concours doit mettre suffisamment de candidats sur sa liste d'admissibles pour être sûr que la condition du mariage soit vérifiée.
De plus, on peut noter que la démonstration que nous avons faite du théorème de Hall est constructive : elle donne un algorithme de calcul de la fonction de mariage m, qui décide quel candidat ira dans quelle école. Chose amusante, cet algorithme contient une part d'aléatoire : deux élèves ayant eu exactement les mêmes résultats n'iront pas forcément dans la même école.

4. *On distribue un jeu de 52 cartes en treize paquets de 4 cartes chacun. Démontrer qu'il est toujours possible d'ordonner ces paquets de sorte que le premier paquet contienne un as, le second un 2, le troisième un 3, et ainsi de suite jusqu'au treizième paquet qui contient un roi.*

   Évidemment, il faut utiliser le lemme des mariages. Mais qui sont les filles ? qui sont les garçons ? et pourquoi la condition du mariage est-elle satisfaite ?

   Notons F l'ensemble des treize paquets de 4 cartes et $G = [\![1;13]\!]$. En outre, considérons l'application $\varphi : F \longrightarrow \mathscr{P}(G)$ qui à un paquet de 4 cartes associe la partie (à quatre éléments) rassemblant les numéros des 4 cartes du paquet (avec la convention que 11 désigne un valet, 12 une dame et 13 un roi).

   Pour tout $k \in [\![0;13]\!]$, si l'on se donne k paquets de 4 cartes, il est clair qu'il y a au moins k numéros de cartes différents (car, dans un jeu, il y a 4 cartes pour chaque numéro). La condition du mariage $\forall A \in \mathscr{P}(F),\ \operatorname{card} \varphi[A] \geqslant \operatorname{card} A$ est donc vérifiée.

   D'après le lemme des mariages, il existe ainsi une injection m de F dans G, ce qui revient à dire qu'

il existe une numérotation des treize paquets de sorte que le premier paquet contienne un as, le second un 2, le troisième un 3, et ainsi de suite jusqu'au treizième paquet qui contient un roi.

EXERCICE 2

Soit Ω un ensemble fini. Pour toutes parties A et X de Ω, on appelle discrépance entre A et X l'entier naturel $\Delta(A,X) = |\operatorname{card}(A\cap X) - \operatorname{card}(A\cap \overline{X})|$.

1. *Soient A et X deux parties de Ω et a un élément de Ω.*

   a) $\alpha]$ *Calculer $\Delta(\varnothing, X)$, $\Delta(\{a\}, X)$ et $\Delta(A,\varnothing)$.*

   On a

$$\begin{aligned}\Delta(\varnothing, X) &= |\operatorname{card}(\varnothing\cap X) - \operatorname{card}(\varnothing\cap\overline{X})|\\ &= |\operatorname{card}\varnothing - \operatorname{card}\varnothing|\\ &= |0-0|,\end{aligned}$$

   donc

$$\boxed{\Delta(\varnothing, X) = 0.}$$

   On a

$$\begin{aligned}\Delta(\{a\}, X) &= |\operatorname{card}(\{a\}\cap X) - \operatorname{card}(\{a\}\cap\overline{X})|\\ &= \begin{cases} |\operatorname{card}\{a\} - \operatorname{card}\varnothing| & \text{si } a\in X\\ |\operatorname{card}\varnothing - \operatorname{card}\{a\}| & \text{si } a\in \overline{X}\end{cases}\\ &= \begin{cases} |1-0| & \text{si } a\in X\\ |0-1| & \text{si } a\in \overline{X}\end{cases}\end{aligned}$$

   donc

$$\boxed{\Delta(\{a\}, X) = 1.}$$

   Enfin, on a

$$\begin{aligned}\Delta(A,\varnothing) &= |\operatorname{card}(A\cap\varnothing) - \operatorname{card}(A\cap\overline{\varnothing})|\\ &= |\operatorname{card}(A\cap\varnothing) - \operatorname{card}(A\cap\Omega)|\\ &= |\operatorname{card}\varnothing - \operatorname{card}A|\\ &= |0-\operatorname{card}A|,\end{aligned}$$

   donc

$$\boxed{\Delta(A,\varnothing) = \operatorname{card}A.}$$

   $\beta]$ *Démontrer que $\Delta(A,X)$ est un entier de $[\![0;\operatorname{card}A]\!]$, de même parité que* $\operatorname{card}A$.

   Remarquons que les parties $A\cap X$ et $A\cap\overline{X}$ sont disjointes (puisque la première est incluse dans X et la seconde est incluse dans le complémentaire de X) et que l'on a

$$(A\cap X)\sqcup(A\cap\overline{X}) = A\cap(X\sqcup\overline{X}) = A\cap\Omega = A.$$

   Il s'ensuit d'une part que

$$\begin{aligned}\Delta(A,X) &= |\operatorname{card}(A\cap X) - \operatorname{card}(A\cap\overline{X})|\\ &\leqslant \operatorname{card}(A\cap X) + \operatorname{card}(A\cap\overline{X}) & &\text{par inégalité triangulaire}\\ &= \operatorname{card}\big((A\cap X)\sqcup(A\cap\overline{X})\big)\\ &= \operatorname{card}A\end{aligned}$$

   et, d'autre part, que

$$\begin{aligned}\Delta(A,X) &= |\operatorname{card}(A\cap X) - \operatorname{card}(A\cap\overline{X})|\\ &= \big|\operatorname{card}(A\cap X) - \big(\operatorname{card}A - \operatorname{card}(A\cap X)\big)\big|\\ &= |2\operatorname{card}(A\cap X) - \operatorname{card}A|\\ &\equiv \operatorname{card}A \quad [2].\end{aligned}$$

   Donc

$$\boxed{\Delta(A,X) \text{ est un entier de l'intervalle } [\![0;\operatorname{card}A]\!], \text{ de même parité que } \operatorname{card}A.}$$

b) *Démontrer que* $\Delta(A,X) = \Delta(A, A\cap X)$.

On a

$$\begin{aligned}
\Delta(A, A\cap X) &= \left|\operatorname{card}(A\cap A\cap X) - \operatorname{card}(A\cap \overline{A\cap X})\right| \\
&= \left|\operatorname{card}(A\cap X) - \operatorname{card}\left(A\cap(\overline{A}\cup\overline{X})\right)\right| \\
&= \left|\operatorname{card}(A\cap X) - \operatorname{card}\left(\underbrace{(A\cap\overline{A})}_{=\varnothing}\cup(A\cap\overline{X})\right)\right| \\
&= \left|\operatorname{card}(A\cap X) - \operatorname{card}(A\cap\overline{X})\right| \\
&= \Delta(A,X),
\end{aligned}$$

donc

$$\boxed{\Delta(A,X) = \Delta(A, A\cap X).}$$

c) *Démontrer que* $\Delta(A,X) = \Delta(A, A\setminus X)$. *Préciser* $\Delta(A,A)$.

On a

$$\begin{aligned}
\Delta(A,X) &= \Delta(A,\overline{X}) && \text{c'est clair !} \\
&= \Delta(A, A\cap\overline{X}) && \text{d'après b)} \\
&= \Delta(A, A\setminus X),
\end{aligned}$$

donc

$$\boxed{\Delta(A,X) = \Delta(A, A\setminus X).}$$

Il s'ensuit que

$$\Delta(A,A) = \Delta(A, A\setminus A) = \Delta(A,\varnothing) = \operatorname{card} A$$

d'après la question a). Donc

$$\boxed{\Delta(A,A) = \operatorname{card} A.}$$

2. *Soit A une partie de Ω.*

a) *Calculer* $\left(\operatorname{card}\mathscr{P}(A)\right)^{-1}\sum_{X\in\mathscr{P}(A)}\operatorname{card} X$ *et* $\left(\operatorname{card}\mathscr{P}(A)\right)^{-1}\sum_{X\in\mathscr{P}(A)}(\operatorname{card} X)^2$.

On a

$$\mathscr{P}(A) = \bigsqcup_{k=0}^{\operatorname{card} A}\mathscr{P}_k(A),$$

où, pour tout $k\in[\![0;\operatorname{card} A]\!]$, la notation $\mathscr{P}_k(A)$ désigne l'ensemble des k-combinaisons de A, c'est-à-dire

$$\mathscr{P}_k(A) = \{X\in\mathscr{P}(A) : \operatorname{card} X = k\}.$$

Il s'ensuit que

$$\begin{aligned}
\frac{1}{\operatorname{card}\mathscr{P}(A)}\sum_{X\in\mathscr{P}(A)}\operatorname{card} X &= \frac{1}{\operatorname{card}\mathscr{P}(A)}\sum_{k=0}^{\operatorname{card} A}\sum_{\substack{X\in\mathscr{P}(A)\\ \operatorname{card} X=k}}\operatorname{card} X \\
&= \frac{1}{\operatorname{card}\mathscr{P}(A)}\sum_{k=0}^{\operatorname{card} A}\sum_{\substack{X\in\mathscr{P}(A)\\ \operatorname{card} X=k}} k.
\end{aligned}$$

On sait que

$$\operatorname{card}\mathscr{P}_k(A) = \binom{\operatorname{card} A}{k},$$

donc

$$\frac{1}{\operatorname{card}\mathscr{P}(A)}\sum_{X\in\mathscr{P}(A)}\operatorname{card} X = \frac{1}{\operatorname{card}\mathscr{P}(A)}\sum_{k=0}^{\operatorname{card} A} k\binom{\operatorname{card} A}{k}.$$

En remarquant que le premier terme est nul et en utilisant la formule du pion, il vient

$$\begin{aligned}
\frac{1}{\operatorname{card}\mathscr{P}(A)}\sum_{X\in\mathscr{P}(A)}\operatorname{card} X &= \frac{1}{\operatorname{card}\mathscr{P}(A)}\sum_{k=1}^{\operatorname{card} A}(\operatorname{card} A)\binom{\operatorname{card} A-1}{k-1} \\
&= \frac{\operatorname{card} A}{\operatorname{card}\mathscr{P}(A)}\sum_{\ell=0}^{\operatorname{card} A-1}\binom{\operatorname{card} A-1}{\ell} && \text{en posant } \ell = k-1.
\end{aligned}$$

Or

$$\begin{aligned}
\sum_{\ell=0}^{\operatorname{card} A-1} \binom{\operatorname{card} A - 1}{\ell} &= \sum_{\ell=0}^{\operatorname{card} A-1} \binom{\operatorname{card} A - 1}{\ell} 1^{\ell} 1^{\operatorname{card} A-1-\ell} \\
&= (1+1)^{\operatorname{card} A-1} && \text{formule du binôme} \\
&= 2^{\operatorname{card} A-1} \\
&= \frac{\operatorname{card} \mathscr{P}(A)}{2},
\end{aligned}$$

donc

$$\boxed{\frac{1}{\operatorname{card} \mathscr{P}(A)} \sum_{X \in \mathscr{P}(A)} \operatorname{card} X = \frac{\operatorname{card} A}{2}\cdot}$$

En procédant *mutatis mutandis*, on a

$$\begin{aligned}
&\frac{1}{\operatorname{card} \mathscr{P}(A)} \sum_{X \in \mathscr{P}(A)} (\operatorname{card} X)^2 \\
={}& \frac{1}{\operatorname{card} \mathscr{P}(A)} \sum_{k=0}^{\operatorname{card} A} \sum_{\substack{X \in \mathscr{P}(A) \\ \operatorname{card} X = k}} (\operatorname{card} X)^2 \\
={}& \frac{1}{\operatorname{card} \mathscr{P}(A)} \sum_{k=0}^{\operatorname{card} A} \sum_{\substack{X \in \mathscr{P}(A) \\ \operatorname{card} X = k}} k^2 \\
={}& \frac{1}{\operatorname{card} \mathscr{P}(A)} \sum_{k=\cancel{0}\,1}^{\operatorname{card} A} k^2 \binom{\operatorname{card} A}{k} \\
={}& \frac{1}{\operatorname{card} \mathscr{P}(A)} \sum_{k=1}^{\operatorname{card} A} k (\operatorname{card} A) \binom{\operatorname{card} A - 1}{k-1} && \text{formule du pion} \\
={}& \frac{\operatorname{card} A}{\operatorname{card} \mathscr{P}(A)} \sum_{k=1}^{\operatorname{card} A} (k-1+1) \binom{\operatorname{card} A - 1}{k-1} && \text{Binet} \\
={}& \frac{\operatorname{card} A}{\operatorname{card} \mathscr{P}(A)} \sum_{k=\cancel{1}\,2}^{\operatorname{card} A} (k-1) \binom{\operatorname{card} A - 1}{k-1} + \frac{\operatorname{card} A}{\operatorname{card} \mathscr{P}(A)} \sum_{k=1}^{\operatorname{card} A} \binom{\operatorname{card} A - 1}{k-1} \\
={}& \frac{\operatorname{card} A}{\operatorname{card} \mathscr{P}(A)} \sum_{k=2}^{\operatorname{card} A} (\operatorname{card} A - 1) \binom{\operatorname{card} A - 2}{k-2} + \frac{\operatorname{card} A}{\operatorname{card} \mathscr{P}(A)} \sum_{k=1}^{\operatorname{card} A} \binom{\operatorname{card} A - 1}{k-1} && \text{formule du pion} \\
={}& \frac{(\operatorname{card} A)(\operatorname{card} A - 1)}{\operatorname{card} \mathscr{P}(A)} \sum_{k=2}^{\operatorname{card} A} \binom{\operatorname{card} A - 2}{k-2} + \frac{\operatorname{card} A}{\operatorname{card} \mathscr{P}(A)} \sum_{k=1}^{\operatorname{card} A} \binom{\operatorname{card} A - 1}{k-1} \\
={}& \frac{(\operatorname{card} A)(\operatorname{card} A - 1)}{\operatorname{card} \mathscr{P}(A)} \sum_{\ell=0}^{\operatorname{card} A-2} \binom{\operatorname{card} A - 2}{\ell} + \frac{\operatorname{card} A}{\operatorname{card} \mathscr{P}(A)} \sum_{\ell=0}^{\operatorname{card} A-1} \binom{\operatorname{card} A - 1}{\ell} \\
={}& \frac{(\operatorname{card} A)(\operatorname{card} A - 1)}{\operatorname{card} \mathscr{P}(A)} (1+1)^{\operatorname{card} A-2} + \frac{\operatorname{card} A}{\operatorname{card} \mathscr{P}(A)} (1+1)^{\operatorname{card} A-1} && \text{formule du binôme} \\
={}& \frac{(\operatorname{card} A)(\operatorname{card} A - 1)}{\operatorname{card} \mathscr{P}(A)} 2^{\operatorname{card} A-2} + \frac{\operatorname{card} A}{\operatorname{card} \mathscr{P}(A)} 2^{\operatorname{card} A-1} \\
={}& \frac{(\operatorname{card} A)(\operatorname{card} A - 1))}{4} + \frac{\operatorname{card} A}{2} && \text{car } \operatorname{card} \mathscr{P}(A) = 2^{\operatorname{card} A},
\end{aligned}$$

donc

$$\boxed{\frac{1}{\operatorname{card} \mathscr{P}(A)} \sum_{X \in \mathscr{P}(A)} (\operatorname{card} X)^2 = \frac{(\operatorname{card} A)(\operatorname{card} A + 1)}{4}\cdot}$$

b) *En déduire que* $\left(\operatorname{card}\mathscr{P}(A)\right)^{-1}\sum_{X\in\mathscr{P}(A)}\Delta(A,X)^2=\operatorname{card}A$.

On a

$$\begin{aligned}
& \frac{1}{\operatorname{card}\mathscr{P}(A)}\sum_{X\in\mathscr{P}(A)}\Delta(A,X)^2\\
= & \frac{1}{\operatorname{card}\mathscr{P}(A)}\sum_{X\in\mathscr{P}(A)}\left(\operatorname{card}(A\cap X)-\operatorname{card}(A\cap\overline{X})\right)^2\\
= & \frac{1}{\operatorname{card}\mathscr{P}(A)}\sum_{X\in\mathscr{P}(A)}\left(\operatorname{card}X-(\operatorname{card}A-\operatorname{card}X)\right)^2 \qquad \text{car } X\subset A\\
= & \frac{1}{\operatorname{card}\mathscr{P}(A)}\sum_{X\in\mathscr{P}(A)}(2\operatorname{card}X-\operatorname{card}A)^2\\
= & \frac{1}{\operatorname{card}\mathscr{P}(A)}\sum_{X\in\mathscr{P}(A)}\left(4(\operatorname{card}X)^2-4\operatorname{card}A.\operatorname{card}X+(\operatorname{card}A)^2\right)\\
= & \frac{4}{\operatorname{card}\mathscr{P}(A)}\sum_{X\in\mathscr{P}(A)}(\operatorname{card}X)^2-\frac{4\operatorname{card}A}{\operatorname{card}\mathscr{P}(A)}\sum_{X\in\mathscr{P}(A)}\operatorname{card}X+\frac{(\operatorname{card}A)^2}{\operatorname{card}\mathscr{P}(A)}\sum_{X\in\mathscr{P}(A)}1\\
= & 4\frac{(\operatorname{card}A)(\operatorname{card}A+1)}{4}-4(\operatorname{card}A)\frac{\operatorname{card}A}{2}+(\operatorname{card}A)^2,
\end{aligned}$$

d'où

$$\boxed{\frac{1}{\operatorname{card}\mathscr{P}(A)}\sum_{X\in\mathscr{P}(A)}\Delta(A,X)^2=\operatorname{card}A.}$$

3. *Soit A une partie de Ω.*

a) *Démontrer que* $\varphi:\mathscr{P}(\Omega)\longrightarrow\mathscr{P}(A)\times\mathscr{P}(\overline{A})$ *définie par* $\forall X\in\mathscr{P}(\Omega),\ \varphi(X)=(X\cap A,X\cap\overline{A})$ *est une bijection.*

Considérons l'application

$$\psi\left\{\begin{array}{ccc}\mathscr{P}(A)\times\mathscr{P}(\overline{A}) & \longrightarrow & \mathscr{P}(\Omega)\\ (Y,Z) & \longmapsto & Y\sqcup Z\end{array}\right.$$

Pour tout $X\in\mathscr{P}(\Omega)$, on a

$$\begin{aligned}
(\psi\circ\varphi)(X) &= \psi\big(\varphi(X)\big)\\
&= \psi(X\cap A,X\cap\overline{A})\\
&= (X\cap A)\sqcup(X\cap\overline{A})\\
&= X\cap(A\sqcup\overline{A})\\
&= X\cap\Omega\\
&= X,
\end{aligned}$$

donc

$$\psi\circ\varphi=\mathrm{Id}_{\mathscr{P}(\Omega)}\,.$$

Pour tout $(Y,Z)\in\mathscr{P}(A)\times\mathscr{P}(\overline{A})$, on a

$$\begin{aligned}
(\varphi\circ\psi)(Y,Z) &= \varphi\big(\psi(Y,Z)\big)\\
&= \varphi(Y\sqcup Z)\\
&= \big((Y\sqcup Z)\cap A,(Y\sqcup Z)\cap\overline{A}\big)\\
&= \big((Y\cap A)\sqcup(Z\cap A),(Y\cap\overline{A})\sqcup(Z\cap\overline{A})\big)\\
&= (Y\sqcup\varnothing,\varnothing\sqcup Z)\\
&= (Y,Z),
\end{aligned}$$

donc

$$\varphi\circ\psi=\mathrm{Id}_{\mathscr{P}(A)\times\mathscr{P}(\overline{A})}\,.$$

On en déduit que

$$\boxed{\varphi\text{ est une bijection (de réciproque }\psi).}$$

b) *Démontrer que* $\left(\operatorname{card}\mathscr{P}(\Omega)\right)^{-1}\sum_{X\in\mathscr{P}(\Omega)}\Delta(A,X)^2=\operatorname{card}A$.

On a

$$\begin{aligned}
&\frac{1}{\operatorname{card}\mathscr{P}(\Omega)}\sum_{X\in\mathscr{P}(\Omega)}\Delta(A,X)^2\\
=\;&\frac{1}{\operatorname{card}\mathscr{P}(\Omega)}\sum_{(Y,Z)\in\mathscr{P}(A)\times\mathscr{P}(\overline{A})}\Delta(A,Y\sqcup Z)^2\\
=\;&\frac{1}{\operatorname{card}\mathscr{P}(\Omega)}\sum_{(Y,Z)\in\mathscr{P}(A)\times\mathscr{P}(\overline{A})}\Delta\big(A,A\cap(Y\sqcup Z)\big)^2 \qquad \text{d'après 1. b)}\\
=\;&\frac{1}{\operatorname{card}\mathscr{P}(\Omega)}\sum_{(Y,Z)\in\mathscr{P}(A)\times\mathscr{P}(\overline{A})}\Delta\big(A,\underbrace{(A\cap Y)}_{=Y}\sqcup\underbrace{(A\cap Z)}_{=\varnothing}\big)^2\\
=\;&\frac{1}{\operatorname{card}\mathscr{P}(\Omega)}\sum_{(Y,Z)\in\mathscr{P}(A)\times\mathscr{P}(\overline{A})}\Delta(A,Y)^2\\
=\;&\frac{1}{\operatorname{card}\mathscr{P}(\Omega)}\sum_{Y\in\mathscr{P}(A)}\sum_{Z\in\mathscr{P}(\overline{A})}\Delta(A,Y)^2\\
=\;&\frac{1}{\operatorname{card}\mathscr{P}(\Omega)}\sum_{Y\in\mathscr{P}(A)}\Delta(A,Y)^2\operatorname{card}\mathscr{P}(\overline{A})\\
=\;&\frac{1}{\operatorname{card}\mathscr{P}(A)}\sum_{Y\in\mathscr{P}(A)}\Delta(A,Y)^2 \qquad \begin{array}{l}\text{car } \operatorname{card}\mathscr{P}(\Omega)=\operatorname{card}\mathscr{P}(A).\operatorname{card}\mathscr{P}(\overline{A})\\ \text{puisque } \varphi \text{ est une bijection}\end{array}\\
=\;&\operatorname{card}A \qquad \text{d'après 2. b)},
\end{aligned}$$

donc

$$\boxed{\frac{1}{\operatorname{card}\mathscr{P}(\Omega)}\sum_{X\in\mathscr{P}(\Omega)}\Delta(A,X)^2=\operatorname{card}A.}$$

4. *Soit* $(A_1,\dots,A_p)$ *une partition de* Ω. *Pour toute partie* X *de* Ω, *on appelle discrépance entre* $(A_1,\dots,A_p)$ *et* X *l'entier naturel* $\Delta(A_1,\dots,A_p,X)=\sqrt{\Delta(A_1,X)^2+\cdots+\Delta(A_p,X)^2}$. *Démontrer que* $\left(\operatorname{card}\mathscr{P}(\Omega)\right)^{-1}\sum_{X\in\mathscr{P}(\Omega)}\Delta(A_1,\dots,A_p,X)^2=\operatorname{card}\Omega$.

On a

$$\begin{aligned}
\frac{1}{\operatorname{card}\mathscr{P}(\Omega)}\sum_{X\in\mathscr{P}(\Omega)}\Delta(A_1,\dots,A_p,X)^2 &= \frac{1}{\operatorname{card}\mathscr{P}(\Omega)}\sum_{X\in\mathscr{P}(\Omega)}\sum_{k=1}^{p}\Delta(A_k,X)^2\\
&= \sum_{k=1}^{p}\frac{1}{\operatorname{card}\mathscr{P}(\Omega)}\sum_{X\in\mathscr{P}(\Omega)}\Delta(A_k,X)^2\\
&= \sum_{k=1}^{p}\operatorname{card}A_k \qquad \text{d'après 3. b)}\\
&= \operatorname{card}\Big(\bigsqcup_{k=1}^{p}A_k\Big)\\
&= \operatorname{card}\Omega,
\end{aligned}$$

donc

$$\boxed{\frac{1}{\operatorname{card}\mathscr{P}(\Omega)}\sum_{X\in\mathscr{P}(\Omega)}\Delta(A_1,\dots,A_p,X)^2=\operatorname{card}\Omega.}$$

EXERCICE 3

Soit A un anneau commutatif. Une partie X de A est appelée un idéel de A lorsqu'il existe un élément x de A et un idéal I de A tel que $X = x + I$ (c'est-à-dire $X = \{x + i : i \in I\}$).

1. a) *Parmi les propositions suivantes, reconnaître (en justifiant) les idéels : $\varnothing$; les idéaux de A ; les singletons de A ; les sous-anneaux de A.*

Un idéal I n'est jamais vide (il contient 0_A) donc l'idéel $x + I$ n'est pas vide non plus. Par conséquent,

$$\boxed{\varnothing \text{ n'est pas un idéel de } A.}$$

Si I est un idéal de A, on a $I = 0_A + I$, donc I est un idéel de A. Par conséquent,

$$\boxed{\text{les idéaux de } A \text{ sont des idéels de } A.}$$

Si $\{x\}$ est un singleton de A, on a $\{x\} = x + \{0_A\}$ et $\{0_A\}$ est un idéal de A. Donc

$$\boxed{\text{les singletons de } A \text{ sont des idéels de } A.}$$

Plaçons nous dans le corps $\mathbb{C}$. Les seuls idéaux d'un corps étant les triviaux, on sait que les idéaux de $\mathbb{C}$ sont $\{0\}$ et $\mathbb{C}$. Par conséquent, les idéels de $\mathbb{C}$ sont les singletons et $\mathbb{C}$. Il s'ensuit que $\mathbb{R}$ n'est pas un idéel de $\mathbb{C}$. En revanche, c'est bien un sous-anneau (c'est même un sous-corps). Donc

$$\boxed{\text{les sous-anneaux de } A \text{ ne sont pas tous des idéels de } A.}$$

b) *Quels sont les idéels de $\mathbb{Z}$?*

On sait que les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$ où $n \in \mathbb{N}$. Par conséquent, les idéels de $\mathbb{Z}$ sont les $x + n\mathbb{Z}$ où $x \in \mathbb{Z}$. Autrement dit,

$$\boxed{\text{les idéels de } \mathbb{Z} \text{ sont les progressions arithmétiques de } \mathbb{Z}.}$$

2. *Soit X un idéel de A. On considère un élément x de A et un idéal I de A tel que $X = x + I$.*

a) *Démontrer que $x \in X$. Réciproquement, démontrer que, si $y \in X$, alors $X = y + I$.*

Comme $0_A \in I$, on a $x + 0_A \in X$, donc

$$\boxed{x \in X.}$$

Soit $y \in X$. Il existe $i \in I$ tel que $y = x + i$. Alors $X = x + I = (y - i) + I = y + (-i + I)$. Comme $(I, +)$ est un groupe et comme $-i \in I$, on a $-i + I = I$. Donc $X = y + I$. Ainsi,

$$\boxed{\text{si } y \in X, \text{ alors } X = y + I.}$$

b) *On suppose qu'il existe un élément y de A et un idéal J de A tel que $X = y + J$. Démontrer que $x - y \in I$ et $J = I$. On dit que I est la direction de X.*

Comme $x \in X$, la question a) dit que $x \in y + J$, ce qui démontre immédiatement que $x - y \in J$. De même, on a $x - y \in I$.

Sachant que $x + I = y + J$ avec $x - y \in I \cap J$, démontrons que $I = J$ par double inclusion.

- $\subset$ Soit $i \in I$. Alors $x + i \in x + I$ d'où $x + i \in y + J$. Il existe donc $j \in J$ tel que $x + i = y + j$, c'est-à-dire $i = j - (x - y)$. Comme j et $x - y$ appartiennent à J, il s'ensuit que i appartient à J. Donc $I \subset J$.
- $\supset$ En échangeant les rôles de I et J, on obtient de même $J \subset I$.

Donc $I = J$.

En conclusion,

$$\boxed{\text{s'il existe un élément } y \text{ de } A \text{ et un idéal } J \text{ de } A \text{ tel que } X = y + J, \text{ alors } x - y \in I \text{ et } J = I.}$$

3. *Démontrer qu'un idéel est un idéal si, et seulement si, il contient 0_A.*
Soit X un idéel de direction I. On procède par double implication.
   $\Rightarrow$ Supposons que X est un idéal. Alors 0_A appartient à X puisque tout idéal contient 0_A.
   $\Leftarrow$ Supposons que $0_A \in X$. D'après la question 2. a), on a $X = 0_A + I = I$. Donc X est un idéal.
En conclusion,

$$\boxed{\text{un idéel est un idéal si, et seulement si, il contient } 0_A.}$$

4. a) *Démontrer qu'une intersection quelconque d'idéels de A est ou bien vide ou bien un idéel de A.*
Soit L un ensemble d'indices et $(X_\ell)_{\ell \in L}$ une famille d'idéels de A. Posons $\widehat{X} = \bigcap_{\ell \in L} X_\ell$ et démontrons que $\widehat{X}$ est ou bien vide ou bien un idéel de A.
Pour cela, on suppose que $\widehat{X} \neq \varnothing$ et on va démontrer que $\widehat{X}$ est un idéel de A.
Comme $\widehat{X} \neq \varnothing$, il existe $x \in \widehat{X}$, c'est-à-dire $\forall \ell \in L,\ x \in X_\ell$. D'après la question 2. a), on en déduit que, pour tout $\ell \in L$, on a $X_\ell = x + I_\ell$ où I_ℓ est la direction de X_ℓ. On a donc

$$\begin{array}{rcl} \widehat{X} & = & \bigcap_{\ell \in L}(x + I_\ell) \\ & = & \{y \in A : \forall \ell \in L,\ y \in x + I_\ell\} \\ & = & \{y \in A : \forall \ell \in L,\ y - x \in I_\ell\} \\ & = & \{y \in A : y - x \in \bigcap_{\ell \in L} I_\ell\} \\ & = & \{y \in A : y \in x + \bigcap_{\ell \in L} I_\ell\} \\ & = & x + \bigcap_{\ell \in L} I_\ell. \end{array}$$

Comme $\bigcap_{\ell \in L} I_\ell$ est un idéal en tant qu'intersection d'idéaux, on en déduit que $\widehat{X}$ est un idéel.
En conclusion,

$$\boxed{\text{une intersection (quelconque) d'idéels de } A \text{ est ou bien vide ou bien un idéel de } A.}$$

b) *Démontrer qu'une somme de deux idéels de A est un idéel de A.*
Soient X_1, X_2 deux idéels de A. Il existe x_1, x_2 deux éléments de A et I_1, I_2 deux idéaux de A tels que $X_1 = x_1 + I_1$ et $X_2 = x_2 + I_2$. Alors $X_1 + X_2 = (x_1 + I_1) + (x_2 + I_2)$, c'est-à-dire $X_1 + X_2 = (x_1 + x_2) + (I_1 + I_2)$. Or $I_1 + I_2$ est un idéal en tant que somme de deux idéaux, donc $X_1 + X_2$ est un idéel. Ainsi,

$$\boxed{\text{une somme de deux idéels de } A \text{ est un idéel de } A.}$$

5. *Soit $\varphi : A \longrightarrow A'$ un morphisme d'anneaux commutatifs.*
   a) $\alpha]$ *Soit X un idéel de A. Démontrer que $\varphi(X)$ est un idéel de l'anneau $\varphi(A)$.*
Il existe un élément x de A et un idéal I de A tel que $X = x + I$.
On a $\varphi(A) = \varphi(x + I) = \varphi(x) + \varphi(I)$ puisque φ est un morphisme.
Or $\varphi(I)$ est un idéal de l'anneau $\varphi(A)$ d'après le cours, donc $\varphi(X)$ est un idéel de $\varphi(A)$.
En conclusion,

$$\boxed{\text{l'image morphique d'un idéel de } A \text{ est un idéel de } \varphi(A).}$$

$\beta]$ *Soit X' un idéel de A'. Démontrer que $\varphi^{-1}(X')$ est ou bien vide ou bien un idéel de A.*
Supposons que $\varphi^{-1}(X') \neq \varnothing$. Il existe alors $x' \in X'$ et $x \in X$ tels que $\varphi(x) = x'$. D'après 2. a), on a $X' = x' + I'$ où I' est la direction de X'. D'où

$$\begin{array}{rcl} \varphi^{-1}(X') & = & \varphi^{-1}(x' + I') \\ & = & \{a \in A : \varphi(a) \in x' + I'\} \\ & = & \{a \in A : \varphi(a) - x' \in I'\} \\ & = & \{a \in A : \varphi(a) - \varphi(x) \in I'\} \\ & = & \{a \in A : \varphi(a - x) \in I'\} \\ & = & \{a \in A : a - x \in \varphi^{-1}(I')\} \\ & = & \{a \in A : a \in x + \varphi^{-1}(I')\} \\ & = & x + \varphi^{-1}(I'). \end{array}$$

Or $\varphi^{-1}(I')$ est un idéal de A d'après le cours, donc $\varphi^{-1}(X')$ est un idéel de A.
En conclusion,

$$\boxed{\text{l'image réciproque morphique d'un idéel de } A' \text{ est un idéel de } A.}$$

b) *Pour tout* $x' \in A'$, *on pose* $\mathrm{Ben}(\varphi, x') = \{a \in A : \varphi(a) = x'\} = \varphi^{-1}(\{x'\})$.

α] *Reconnaître* $\mathrm{Ben}(\varphi, 0_{A'})$.

On a clairement
$$\boxed{\mathrm{Ben}(\varphi, 0_{A'}) = \mathrm{Ker}\,\varphi.}$$

β] *Justifier que, pour tout* $x' \in A'$, $\mathrm{Ben}(\varphi, x')$ *est ou bien vide ou bien un idéel de* A *dont on précisera la direction.*

Soit $x' \in A'$. Supposons que $\mathrm{Ben}(\varphi, x') \neq \varnothing$, c'est-à-dire $\varphi^{-1}(\{x'\}) \neq \varnothing$. Il existe donc $x \in A$ tel que $\varphi(x) = x'$. Alors

$$\begin{aligned}
\mathrm{Ben}(\varphi, x') &= \{a \in A : \varphi(a) = x'\} \\
&= \{a \in A : \varphi(a) = \varphi(x)\} \\
&= \{a \in A : \varphi(a - x) = 0_{A'}\} \\
&= \{a \in A : a - x \in \mathrm{Ker}\,\varphi\} \\
&= \{a \in A : a \in x + \mathrm{Ker}\,\varphi\} \\
&= x + \mathrm{Ker}\,\varphi,
\end{aligned}$$

ce qui démontre que $\mathrm{Ben}(\varphi, x')$ est un idéel de A de direction $\mathrm{Ker}\,\varphi$. En conclusion,

$$\boxed{\text{pour tout } x' \in A',\ \mathrm{Ben}(\varphi, x') \text{ est ou bien vide ou bien un idéel de } A \text{ de direction } \mathrm{Ker}\,\varphi.}$$

γ] *Démontrer que* φ *est injectif si, et seulement si, il existe un élément* x' *de* A' *tel que* $\mathrm{Ben}(\varphi, x')$ *est un singleton.*

On raisonne par double implication.

$\boxed{\Rightarrow}$ Supposons que φ est injectif. Alors $\mathrm{Ker}\,\varphi = \{0_A\}$, c'est-à-dire $\mathrm{Ben}(\varphi, 0_{A'}) = \{0_A\}$. Il existe donc bien un élément x' de A' tel que $\mathrm{Ben}(\varphi, x')$ est un singleton.

$\boxed{\Leftarrow}$ Supposons qu'il existe un élément x' de A' tel que $\mathrm{Ben}(\varphi, x')$ est un singleton. Alors, la direction de $\mathrm{Ben}(\varphi, x')$ est égale à $\{0_A\}$, c'est-à-dire $\mathrm{Ker}\,\varphi = \{0_A\}$. Donc φ est injectif.

En conclusion,

$$\boxed{\varphi \text{ est injectif si, et seulement si, il existe } x' \in A' \text{ tel que } \mathrm{Ben}(\varphi, x') \text{ est un singleton.}}$$

6. *Soit* I *un idéal de* A. *Sur* A, *on définit la relation de congruence modulo* I, *notée* $\equiv [I]$, *par* $\forall a, b \in A,\ (a \equiv b\ [I]) \Leftrightarrow (b - a \in I)$.

a) *Vérifier que* $\equiv [I]$ *est un relation d'équivalence sur* A.

Soit $a \in A$. On a $a - a = 0_A \in I$ donc $a \equiv a\ [I]$. Donc la relation $\equiv [I]$ est réflexive.

Soient $a_1, a_2, a_3 \in A$ tels que $a_2 \equiv a_1\ [I]$ et $a_3 \equiv a_2\ [I]$. On a $a_2 - a_1 \in I$ et $a_3 - a_2 \in I$. Donc $(a_2 - a_1) + (a_3 - a_2) \in I$, c'est-à-dire $a_3 - a_1 \in I$. D'où $a_3 \equiv a_1\ [I]$. Cela démontre que la relation $\equiv [I]$ est transitive.

Soient $a_1, a_2 \in A$ tels que $a_2 \equiv a_1\ [I]$. On a $a_2 - a_1 \in I$ donc $a_1 - a_2 \in I$, c'est-à-dire $a_1 \equiv a_2\ [I]$. Cela démontre que la relation $\equiv [I]$ est symétrique.

Donc
$$\boxed{\equiv [I] \text{ est un relation d'équivalence sur } A.}$$

b) *Soit* $x \in A$. *Démontrer que la classe d'équivalence de* x *modulo* $\equiv [I]$ *est l'idéel* $x + I$.

La classe d'équivalence $\widehat{x}$ de x modulo $\equiv [I]$ est donnée par

$$\begin{aligned}
\widehat{x} &= \{y \in A : y \equiv x\ [I]\} \\
&= \{y \in A : y - x \in I\} \\
&= \{y \in A : y \in x + I\} \\
&= x + I,
\end{aligned}$$

donc
$$\boxed{\text{la classe d'équivalence de } x \text{ modulo la relation } \equiv [I] \text{ est l'idéel } x + I.}$$

c) *On note $A/_I$ l'ensemble quotient de A par la relation d'équivalence $\equiv[I]$. La question précédente nous dit que $A/_I = \{x+I : x \in A\}$, c'est-à-dire que $A/_I$ est l'ensemble des idéels de A. Sur $A/_I$, on considère l'addition et la multiplication définies, pour tous éléments $x+I$ et $y+I$ de $A/_I$, par $(x+I)+(y+I) = (x+y)+I$ et $(x+I)(y+I) = xy+I$. Justifier que l'addition et la multiplication sur $A/_I$ sont bien définies et démontrer que $A/_I$, muni de ces lois, est un anneau commutatif.*

Pour que l'addition et la multiplication sur $A/_I$ soient bien définies, il faut vérifier que la somme ou le produit de deux idéels ne dépendent pas des représentants choisis dans ces idéels.

Soient X_1, X_2 deux idéels de A de direction I. Soient $x_1, y_1 \in X_1$ et $x_2, y_2 \in X_2$. D'après la question 2. b), on a $y_1 - x_1 \in I$ et $y_2 - x_2 \in I$. Par conséquent, on a

$$x_1 + x_2 = y_1 + y_2 + \underbrace{x_1 - y_1}_{\in I} + \underbrace{x_2 - y_2}_{\in I} \equiv y_1 + y_2 \ [I]$$

et

$$x_1x_2 = x_1(x_2 - y_2) + x_1y_2 = \underbrace{x_1(x_2 - y_2)}_{\in I} + \underbrace{(x_1 - y_1)y_2}_{\in I} + y_1y_2 \equiv y_1y_2 \ [I].$$

Cela démontre que l'addition et la multiplication sont compatibles avec la relation $\equiv[I]$, ce qui signifie que

$$\boxed{\text{l'addition et la multiplication sur } A/_I \text{ sont bien définies.}}$$

Vérifions que $(A/_I, +, \times)$ est un anneau commutatif.

L'associativité et la commutativité de l'addition sur A se transmettent à l'addition sur $A/_I$.
Pour tout $x \in A$, on a $(x+I)+I = x+I$, donc I est l'élément neutre additif dans $A/_I$.
Pour tout $x \in A$, on a $(x+I)+(-x+I) = I$, donc tout élément de $A/_I$ possède un opposé.
On sait donc que $(A/_I, +)$ est un groupe abélien.

L'associativité et la commutativité du produit sur A se transmettent au produit sur $A/_I$.
Pour tout $x \in A$, on a $(x+I)(1_A+I) = x+I$ donc 1_A+I est le neutre multiplicatif dans $A/_I$.
Ainsi, $(A/_I, \times)$ est un monoïde commutatif.

Enfin, la distributivité de $\times$ sur $+$ dans A se transmet dans $A/_I$.

Donc

$$\boxed{(A/_I, +, \times) \text{ est un anneau commutatif.}}$$

Remarque : On peut aussi remarquer que le morphisme $x \longmapsto x+I$ transporte la structure d'anneau de A vers $A/_I$.

d) *On dit que I est un idéal maximal lorsque $I \neq A$ et I n'est inclus que dans deux idéaux : lui-même et A. Démontrer que $A/_I$ est un corps si, et seulement si, I est maximal.*

On raisonne par double implication.

- $\Rightarrow$ Supposons que $A/_I$ est un corps et démontrons que I est maximal.
  Comme $A/_I$ est un corps, on sait que ce n'est pas l'anneau nul (c'est dans la définition d'un corps). Par conséquent, on a $A/_I \neq \{I\}$, c'est-à-dire $I \neq A$.
  Soit J un idéal de A tel que $I \subset J$. On veut démontrer que J vaut ou bien I ou bien A. Pour cela, on suppose que $J \neq I$, de sorte qu'il existe $j \in J$ et $j \notin I$. On a donc $j \not\equiv 0_A \ [I]$, ce qui implique que $j+I$ est inversible dans le corps $A/_I$. On a donc $jj^{-1} \equiv 1_A \ [I]$. Comme $jj^{-1} \in J$ (par hyperstabilité de J) et comme $I \subset J$, cela démontre que $1_A \in J$ et donc que $J = A$.
  Donc I est maximal.

- $\Leftarrow$ Supposons que I est maximal et démontrons que $A/_I$ est un corps.
  Soit $X \in A/_I$ tel que $X \neq I$.
  Soit $x \in X$. On sait que xA est un idéal de A (c'est dans le cours). Donc $xA + I$ est aussi un idéal de A (c'est aussi dans le cours) et il contient strictement I (puisque $X \neq I$). On a donc $xA + I = A$ puisque I est maximal. En particulier, on a $1_A \in xA + I$, ce qui démontre qu'il existe $y \in A$ et $i \in I$ tels que $1_A = xy + i$. Cela s'écrit encore $1_A \equiv xy \ [I]$ et cela signifie que X est inversible dans $A/_I$.
  Donc $A/_I$ est un corps.

En conclusion,

$$\boxed{A/_I \text{ est un corps si, et seulement si, } I \text{ est maximal.}}$$