

Devoir Surveillé N° 5

Ensembles & Applications Structures & Arithmétique

14 Février 2020

4 heures

Problème 1: Équations dans $\mathcal{P}(E)$

Soit E un ensemble.

Pour toute partie A de E , on note \bar{A} le complémentaire de A dans E .

1. Soit A une partie de E .

On cherche à caractériser les solutions (X, Y) de l'équation $X \cap Y = A$.

- (a) Soit A une partie de E . Montrer que pour tout couple (R, S) de parties de E , les ensembles $\begin{cases} X = A \cup (R \cap \bar{S}) \\ Y = A \cup (\bar{R} \cap S) \end{cases}$ vérifient $X \cap Y = A$.
- (b) Montrer que, réciproquement, toute solution (X, Y) de $X \cap Y = A$ est de la forme ci-dessus pour, au moins, un couple (R, S) de parties de E .
- (c) Conclure.

2. Etudier de même l'équation $X \cup Y = A$.

On donnera deux démonstrations pour cette question :

- (a) Une méthode analogue à la précédente, avec $\begin{cases} X = A \cap (R \cup \bar{S}) \\ Y = A \cap (\bar{R} \cup S) \end{cases}$
- (b) Une méthode qui utilise le *résultat* de la question précédente.

3. Dans cette question, on désire étudier l'équation $(A \cap X) \cup (B \cap \bar{X}) = C$, où A, B, C sont des parties données de E , X étant une partie inconnue de E .

- (a) On suppose que X_0 est solution de cette équation.
- i. Montrer que $A \cap B \subset C$ et $C \subset A \cup B$.
- ii. Montrer que $(\bar{B} \cap C) \cup (B \cap \bar{C}) \cup [X_0 \cap ((A \cap B) \cup (\bar{A} \cap \bar{B}))] = X_0$.

- (b) On suppose que $A \cap B \subset C \subset A \cup B$.

D étant une partie de E , on pose : $X = (\bar{B} \cap C) \cup (B \cap \bar{C}) \cup [D \cap ((A \cap B) \cup (\bar{A} \cap \bar{B}))]$.

Démontrer que :

- i. $A \cap X = C \cap [\bar{B} \cup (D \cap A \cap B)]$.
- ii. $\bar{B} \cup X = \bar{B} \cup (B \cap \bar{C}) \cup (D \cap A \cap B)$.
- iii. $B \cap \bar{X} = C \cap [\bar{A} \cup (\bar{D} \cap B)]$.

- (c) En déduire $(A \cap X) \cup (B \cap \bar{X})$.

- (d) Donner une condition nécessaire et suffisante, portant sur A, B, C , pour que l'équation $(A \cap X) \cup (B \cap \bar{X}) = C$ ait au moins une solution.

- (e) Donner alors la forme générale de la solution.

Problème 2 (Bonus): Trois relations identiques dans $\mathcal{P}(E)$

Etant donné un ensemble E , on désigne par \mathcal{M} une partie non vide de $\mathcal{P}(E)$ telle que :

$$\forall X, Y \in \mathcal{M}, \exists Z \in \mathcal{M}, \text{ tel que } Z \subset X \cap Y.$$

1. Montrer que pour tout ensemble E , il existe de telles parties \mathcal{M} de $\mathcal{P}(E)$.
2. On associe à \mathcal{M} une relation binaire \mathcal{R} définie sur $\mathcal{P}(E)$ par :

$$\forall A, B \in \mathcal{P}(E), \quad A \mathcal{R} B \Leftrightarrow \exists X \in \mathcal{M} \text{ tel que } A \cap X = B \cap X$$

- (a) Montrer que \mathcal{R} est une relation d'équivalence.
- (b) Montrer que \mathcal{R} est l'égalité si et seulement si $\mathcal{M} = \{E\}$.
- (c) Montrer que \mathcal{R} est l'équivalence universelle si et seulement si $\emptyset \in \mathcal{M}$.
3. On note \widehat{A} la classe d'équivalence, pour \mathcal{R} , d'une partie A quelconque de E .
 - (a) Déterminer \widehat{E} et $\widehat{\emptyset}$.
 - (b) Montrer que si $A \in \widehat{E}$ et $B \in \widehat{E}$, alors $A \cap B \in \widehat{E}$.
 - (c) On pose $\mathcal{N} = \widehat{E}$, et dans $\mathcal{P}(E)$ on désigne par \mathcal{S} la relation :

$$\forall A, B \in \mathcal{P}(E), \quad A \mathcal{S} B \Leftrightarrow \exists Y \in \mathcal{N} \text{ tel que } A \cap Y = B \cap Y$$

Montrer que les relations \mathcal{R} et \mathcal{S} sont identiques.

4. On définit sur $\mathcal{P}(E)$ la différence symétrique :

$$\forall A, B \in \mathcal{P}(E), \quad A \Delta B = (A \cap \overline{B}) \cup (\overline{A} \cap B)$$

Soit \mathcal{T} la relation définie sur $\mathcal{P}(E)$ par :

$$\forall A, B \in \mathcal{P}(E), \quad A \mathcal{T} B \Leftrightarrow \exists X \in \mathcal{M} \text{ tel que } (A \Delta B) \cap X = \emptyset$$

- (a) Montrer que les relations \mathcal{T} et \mathcal{R} sont identiques.
- (b) A, A', B, B' étant des parties de E telles que $A \mathcal{R} A'$ et $B \mathcal{R} B'$, montrer que :
 $(A \cap B) \mathcal{R} (A' \cap B')$, $(A \cup B) \mathcal{R} (A' \cup B')$, $\overline{A} \mathcal{R} \overline{A'}$, et $(A \Delta B) \mathcal{R} (A' \Delta B')$.
5. Déterminer les classes d'équivalence de $\mathcal{P}(E)$ pour la relation \mathcal{R} dans les cas suivants :
 - (a) $\mathcal{M} = \{E\}$.
 - (b) $\emptyset \in \mathcal{M}$.
 - (c) $\mathcal{M} = \{\{x\}\}$, où $x \in E$.
 - (d) $\mathcal{M} \supset \{\{x\}, \{y\}\}$, où x, y sont deux éléments distincts de E .

Problème 3: Sous-groupes distingués

Soit G un groupe, qui n'est pas supposé abélien. On note $(a, b) \mapsto ab$ la loi de G .

On note e le neutre de G , et a^{-1} le symétrique de tout élément a de G .

Pour toute partie X non vide de G , et pour tous éléments a, b de G , on pose :

$$aX = \{ax, x \in X\} \quad Xb = \{xb, x \in X\} \quad aXb = a(Xb) = (aX)b = \{axb, x \in X\}$$

Les propriétés suivantes sont évidentes et n'ont pas à être démontrées :

$$X \subset Y \Rightarrow \begin{cases} aX \subset aY \\ Xb \subset Yb \\ aXb \subset aYb \end{cases} \quad \begin{cases} a(bX) = (ab)X \\ (Xa)b = X(ab) \\ a(bXc)d = (ab)X(cd) \end{cases} \quad eX = Xe = X$$

On rappelle que les automorphismes intérieurs de G sont les applications φ_a définies par :

$$\forall a \in G, \forall x \in G, \varphi_a(x) = axa^{-1}$$

I. Définition des sous-groupes distingués

1. Soit H un sous-groupe de G . Montrer que les conditions suivantes sont équivalentes :

- i) Pour tout a de G , $aH \subset Ha$
- ii) Pour tout a de G , $Ha \subset aH$
- iii) Pour tout a de G , $aH = Ha$

On dit qu'un sous-groupe H de G est *distingué* s'il vérifie ces conditions.

2. Soit H un sous-groupe d'un groupe G .

Montrer que les conditions suivantes sont équivalentes :

- i) H est distingué dans G
- ii) $\forall a \in G, aHa^{-1} = H$
- iii) $\forall a \in G, aHa^{-1} \subset H$

Exprimer cette propriété avec la terminologie des automorphismes intérieurs de G .

II. Exemples de sous-groupes distingués

1. Soit G un groupe. Vérifier que $\{e\}$ et G sont distingués dans G .

2. Que peut-on dire des sous-groupes distingués d'un groupe abélien G ?

3. Soient G et \tilde{G} deux groupes. Soit $f : G \rightarrow \tilde{G}$ un morphisme de groupes.

(a) On suppose que \tilde{H} est un sous-groupe distingué de \tilde{G} .

Montrer que son image réciproque par f est un sous-groupe distingué H de G .

(b) Dans cette question, on suppose que le morphisme f est surjectif.

Soit H un sous-groupe distingué de G .

Montrer que $\tilde{H} = f(H)$ est un sous-groupe distingué de \tilde{G} .

(c) Que dire du noyau de f ?

III. Centre et centralisateurs

Soit G un groupe. Soit X une partie non vide quelconque de G .

On appelle *centralisateur* de X l'ensemble $X' = \{a \in G, \forall x \in X, ax = xa\}$.

On appelle *centre* de G l'ensemble $C = \{a \in G, \forall x \in G, ax = xa\}$.

Le centre de G est donc le centralisateur G' de G lui-même.

1. (a) Montrer que X' est un sous-groupe de G .
(b) Montrer que le sous-groupe C est distingué dans G .
2. Avec les automorphismes intérieurs, retrouver que C est distingué dans G .
3. Dans cette question X et Y sont deux parties non vides quelconques de G .
(a) Vérifier que $X \subset Y \Rightarrow Y' \subset X'$.
(b) On pose $X'' = (X')'$. Montrer que X est inclus dans X'' .
(c) On pose $X''' = ((X')')'$. Montrer que $X' = X'''$.
4. Dans cette question, on suppose que H est un sous-groupe de G .
(a) Montrer les équivalences : H abélien $\Leftrightarrow H \subset H' \Leftrightarrow H''$ abélien.
(b) Montrer que si H est distingué, alors H' est distingué.

IV. Produit de deux sous-groupes

Dans cette partie, H et K sont deux sous-groupes quelconques de G .

On pose $HK = \{hk, h \in H, k \in K\}$ et $KH = \{kh, k \in K, h \in H\}$.

1. Montrer que $HK \subset KH \Leftrightarrow KH \subset HK \Leftrightarrow HK = KH$.
2. Montrer que HK est un sous-groupe de G si et seulement si $HK = KH$.
3. On suppose que l'un des deux sous-groupes H ou K est distingué.
Montrer que $HK = KH$. Conclusion ?

V. Quotient par un sous-groupe distingué

Soit H un sous-groupe quelconque de G .

On définit sur G une relation \mathcal{R} par $x\mathcal{R}y \Leftrightarrow x^{-1}y \in H$.

1. Montrer que \mathcal{R} est une relation d'équivalence sur G .
Quelle est cette relation si $H = G$? si $H = \{e\}$?
2. Vérifier que la classe d'équivalence d'un élément a de G est $\bar{a} = aH$.
3. Dans cette question, on suppose que H est un sous-groupe distingué de G .

On note G/H l'ensemble des classes d'équivalence de G pour la relation \mathcal{R} .

(a) Soient x et y deux éléments de G . Montrer que \overline{xy} ne dépend que de \bar{x} et de \bar{y} .

(b) On peut donc définir une loi sur G/H en posant : $\forall (x, y) \in G^2, \bar{x}\bar{y} = \overline{xy}$.

Montrer qu'alors G/H est un groupe. Quel est le neutre? l'inverse de \bar{x} ?

On dit que G/H est le *groupe quotient* de G par le sous-groupe distingué H .

(c) Montrer l'équivalence des deux propriétés :

- Le groupe G/H est commutatif.
- Pour tous x, y de G , l'élément $y^{-1}x^{-1}yx$ est dans H .

Problème 4: Voyage au coeur de l'arithmétique

Notations

On appelle **fonction arithmétique** toute fonction de \mathbb{N}^* dans \mathbb{R} . L'objectif du problème est d'étudier deux fonctions arithmétiques célèbres : la fonction indicatrice d'Euler et la fonction μ de Möbius, puis d'étudier une opération sur les fonctions arithmétiques : le produit de convolution.

Si a et b sont deux entiers, on note $a \wedge b$ le plus grand commun diviseur de a et b . On notera bien que pour tout $a \geq 1$, $0 \wedge a = a$.

En l'absence de précisions supplémentaires, lorsque que l'on parle de décomposition de $n \in \mathbb{N}^*$ en facteurs premiers :

$$n = \prod_{i=1}^r p_i^{\alpha_i}$$

il sera implicite que pour tout $i \in \llbracket 1, r \rrbracket$, les α_i sont des entiers non nuls et les p_i des nombres premiers distincts.

On dit que $n \in \mathbb{N}^*$ a un facteur carré si et seulement si il existe $k \in \mathbb{N}^*$ tel que k^2 divise n .

On rencontrera souvent le symbole $\sum_{d|n}$, cela signifiera que la somme porte sur les entiers $d \geq 1$ qui divisent n .

A-L'indicatrice d'Euler

Soit $n \in \mathbb{N}^*$, on définit l'**indicatrice d'Euler** par :

$$\varphi(n) = \text{Card}\{k \in \llbracket 0, n-1 \rrbracket, k \wedge n = 1\}.$$

Autrement dit, $\varphi(n)$ est le nombre d'entiers naturels premiers avec n et inférieurs strictement à n .

- Calculer $\varphi(n)$ pour $1 \leq n \leq 12$, on présentera les résultats sous forme de tableau et on détaillera le calcul uniquement pour $n = 12$.
- Montrer que p est premier si et seulement si $\varphi(p) = p - 1$.
- Soit p premier et $\alpha \in \mathbb{N}^*$.
 - Soit $k \in \mathbb{N}^*$, montrer que k et p^α ne sont pas premiers entre eux si et seulement si p divise k .
 - Dénombrer les multiples de p compris entre 0 et $p^\alpha - 1$.
 - En déduire $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.
- Dans la suite de cette partie, on souhaite trouver une formule pour calculer $\varphi(n)$ pour n quelconque sachant que d'après la question précédente, on connaît une expression de $\varphi(p^\alpha)$ pour p premier. Pour ce faire nous allons d'abord démontrer que φ est une fonction multiplicative, c'est-à-dire que pour $(m, n) \in (\mathbb{N}^*)^2$, on a :

$$m \wedge n = 1 \Rightarrow \varphi(mn) = \varphi(m)\varphi(n).$$

On définit pour tout $n \in \mathbb{N}^*$, l'ensemble :

$$\mathcal{A}(n) = \{k \in \llbracket 0, n-1 \rrbracket, k \wedge n = 1\}.$$

On se donne désormais $(m, n) \in (\mathbb{N}^*)^2$ premiers entre eux et on définit l'application :

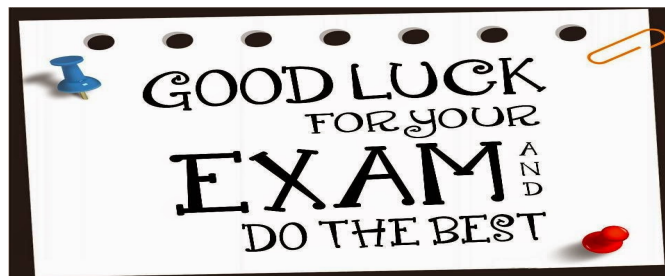
$$f : \begin{array}{ccc} \mathcal{A}(mn) & \rightarrow & \mathcal{A}(m) \times \mathcal{A}(n) \\ x & \mapsto & (r, s) \end{array}$$

où r est le reste de la division euclidienne de x par m et s est le reste de la division euclidienne de x par n .

- (a) Justifier que f est bien définie.
- (b) On veut montrer que f est injective, pour cela on suppose que $f(x) = f(y) = (r, s)$ avec $(x, y) \in \mathcal{A}(mn)^2$.
- i. Ecrire les divisions euclidiennes de x puis y par m et n .
 - ii. En déduire que mn divise $x - y$.
 - iii. Démontrer que $|x - y| \leq mn - 1$.
 - iv. Justifier alors que f est injective.
- (c) On veut montrer que f est surjective, pour cela on se donne $(r, s) \in \mathcal{A}(m) \times \mathcal{A}(n)$.
- i. Justifier l'existence de deux entiers relatifs u et v tels que $um + vn = 1$.
 - ii. Vérifier que $a = sum + rvn$ satisfait : $a = r [m]$ et $a = s [n]$.
 - iii. En déduire que f est surjective.
- (d) Démontrer que φ est multiplicative.
5. Soit $n \geq 2$ et $r \geq 1$, on suppose que la décomposition de n en facteurs premiers s'écrit : $n = \prod_{i=1}^r p_i^{\alpha_i}$.
- (a) Démontrer que :

$$\varphi(n) = n \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right).$$

- (b) Calculer $\varphi(105)$, $\varphi(120)$ et $\varphi(1000)$.
- (c) Démontrer que pour tout $n \geq 3$, $\varphi(n)$ est pair.



Corrigé

Problème 1: Équations dans $\mathcal{P}(E)$

1. (a) On a :

$$\begin{aligned} X \cap Y &= [A \cup (R \cap \bar{S})] \cap [A \cup (\bar{R} \cap S)] && \text{(La définition de } X \text{ et } Y) \\ &= A \cup [(R \cap \bar{S}) \cap (\bar{R} \cap S)] && \text{(Distributivité de } \cup \text{ par rapport à } \cap) \\ &= A \cup [(R \cap \bar{R}) \cap (\bar{S} \cap S)] && \text{(Associativité et commutativité de } \cap) \\ &= A \cup \emptyset = A \end{aligned}$$

(b) Choisissons par exemple $R = X$ et $S = Y$. Alors :

$$\begin{cases} A \cup (R \cap \bar{S}) = (X \cap Y) \cup (X \cap \bar{Y}) = X \cap (Y \cup \bar{Y}) = X \cap E = X \\ A \cup (\bar{R} \cap S) = (X \cap Y) \cup (\bar{X} \cap Y) = (X \cup \bar{X}) \cap Y = E \cap Y = Y \end{cases}$$

(c) Soit A une partie de E .

Le couple (X, Y) est solution de l'équation $X \cap Y = A \Leftrightarrow$

$$\text{il existe deux parties } R \text{ et } S \text{ de } E \text{ telles que } \begin{cases} X = A \cup (R \cap \bar{S}) \\ Y = A \cup (\bar{R} \cap S) \end{cases}$$

2. (a) Soit A une partie de E .

– *Sens direct* : Soient R et S deux parties de E .

On pose $X = A \cap (R \cup \bar{S})$ et $Y = A \cap (\bar{R} \cup S)$. On constate que :

$$\begin{aligned} X \cup Y &= [A \cap (R \cup \bar{S})] \cup [A \cap (\bar{R} \cup S)] = A \cap [(R \cup \bar{S}) \cup (\bar{R} \cup S)] \\ &= A \cap [(R \cup \bar{R}) \cup (\bar{S} \cup S)] = A \cap E = A \end{aligned}$$

– *Réciproque* : Soient X, Y deux parties de E telles que $X \cup Y = A$.

Si on pose $R = X$ et $S = Y$, on observe que :

$$\begin{cases} A \cap (R \cup \bar{S}) = (X \cup Y) \cap (X \cup \bar{Y}) = X \cup (Y \cap \bar{Y}) = X \cup \emptyset = X \\ A \cap (\bar{R} \cup S) = (X \cup Y) \cap (\bar{X} \cup Y) = (X \cap \bar{X}) \cup Y = \emptyset \cup Y = Y \end{cases}$$

– *Conclusion* : $X \cup Y = A \Leftrightarrow$ il existe R, S dans E tels que $\begin{cases} X = A \cap (R \cup \bar{S}) \\ Y = A \cap (\bar{R} \cup S) \end{cases}$

(b) Soit A une partie de E .

$X \cup Y = A$ équivaut à $\bar{X} \cap \bar{Y} = \bar{A}$ et nous ramène à la première question.

Plus précisément :

$$\begin{aligned} X \cup Y = A &\Leftrightarrow \bar{X} \cap \bar{Y} = \bar{A} \\ &\Leftrightarrow \exists P, Q \subset E, \text{ tels que } \begin{cases} \bar{X} = \bar{A} \cup (P \cap \bar{Q}) \\ \bar{Y} = \bar{A} \cup (\bar{P} \cap Q) \end{cases} \quad \left(\begin{array}{l} \text{On utilise le résultat} \\ \text{de la première question} \end{array} \right) \\ &\Leftrightarrow \exists P, Q \subset E, \text{ tels que } \begin{cases} X = A \cap (\bar{P} \cup Q) \\ Y = A \cap (P \cup \bar{Q}) \end{cases} \quad \left(\begin{array}{l} \text{On est passé} \\ \text{aux complémentaires} \end{array} \right) \end{aligned}$$

Ce qui équivaut au résultat attendu, en posant $R = Q$ et $S = P$.

3. (a) i. X_0 vérifie donc $(A \cap X_0) \cup (B \cap \bar{X}_0) = C$.

Dans un premier temps, on en déduit :

$$\begin{aligned}(A \cap B) \cap C &= (A \cap B) \cap [(A \cap X_0) \cup (B \cap \bar{X}_0)] \\ &= (A \cap B \cap A \cap X_0) \cup (A \cap B \cap B \cap \bar{X}_0) \\ &= (A \cap B \cap X_0) \cup (A \cap B \cap \bar{X}_0) \\ &= (A \cap B) \cap (X_0 \cup \bar{X}_0) = (A \cap B) \cap E = A \cap B\end{aligned}$$

Enfin l'égalité $(A \cap B) \cap C = A \cap B$ équivaut à $A \cap B \subset C$.

D'autre part :

$$\left. \begin{array}{l} A \cap X_0 \subset A \\ B \cap \bar{X}_0 \subset B \end{array} \right\} \Rightarrow (A \cap X_0) \cup (B \cap \bar{X}_0) \subset A \cup B. \text{ Donc } C \subset A \cup B$$

On a donc démontré la double inclusion demandée.

ii. Reprenons notre solution X_0 et procédons par ordre.

Puisque $C = (A \cap X_0) \cup (B \cap \bar{X}_0)$, il vient :

$$\begin{aligned}\bar{B} \cap C &= \bar{B} \cap [(A \cap X_0) \cup (B \cap \bar{X}_0)] \\ &= (\bar{B} \cap A \cap X_0) \cup \underbrace{(\bar{B} \cap B \cap \bar{X}_0)}_{=\emptyset} = \bar{B} \cap A \cap X_0\end{aligned}$$

De la même manière :

$$\begin{aligned}B \cap \bar{C} &= B \cap (\bar{A} \cup \bar{X}_0) \cap (\bar{B} \cup X_0) \\ &= B \cap (\bar{A} \cup \bar{X}_0) \cap X_0 \quad (\text{Car } B \cap (\bar{B} \cup X_0) = B \cap X_0) \\ &= B \cap \bar{A} \cap X_0 \quad (\text{Car } (\bar{A} \cup \bar{X}_0) \cap X_0 = \bar{A} \cap X_0)\end{aligned}$$

Soit Z l'ensemble dont on doit montrer qu'il est égal à X_0 .

$$\begin{aligned}Z &= \underbrace{(\bar{B} \cap A \cap X_0)}_{\bar{B} \cap C} \cup \underbrace{(B \cap \bar{A} \cap X_0)}_{B \cap \bar{C}} \cup [X_0 \cap ((A \cap B) \cup (\bar{A} \cap \bar{B}))] \\ &= (X_0 \cap A \cap \bar{B}) \cup (X_0 \cap \bar{A} \cap B) \cup (X_0 \cap A \cap B) \cup (X_0 \cap \bar{A} \cap \bar{B}) \\ &= X_0 \cap \underbrace{[(A \cap \bar{B}) \cup (\bar{A} \cap B) \cup (A \cap B) \cup (\bar{A} \cap \bar{B})]}_{=E} \\ &= X_0 \cap E = X_0, \text{ ce qu'il fallait démontrer}\end{aligned}$$

(b) i. Evaluons d'abord le membre de droite :

$$C \cap [\bar{B} \cup (D \cap A \cap B)] = (C \cap \bar{B}) \cup (C \cap A \cap B \cap D) = (C \cap \bar{B}) \cup (A \cap B \cap D)$$

(On a utilisé $A \cap B \subset C$ et donc $C \cap A \cap B = A \cap B$)

Evaluons maintenant le membre de gauche :

$$\begin{aligned}A \cap X &= A \cap [(\bar{B} \cap C) \cup (B \cap \bar{C}) \cup [D \cap ((A \cap B) \cup (\bar{A} \cap \bar{B}))]] \\ &= A \cap [(\bar{B} \cap C) \cup (B \cap \bar{C}) \cup (D \cap A \cap B) \cup (D \cap \bar{A} \cap \bar{B})] \\ &= (A \cap \bar{B} \cap C) \cup (A \cap B \cap \bar{C}) \cup (A \cap B \cap D)\end{aligned}$$

(Dans le développement on a utilisé $A \cap D \cap \bar{A} \cap \bar{B} = \emptyset$.)

On sait que $A \cap B \subset C$. On en déduit $A \cap B \cap \bar{C} = \emptyset$.

D'autre part :

$$C \subset A \cup B \Rightarrow C \cap \bar{B} \subset (A \cup B) \cap \bar{B} = A \cap \bar{B} \subset A$$

Ce qui implique $C \cap \bar{B} \cap A = C \cap \bar{B}$

Puis $A \cap X = (C \cap \bar{B}) \cup (A \cap B \cap D)$, ce qui répond à la question.

ii. Puisque $X = (\bar{B} \cap C) \cup (B \cap \bar{C}) \cup (D \cap A \cap B) \cup (D \cap \bar{A} \cap \bar{B})$,

il vient : $X \cup \bar{B} = \bar{B} \cup (B \cap \bar{C}) \cup (D \cap A \cap B)$

(dans le développement, \bar{B} a "absorbé" $\bar{B} \cap C$ et $D \cap \bar{A} \cap \bar{B}$.)

iii. Puisque $\bar{X} = (B \cup \bar{C}) \cap (\bar{B} \cup C) \cap (\bar{D} \cup \bar{A} \cup \bar{B}) \cap (\bar{D} \cup A \cup B)$, Il vient :

$$\begin{aligned} B \cap \bar{X} &= B \cap (\bar{B} \cup C) \cap (\bar{D} \cup \bar{A} \cup \bar{B}) \quad \left(\begin{array}{l} B \text{ a "absorbé"} \\ B \cup \bar{C} \text{ et } \bar{D} \cup A \cup B \end{array} \right) \\ &= C \cap B \cap (\bar{D} \cup \bar{A} \cup \bar{B}) \quad (\text{car } B \cap (\bar{B} \cup C) = B \cap C) \\ &= (C \cap B \cap \bar{D}) \cup (C \cap B \cap \bar{A}) \quad (\text{car } C \cap B \cap \bar{B} = \emptyset) \end{aligned}$$

Or $C \subset A \cup B$. Donc $C \cap \bar{A} \subset (A \cup B) \cap \bar{A} = B \cap \bar{A}$.

On en déduit $C \cap \bar{A} \cap B \cap \bar{A} = C \cap \bar{A}$, c'est-à-dire $C \cap \bar{A} \cap B = C \cap \bar{A}$.

Finalement :

$$\begin{aligned} B \cap \bar{X} &= (C \cap B \cap \bar{D}) \cup (C \cap \bar{A}) \\ &= C \cap [\bar{A} \cup (\bar{D} \cap B)] \quad (\text{ce qu'il fallait démontrer.}) \end{aligned}$$

(c) On déduit des questions (i) et (iii) que :

$$\begin{aligned} (A \cap X) \cup (B \cap \bar{X}) &= [C \cap [\bar{B} \cup (D \cap A \cap B)]] \cup [C \cap [\bar{A} \cup (\bar{D} \cap B)]] \\ &= C \cap [\bar{B} \cup (D \cap A \cap B) \cup \bar{A} \cup (\bar{D} \cap B)] \\ &= C \cap \underbrace{[\bar{A} \cap \bar{B} \cup ((A \cap B) \cap D)]}_{\bar{A} \cap \bar{B} \cup D} \cup (\bar{D} \cap B) \\ &= C \cap \underbrace{[\bar{A} \cap \bar{B} \cup D \cup (\bar{D} \cap B)]}_{D \cup B} \\ &= C \cap \underbrace{(\bar{A} \cup \bar{B} \cup D \cup B)}_E = C \end{aligned}$$

(d) Des questions précédentes, on tire :

L'équation $A \cap X \cup (B \cap \bar{X})$ possède au moins une solution \Leftrightarrow

A, B et C vérifient la double inclusion : $A \cap B \subset C \subset A \cap B$.

(e) Supposons que la condition $A \cap B \subset C \subset A \cap B$ soit réalisée.

Alors l'ensemble des solutions est l'ensemble des parties X de E de la forme :

$$X = (\bar{B} \cap C) \cup (B \cap \bar{C}) \cup [D \cap ((A \cap B) \cup (\bar{A} \cap \bar{B}))],$$

où D est une partie quelconque de E .

Problème 2:

1. $\mathcal{M} = \mathcal{P}(E)$ convient.

2. (a) – *Réflexivité*

Soit A dans $\mathcal{P}(E)$. Puisque $\mathcal{M} \neq \emptyset$, soit X un élément de \mathcal{M} .

On a... $A \cap X = A \cap X$, ce qui prouve $A \mathcal{R} A$.

– *Symétrie* : Elle est évidente par définition (car X, Y jouent le même rôle.)

– *Transitivité*

Soient A, B, C dans $\mathcal{P}(E)$, tels que : $A \mathcal{R} B$ et $B \mathcal{R} C$.

Il existe X et Y dans \mathcal{M} tels que $A \cap X = B \cap X$ et $B \cap Y = C \cap Y$.

On sait qu'il existe Z dans \mathcal{M} tel que $Z \subset X \cap Y$.

$$\text{On en déduit } \begin{cases} A \cap X \cap Z = B \cap X \cap Z \\ B \cap Y \cap Z = C \cap Y \cap Z \end{cases}$$

$$\text{puis } \begin{cases} A \cap Z = B \cap Z \\ B \cap Z = C \cap Z \end{cases} \quad \text{car } X \cap Z = Z \text{ et } Y \cap Z = Z.$$

Ainsi $A \cap Z = C \cap Z$, et Z est élément de \mathcal{M} . Donc $A \mathcal{R} C$.

– *Conclusion* : \mathcal{R} est une relation d'équivalence sur $\mathcal{P}(E)$.

(b) – *Supposons* $\mathcal{M} = \{E\}$

Pour tous A et B de $\mathcal{P}(E)$, $A \mathcal{R} B \Leftrightarrow A \cap E = B \cap E \Leftrightarrow A = B$.

La relation \mathcal{R} est donc l'égalité.

– *Réciproquement*

On suppose que \mathcal{M} est différent de $\{E\}$. Montrons que \mathcal{R} n'est pas l'égalité.

Puisque $\mathcal{M} \neq \emptyset$, il existe X dans \mathcal{M} , avec $X \neq E$.

On constate que $X \mathcal{R} E$ (car $X \cap X = E \cap X$ et $X \in \mathcal{M}$.)

Or X et E sont distincts : \mathcal{R} n'est pas donc pas la relation égalité.

– *Conclusion* : \mathcal{R} est la relation "égalité" $\Leftrightarrow \mathcal{M}$ se réduit au singleton $\{E\}$.

(c) – *Supposons* $\emptyset \in \mathcal{M}$

Pour tous A, B de $\mathcal{P}(E)$ on a alors $A \mathcal{R} B$ car $A \cap \emptyset = B \cap \emptyset$.

\mathcal{R} est donc l'équivalence universelle.

– *Réciproquement*

Supposons que \mathcal{R} soit l'équivalence universelle dans $\mathcal{P}(E)$. Alors en particulier $\emptyset \mathcal{R} E$.

Il existe donc un élément X de $\mathcal{P}(E)$ tel que $E \cap X = \emptyset \cap X$.

Mais cela signifie que $X = \emptyset$. Donc $\emptyset \in \mathcal{M}$.

– *Conclusion* : \mathcal{R} est l'équivalence universelle $\Leftrightarrow \emptyset$ est élément de \mathcal{M} .

3. (a) – *Classe de* E

$$\begin{aligned} A \in \widehat{E} &\Leftrightarrow \exists X \in \mathcal{M} \text{ tel que } A \cap X = E \cap X \\ &\Leftrightarrow \exists X \in \mathcal{M} \text{ tel que } A \cap X = X \Leftrightarrow \exists X \in \mathcal{M} \text{ tel que } X \subset A \end{aligned}$$

\widehat{E} est donc formée des parties de E contenant au moins un élément de \mathcal{M} .

En particulier tous les éléments de \mathcal{M} sont dans la classe de E .

– Classe de \emptyset

$$A \in \widehat{\emptyset} \Leftrightarrow \exists X \in \mathcal{M} \text{ tel que } A \cap X = \emptyset \cap X \Leftrightarrow \exists X \in \mathcal{M} \text{ tel que } A \cap X = \emptyset$$

$\widehat{\emptyset}$ est donc l'ensemble des parties de E qui ont une intersection vide avec au moins un élément de \mathcal{M} .

(b) Soient A et B deux éléments de \widehat{E} .

Comme on l'a vu, il existe X et Y dans \mathcal{M} tels que $X \subset A$ et $Y \subset B$.

On sait qu'il existe un élément Z de \mathcal{M} tel que $Z \subset X \cap Y$.

On a donc $Z \subset A \cap B$, ce qui prouve que $A \cap B$ appartient à \widehat{E} .

(c) Il s'agit de démontrer que pour tous A, B de $\mathcal{P}(E)$, $A \mathcal{R} B \Leftrightarrow A \mathcal{S} B$.

– Supposons $A \mathcal{R} B$

Alors il existe X dans \mathcal{M} tel que $A \cap X = B \cap X$.

On X est aussi élément de $N = \widehat{E}$ (car X contient X !). Donc $A \mathcal{S} B$.

– Supposons $A \mathcal{S} B$

Alors il existe X dans \mathcal{N} tel que $A \cap X = B \cap X$.

Par définition, il existe un élément Y de \mathcal{M} tel que $Y \subset X$.

On en déduit $A \cap X \cap Y = B \cap X \cap Y$ puis $A \cap Y = B \cap Y$. Donc $A \mathcal{R} B$.

– Conclusion : Les relations \mathcal{R} et \mathcal{S} sont identiques.

4. (a) Il s'agit de démontrer que pour tous A, B de $\mathcal{P}(E)$, $A \mathcal{R} B \Leftrightarrow A \mathcal{T} B$.

Pour toutes parties A et B de E et tout élément X de \mathcal{M} :

$$\begin{aligned} (A \Delta B) \cap X = \emptyset &\Leftrightarrow [(A \cap \bar{B}) \cup (\bar{A} \cap B)] \cap X = \emptyset \\ &\Leftrightarrow (A \cap \bar{B} \cap X) \cup (\bar{A} \cap B \cap X) = \emptyset \\ &\Leftrightarrow A \cap \bar{B} \cap X = \emptyset \text{ et } \bar{A} \cap B \cap X = \emptyset \\ &\Leftrightarrow A \cap X \subset B \text{ et } B \cap X \subset A. \end{aligned}$$

On aura terminé la démonstration quand on aura prouvé l'équivalence :

$$(A \cap X \subset B \text{ et } B \cap X \subset A) \Leftrightarrow A \cap X = B \cap X$$

Dans le sens \Leftarrow : c'est évident.

Dans le sens \Rightarrow :

$$\left. \begin{array}{l} A \cap X \subset B \\ B \cap X \subset A \end{array} \right\} \Rightarrow \left. \begin{array}{l} A \cap X \cap X \subset B \cap X \\ B \cap X \cap X \subset A \cap X \end{array} \right\} \Rightarrow \left. \begin{array}{l} A \cap X \subset B \cap X \\ B \cap X \subset A \cap X \end{array} \right\} \Rightarrow A \cap X = B \cap X$$

Les relations \mathcal{R} et \mathcal{T} sont donc identiques.

(b) Par hypothèse, il existe X et Y dans \mathcal{M} tels que : $(S) \begin{cases} A \cap X = A' \cap X \\ B \cap Y = B' \cap Y \end{cases}$

On sait qu'il existe Z dans \mathcal{M} tel que $Z \subset X \cap Y$.

Le système (S) implique alors $(\Sigma) \begin{cases} A \cap Z = A' \cap Z \\ B \cap Z = B' \cap Z \end{cases}$

– Intersection

$$\begin{aligned}(\Sigma) \Rightarrow A \cap Z \cap B \cap Z &= A' \cap Z \cap B' \cap Z \\ \Rightarrow (A \cap B) \cap Z &= (A' \cap B') \cap Z\end{aligned}$$

On en déduit $(A \cap B) \mathcal{R} (A' \cap B')$.

– Réunion

$$\begin{aligned}(S) \Rightarrow (A \cap Z) \cup (B \cap Z) &= (A' \cap Z) \cup (B' \cap Z) \\ \Rightarrow (A \cup B) \cap Z &= (A' \cup B') \cap Z\end{aligned}$$

On en déduit $(A \cup B) \mathcal{R} (A' \cup B')$.

– Complémentaire

Pour toutes parties C et D de E , on remarque que $C \Delta D = \bar{C} \Delta \bar{D}$.

Dans ces conditions :

$$\begin{aligned}A \mathcal{R} A' \Rightarrow A \mathcal{T} A' \Rightarrow \exists X \in \mathcal{M} \text{ tel que } (A \Delta A') \cap X &= \emptyset \\ \Rightarrow \exists X \in \mathcal{M} \text{ tel que } (\bar{A} \Delta \bar{A}') \cap X &= \emptyset \Rightarrow \bar{A} \mathcal{T} \bar{A}' \Rightarrow \bar{A} \mathcal{R} \bar{A}'\end{aligned}$$

– Différence symétrique

On utilise les résultats précédents :

$$\begin{aligned}\begin{cases} A \mathcal{R} A' \\ B \mathcal{R} B' \end{cases} &\Rightarrow \begin{cases} A \mathcal{R} A' \text{ et } \bar{B} \mathcal{R} \bar{B}' \\ B \mathcal{R} B' \text{ et } \bar{A} \mathcal{R} \bar{A}' \end{cases} \Rightarrow \begin{cases} (A \cap \bar{B}) \mathcal{R} (A' \cap \bar{B}') \\ (B \cap \bar{A}) \mathcal{R} (B' \cap \bar{A}') \end{cases} \\ &\Rightarrow (A \cap \bar{B}) \cup (B \cap \bar{A}) \mathcal{R} (A' \cap \bar{B}') \cup (B' \cap \bar{A}')\end{aligned}$$

Ce dernier résultat n'est autre que $(A \Delta B) \mathcal{R} (A' \Delta B')$.

5. (a) Si $\mathcal{M} = \{E\}$, \mathcal{R} est l'égalité. Il y a donc autant de classes que de parties de E .

Plus précisément : pour toute partie A de E , $\hat{A} = \{A\}$.

(b) Si $\emptyset \in \mathcal{M}$, \mathcal{R} est l'équivalence universelle.

Il n'a donc qu'une seule classe d'équivalence, à savoir $\mathcal{P}(E)$.

(c) Pour toutes parties A et B de E ,

$$A \mathcal{R} B \Leftrightarrow A \cap \{x\} = B \cap \{x\} \Leftrightarrow (x \in A \cap B) \text{ ou } (x \notin A \text{ et } x \notin B)$$

Il y a donc deux classes d'équivalence :

– Celle formée des parties de E qui contiennent x .

– Celle formée des parties de E qui ne contiennent pas x .

(d) On suppose donc que $\{x\}$ et $\{y\}$ sont deux éléments de \mathcal{M} .

Mais on sait qu'il existe Z dans \mathcal{M} tel que $Z \subset \{x\} \cap \{y\}$.

Dans ce cas cela signifie que $\emptyset \in \mathcal{M}$.

On est ainsi ramené au cas (b).

Problème 3:

I. Définition des sous-groupes distingués

- Il suffit évidemment de montrer l'équivalence des conditions *i*) et *ii*).
 - On suppose que l'hypothèse *i*) est vérifiée. Soit a dans G .
Avec l'hypothèse, $a^{-1}H \subset Ha^{-1}$. On multiplie par a à gauche et à droite.
On en déduit $a(a^{-1}H)a \subset a(Ha^{-1})a$ c'est-à-dire $Ha \subset aH$.
 - C'est la même démonstration pour passer de *ii*) à *i*).
On part de $Ha^{-1} \subset a^{-1}H$ qui découle de *ii*) et on multiplie par a des deux cotés.
- On suppose que H est distingué dans G .
 - Pour tout a de G : $aHa^{-1} = a(Ha^{-1}) = a(a^{-1}H) = (aa^{-1})H = H$.
 - La condition *ii*) implique évidemment la condition *iii*).
 - On suppose que la condition *iii*) est vérifiée.
Pour tout a de G : $aH \supset a(a^{-1}Ha)$, et $a(a^{-1}Ha) = (aa^{-1})Ha = Ha$.
On en déduit $aH \supset Ha$: H est donc distingué, ce qui achève la démonstration.
 - Les automorphismes intérieurs de G sont les $\varphi_a : x \mapsto axa^{-1}$.
Soit H un sous-groupe de G . Pour tout a de G , on a $\varphi_a(H) = aHa^{-1}$.
Donc H est distingué \Leftrightarrow il vérifie les deux conditions équivalentes suivantes :
 - H est *stable* par les automorphismes intérieurs : $\forall a \in G, \varphi_a(H) \subset H$.
 - H est *invariant* par les automorphismes intérieurs : $\forall a \in G, \varphi_a(H) = H$.

II. Exemples de sous-groupes distingués

- Pour tout a de G : $a\{e\} = \{e\}a = \{a\}$. Le sous-groupe $\{e\}$ est distingué dans G .
Pour tout a de G , $x \mapsto ax$ et $x \mapsto xa$ sont des bijections de G dans lui-même.
On a donc $aG = Ga = G$: le groupe G est un sous-groupe distingué de G .
- Si G était abélien, tout sous-groupe H de G serait distingué ($aH = Ha$ étant évident)
- (a) H est un sous-groupe de G (image réciproque de \tilde{H} par un morphisme de groupes.)
Soit a un élément de G . Il reste à montrer, par exemple, que $aHa^{-1} \subset H$.
Pour tout h de H , on a : $f(aha^{-1}) = f(a)f(h)f(a^{-1}) = bf(h)b^{-1}$, en notant $b = f(a)$.
Or $\tilde{h} = f(h)$ est dans \tilde{H} qui est distingué dans \tilde{G} .
On en déduit $f(aha^{-1}) = b\tilde{h}b^{-1} \in \tilde{H}$.
Autrement dit, aha^{-1} est dans H , ce qui prouve que H est distingué.
- (b) \tilde{H} est un sous-groupe de \tilde{G} (image directe de H par un morphisme de groupes.)
Soient \tilde{a} dans \tilde{G} et \tilde{h} dans \tilde{H} . Il suffit de montrer que $\tilde{a}\tilde{h}\tilde{a}^{-1}$ est dans \tilde{H} .
 f étant surjective, il existe a dans G et h dans H tels que $\tilde{a} = f(a)$ et $\tilde{h} = f(h)$.
On en déduit $\tilde{a}^{-1} = f(a^{-1})$ puis $\tilde{a}\tilde{h}\tilde{a}^{-1} = f(a)f(h)f(a^{-1}) = f(aha^{-1})$.
Hors H est distingué. Il en résulte que aha^{-1} est dans H .
On en déduit que $\tilde{a}\tilde{h}\tilde{a}^{-1}$ est dans \tilde{H} , ce qui prouve que \tilde{H} est distingué.
- (c) $\{e_{\tilde{G}}\}$ est un sous-groupe distingué de \tilde{G} .
Ainsi $\ker f = f^{-1}(\{e_{\tilde{G}}\})$ est un sous-groupe distingué de G .

III. Centre et centralisateurs

1. (a) Le neutre e commute avec tous les éléments de X , donc il est dans X' .
Soient a et b deux éléments de X' . Pour tout x de X :
 \diamond On a $ax = xa$ donc $x = a^{-1}xa$ puis $xa^{-1} = a^{-1}x$. Ainsi $a^{-1} \in X'$.
 \diamond On a $(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$. Ainsi $ab \in X'$.
L'ensemble X' est non vide, stable pour la loi de G et pour le passage à l'inverse.
 X' est donc un sous-groupe de G .
 - (b) Il reste à montrer que le sous-groupe C de G est distingué.
Or : $\forall a \in C, \forall x \in G, ax = xa$ (car a commute avec tous les x de G).
Pour tout x de G , on a donc $xC = Cx$, ce qui achève la démonstration.
Remarque 1 : la restriction à C d'un automorphisme intérieur est l'identité.
2. On sait que $\varphi : a \mapsto \varphi_a$ est un morphisme de G dans le groupe $\text{Aut}(G)$.
Soit a dans $C : a \in C \Leftrightarrow \forall x \in G, ax = xa \Leftrightarrow \forall x \in G, axa^{-1} = x \Leftrightarrow \varphi_a = \text{Id}$.
Ainsi le centre de G est le noyau du morphisme φ .
Or on sait (II.3.c) que le noyau d'un morphisme de groupes est un sous-groupe distingué.
3. (a) Supposons $X \subset Y$. Soit y' un élément de Y .
 y' commute avec tous les éléments de Y donc à fortiori avec ceux de X .
Autrement dit, y' est un élément de X' . On a donc $Y' \subset X'$.
 - (b) Soit x un élément de X . Par définition de X' , x commute avec les éléments de X' .
Autrement dit x appartient au centralisateur X'' de X' .
On a donc l'inclusion $X \subset X''$.
 - (c) En utilisant la question précédente, avec X' à la place de X , on trouve $X' \subset X'''$.
D'autre part, on sait que X est inclus dans X'' (question b).
La question a) donne alors $(X'')' \subset X'$, c'est-à-dire $X''' \subset X'$.
Finalement on a l'égalité $X''' = X'$.
4. (a) – Si H est abélien, tout élément x de H commute avec tous les éléments de H .
Tout x de H est donc dans H' : on a l'inclusion $H \subset H'$.
– Si on a $H \subset H'$, alors $H'' \subset H'$ (question précédente).
Or les éléments de H'' commutent avec ceux de H' ($H'' = \text{centralisateur de } H'$).
 $H'' \subset H' \Rightarrow$ à fortiori tout élément de H'' commute avec tout élément de H'' .
Le groupe H'' est donc abélien.
– Enfin supposons que le groupe H'' soit abélien.
Puisque $H \subset H''$, il en découle que le groupe H est abélien.
- (b) On sait déjà que H' est un sous-groupe de G .
Pour montrer que H' est distingué, on se donne x dans G et a dans H' .
Il faut montrer que $y = xax^{-1} \in H'$, donc que y commute avec les éléments de H .
Soit h un élément quelconque de H . Tout d'abord $yh = (xax^{-1})h = xa(x^{-1}hx)x^{-1}$.
L'élément $x^{-1}hx$ est dans H car H est distingué.
Il en découle que a , qui est dans H' , commute avec $x^{-1}hx$.
Ainsi $yh = x(x^{-1}hx)ax^{-1} = hxax^{-1} = hy$, ce qu'il fallait démontrer.
Conclusion : H' est un sous-groupe distingué de G .

IV. Produit de deux sous-groupes

1. Par symétrie, il suffit bien sûr de prouver $HK \subset KH \Rightarrow KH \subset HK$.

On suppose donc que l'inclusion $HK \subset KH$ est vraie.

Soit $x = kh$ un élément de KH , avec k dans K et h dans H .

L'inverse de x s'écrit $x^{-1} = h^{-1}k^{-1}$ et est donc un élément de HK .

On en déduit $x^{-1} \in KH$, donc $x^{-1} = k'h'$, avec $k' \in K$ et $h' \in H$.

En passant à nouveau à l'inverse, on voit que $x = h'^{-1}k'^{-1}$ est un élément de HK .

On a donc prouvé l'inclusion $KH \subset HK$, ce qui achève la démonstration.

2. – On suppose que HK est un sous-groupe de G .

Il suffit par exemple de prouver l'inclusion $HK \subset KH$.

Soit x un élément de HK . Son inverse est donc dans HK .

Ainsi il existe h dans H et k dans K tels que $x^{-1} = hk$.

En passant à l'inverse, on en déduit que $x = k^{-1}h^{-1}$ est un élément de KH .

On a ainsi obtenu l'inclusion $HK \subset KH$, donc l'égalité $HK = KH$.

- On suppose maintenant qu'on a l'égalité $HK = KH$.

L'ensemble HK est bien sûr non vide.

Soient x et y dans HK . Il faut prouver que xy^{-1} est dans HK .

Il existe (h, h') dans H^2 et (k, k') dans K^2 tels que $x = hk$ et $y = h'k'$.

On a alors $xy^{-1} = hkk'^{-1}h'^{-1}$.

Or kk'^{-1} est dans K et h'^{-1} est dans H .

L'élément $kk'^{-1}h'^{-1}$ est dans KH donc dans HK .

Ainsi il existe h'' dans H et k'' dans K tels que $kk'^{-1}h'^{-1} = h''k''$.

On en déduit $xy^{-1} = h(h''k'') = (hh'')k''$, ce qui est bien un élément de HK .

Conclusion : HK est un sous-groupe de G .

3. Sans perdre de généralité, on peut supposer que H est distingué.

On va prouver l'inclusion $HK \subset KH$, qui on le sait équivaut à l'égalité $HK = KH$.

Soit $x = hk$ un élément de HK , avec h dans H et k dans K .

On en déduit $x^{-1} = k^{-1}h^{-1} = (k^{-1}h^{-1}k)k^{-1}$.

Or H est distingué. L'élément $h' = k^{-1}h^{-1}k$ est donc dans H .

On en déduit $x^{-1} = h'k^{-1}$ puis $x = kh'^{-1}$, ce qui prouve que x est dans KH .

Ainsi $HK \subset KH$, et finalement l'égalité $HK = KH$.

Conclusion : si H ou K est distingué, alors HK est un sous-groupe de G .

V. Quotient par un sous-groupe distingué

1. – Pour tout x de G , on a $x\mathcal{R}x$ car $x^{-1}x = e \in H$: la relation \mathcal{R} est réflexive.

– Soient x, y dans G tels que $x\mathcal{R}y$, c'est-à-dire tels que $z = x^{-1}y \in H$.

H étant un groupe, $z^{-1} = y^{-1}x$ est dans G . Donc $y\mathcal{R}x$: la relation \mathcal{R} est symétrique.

– Soient x, y, z dans G tels que $x\mathcal{R}y$, et $y\mathcal{R}z$.

On a donc $x^{-1}y \in H$ et $y^{-1}z \in H$.

Par stabilité, il en découle $x^{-1}yy^{-1}z \in H$, donc $x^{-1}z \in H$ donc $x\mathcal{R}z$.

Ainsi la relation \mathcal{R} est transitive. Finalement c'est une relation d'équivalence.

– Si $H = G$, alors pour tous x, y de G on a $x\mathcal{R}y$: \mathcal{R} est la relation "universelle".

Si $H = \{e\}$, alors $x\mathcal{R}y \Leftrightarrow x^{-1}y = e \Leftrightarrow x = y$: \mathcal{R} est la relation "égalité".

2. Soit a un élément de G . Pour tout y de G :

$$y \in \bar{a} \Leftrightarrow a^{-1}y \in H \Leftrightarrow \exists h \in H, a^{-1}y = h \Leftrightarrow \exists h \in H, y = ah \Leftrightarrow y \in aH$$

On trouve donc : $\forall a \in G, \bar{a} = aH$.

3. (a) Soient x, x', y, y' quatre éléments de G . On suppose que $x\mathcal{R}x'$ et $y\mathcal{R}y'$.

Cela signifie que $x' \in xH$ et $y' \in yH$ ou ce qui revient au même $yH = y'H$.

On en déduit $x'y' \in (xH)y'$, donc $x'y' \in x(Hy')$.

Ainsi $x'y' \in x(y'H)$ car H est distingué.

Or $y'H = yH$. On en déduit $x'y' \in x(yH)$, donc $x'y' \in (xy)H$ donc $\overline{x'y'} = \overline{xy}$.

Ainsi la classe \overline{xy} ne dépend pas du choix de x dans \bar{x} ni de celui de y dans \bar{y} .

En posant $\bar{x} \bar{y} = \overline{xy}$, on a donc défini une loi interne sur G/H .

On peut également écrire que cette loi est définie par $(xH)(yH) = (xy)H$.

(b) – Pour tous x, y, z dans G , on a :

$$\bar{x} (\bar{y} \bar{z}) = \bar{x} (\overline{yz}) = \overline{x(yz)} = \overline{(xy)z} = \overline{xy} \bar{z} = (\bar{x} \bar{y}) \bar{z}.$$

La loi de G/H est donc associative.

– Pour tout x de G : $\bar{x} \bar{e} = \overline{x e} = \bar{x} = \overline{e x} = \bar{e} \bar{x}$.

On constate donc que $\bar{e} = eH = H$ est le neutre de G/H .

– Pour tout x de G : $\overline{x^{-1} x} = \overline{x^{-1} x} = \bar{e} = \overline{x x^{-1}} = \bar{x} \overline{x^{-1}}$.

On constate donc que l'inverse de \bar{x} existe et est égal à $\overline{x^{-1}}$.

(c) Soient x, y deux éléments de G . On a les équivalences :

$$\bar{x} \bar{y} = \bar{y} \bar{x} \Leftrightarrow \overline{xy} = \overline{yx} \Leftrightarrow (xy)^{-1}yx \in H \Leftrightarrow y^{-1}x^{-1}yx \in H$$

G/H est donc commutatif $\Leftrightarrow H$ contient tous les $y^{-1}x^{-1}yx$, avec $(x, y) \in G^2$.

Problème 4:

A-L'indicatrice d'Euler

Le but de cette partie est d'étudier l'indicatrice d'Euler nommée ainsi en l'honneur du mathématicien suisse qui l'a étudiée en premier. Le point clé est le caractère multiplicatif de φ démontré à la question 4., il suffit ainsi de décomposer un entier n en facteurs premiers pour connaître $\varphi(n)$.

1. Voici les premières valeurs de l'indicatrice d'Euler :

n	1	2	3	4	5	6	7	8	9	10	11	12
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

Pour $n = 12$, il y a uniquement 4 entiers compris entre 0 et 11 qui sont premiers avec 12, ce sont : 1, 5, 7 et 11.

2. On procède par double implication :

(\Rightarrow) On suppose que p est premier, alors pour tout $i \in \llbracket 1, p-1 \rrbracket$, on a $p \wedge i = 1$. Par contre $0 \wedge p = p \neq 1$. Ceci montre que $\varphi(p) = p - 1$.

(\Leftarrow) Réciproquement, on suppose que $\varphi(p) = p - 1$ avec $p \in \mathbb{N}^*$. On remarque déjà que $p \geq 2$ puisque $\varphi(1) = 1$. On a alors pour tout $k \in \llbracket 1, p-1 \rrbracket$, $p \wedge k = 1$, ce qui démontre que p n'a pas de diviseur positif autre que 1 ou lui-même. Ceci implique que p est premier.

Finalement :

$$p \text{ premier} \Leftrightarrow \varphi(p) = p - 1$$

3. (a) On procède par double implication :

(\Rightarrow) On suppose que k et p^α ne sont pas premiers entre eux, il existe un entier $a \geq 2$ tel que $a|k$ et $a|p^\alpha$. Les seuls diviseurs positifs de p^α sont les p^i où $i \in \llbracket 0, \alpha \rrbracket$, ainsi $a = p^\beta$ avec $1 \leq \beta \leq \alpha$ et par suite $p|a$. Par transitivité de la relation de divisibilité, on a bien $p|k$.

(\Leftarrow) Réciproquement, on suppose que p divise k alors il est clair que k et p^α ne sont pas premiers entre eux, puisque tous deux divisibles par p .

On a montré que :

$$k \wedge p^\alpha \neq 1 \Leftrightarrow p|k$$

(b) Les multiples de p compris entre 0 et $p^\alpha - 1$ sont les cp où c est un entier compris entre 0 et $p^{\alpha-1} - 1$. Déjà il est clair que ces entiers sont bien des multiples de p qui n'excèdent pas $p^\alpha - 1$ puisque :

$$(p^{\alpha-1} - 1)p = p^\alpha - p \leq p^\alpha - 1.$$

Ce sont les seuls car le suivant $p^{\alpha-1}p$ est supérieur à $p^\alpha - 1$. D'où :

$$\text{il y a } p^{\alpha-1} \text{ multiples de } p \text{ entre } 0 \text{ et } p^\alpha - 1$$

(c) Parmi les p^α entiers $k \in \llbracket 0, p^\alpha - 1 \rrbracket$, ceux qui ne sont pas premiers avec p^α sont les multiples de p d'après la question 3.(a), il y en a $p^{\alpha-1}$ d'après la question 3.(b). Les entiers $k \in \llbracket 0, p^\alpha - 1 \rrbracket$ premiers avec p^α sont donc au nombre de $p^\alpha - p^{\alpha-1}$. Cela revient à dire que :

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$$

On remarque que l'on retrouve le résultat de la question 2. lorsque $\alpha = 1$.

4. (a) Il s'agit de montrer que $r \in \mathcal{A}(m)$ et $s \in \mathcal{A}(n)$. Démontrons uniquement la première assertion, la seconde s'en déduira par symétrie. Soit $x \in \mathcal{A}(mn)$, effectuons la division euclidienne de x par m , cela donne :

$$x = am + r, \text{ avec } a \in \mathbb{N} \text{ et } r \in \llbracket 0, m-1 \rrbracket.$$

On a immédiatement $r \in \llbracket 0, m-1 \rrbracket$. De plus r est premier avec m , en effet par l'absurde si $b \geq 2$ est un diviseur commun de m et r alors b divise aussi x , ceci est exclu puisque x est premier avec mn . On vient de montrer que $r \in \mathcal{A}(m)$. Ainsi :

f est bien à valeurs dans $\mathcal{A}(m) \times \mathcal{A}(n)$

- (b) i. D'après le théorème de la division euclidienne, il existe $(a, \tilde{a}, b, \tilde{b}) \in \mathbb{N}^4$ tels que :

$$x = am + r, \quad x = bn + s, \quad y = \tilde{a}m + r \quad \text{et} \quad y = \tilde{b}n + s.$$

- ii. On a avec les notations précédentes : $x - y = (a - \tilde{a})m$ et $x - y = (b - \tilde{b})n$.

Ceci montre que $m|x - y$ et $n|x - y$, or m et n sont premiers entre eux donc d'après un corollaire du théorème de Gauss, on a : $mn|x - y$.

- iii. Comme x et y appartiennent à $\mathcal{A}(mn)$, on a : $0 \leq x \leq mn - 1$ et $0 \leq y \leq mn - 1$. Par soustraction, on obtient :

$$-(mn - 1) \leq x - y \leq mn - 1 \Leftrightarrow |x - y| \leq mn - 1.$$

- iv. D'après les deux questions précédentes, on sait que $mn|x - y$ et que $x - y \in \llbracket -(mn - 1), mn - 1 \rrbracket$, cela implique que $x - y = 0$. On a montré finalement que pour tout $(x, y) \in \mathcal{A}(mn)^2$, $f(x) = f(y) \Rightarrow x = y$, d'où :

f est injective

- (c) i. Les entiers m et n sont premiers entre eux, on a donc la relation de Bézout :

$$um + vn = 1$$

avec $(u, v) \in \mathbb{Z}^2$.

- ii. On a les égalités suivantes modulo m :

$$a = sum + rvn = rvn = r(1 - um) = r - rum = r \pmod{m}.$$

De même :

$$a = sum + rvn = sum = s(1 - vn) = s - svn = s \pmod{n}.$$

Ce qui donne le résultat souhaité.

- iii. L'entier a semble être un antécédent de (r, s) cependant il n'appartient pas a priori à $\mathcal{A}(mn)$. Effectuons la division euclidienne de a par mn , il existe $q \in \mathbb{Z}$ tel que :

$$a = qmn + \hat{a}, \text{ avec } \hat{a} \in \llbracket 0, mn - 1 \rrbracket.$$

Montrons que \hat{a} est un antécédent de (r, s) par f , on a :

$$\hat{a} = a - qmn = a \pmod{m} \quad \text{et} \quad \hat{a} = a - qmn = a \pmod{n}.$$

De plus \hat{a} est premier avec mn , pour le démontrer raisonnons par l'absurde. Si t est un nombre premier qui divise \hat{a} et mn , alors $t|a$ puisque $a = qmn + \hat{a}$. De plus comme t est premier $t|mn \Rightarrow t|m$ ou $t|n$, disons m sans perte de généralité. On reprend alors la relation $a = r \pmod{m}$ qui montre que t divise également r , ceci est absurde puisque par hypothèse $r \in \mathcal{A}(m)$ donc m et r sont premiers entre eux.

Finalement, on a bien $\hat{a} \in \mathcal{A}(mn)$ et $f(\hat{a}) = (r, s)$, on a démontré que :

f est surjective

- (d) Finalement f est bijective, or deux ensembles finis qui sont en bijection ont le même nombre d'éléments, ainsi :

$$\text{Card}(\mathcal{A}(mn)) = \text{Card}(\mathcal{A}(m)) \times \text{Card}(\mathcal{A}(n)).$$

Par définition, cette dernière égalité est exactement :

$$\varphi(mn) = \varphi(m)\varphi(n).$$

On a bien démontré que :

$$m \wedge n = 1 \Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$$

On remarque que la réciproque ne tient pas, d'après le tableau de valeurs de la question 1., on a $\varphi(2)\varphi(4) = \varphi(8)$ mais 2 et 4 ne sont pas premiers entre eux.

5. (a) D'après 3.(c), on connaît une expression de $\varphi(p_i^{\alpha_i})$ pour $i \in \llbracket 1, r \rrbracket$, il s'agit de montrer que :

$$\varphi\left(\prod_{i=1}^r p_i^{\alpha_i}\right) = \prod_{i=1}^r \varphi(p_i^{\alpha_i})$$

pour ainsi avoir une formule donnant $\varphi(n)$. Pour ceci on considère l'hypothèse de récurrence pour $r \geq 1$:

$$H_r : \text{Si } (m_i)_{1 \leq i \leq r} \in (\mathbb{N}^*)^r \text{ sont premiers entre eux deux à deux alors } \varphi\left(\prod_{i=1}^r m_i\right) = \prod_{i=1}^r \varphi(m_i).$$

★ Initialisation : la propriété est évidente pour $r = 1$.

★ Hérité : supposons H_r vraie et démontrons H_{r+1} . Pour ceci, considérons une famille d'entiers premiers entre eux deux à deux : $(m_i)_{1 \leq i \leq r+1} \in (\mathbb{N}^*)^{r+1}$. On note $m = \prod_{i=1}^r m_i$, on va démontrer par l'absurde que m et m_{r+1} sont premiers entre eux. Soit p un nombre premier tel que $p|m$ et $p|m_{r+1}$, alors p divise l'un des $(m_i)_{1 \leq i \leq r}$, ceci est absurde car tous les $(m_i)_{1 \leq i \leq r}$ sont premiers avec m_{r+1} . La fonction φ étant multiplicative d'après la question 4., on a $m \wedge m_{r+1} = 1$ qui implique que :

$$\varphi(mm_{r+1}) = \varphi(m)\varphi(m_{r+1}) \Leftrightarrow \varphi\left(\prod_{i=1}^{r+1} m_i\right) = \varphi\left(\prod_{i=1}^r m_i\right)\varphi(m_{r+1}) \Leftrightarrow \varphi\left(\prod_{i=1}^{r+1} m_i\right) = \left(\prod_{i=1}^r \varphi(m_i)\right)\varphi(m_{r+1}).$$

En utilisant l'hypothèse de récurrence pour la dernière équivalence. Ce qui achève la récurrence. Revenons à la question, on applique la propriété H_r avec pour tout $i \in \llbracket 1, r \rrbracket$, $m_i = p_i^{\alpha_i}$ sachant que les entiers de la famille $(p_i^{\alpha_i})_{1 \leq i \leq r}$ sont bien premiers entre eux deux à deux. On obtient :

$$\varphi(n) = \varphi\left(\prod_{i=1}^r p_i^{\alpha_i}\right) = \prod_{i=1}^r \varphi(p_i^{\alpha_i}) = \prod_{i=1}^r (p_i^{\alpha_i} - p_i^{\alpha_i-1}) = \prod_{i=1}^r p_i^{\alpha_i} \left(1 - \frac{1}{p_i}\right) = n \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right).$$

On a bien démontré que :

$$\varphi(n) = n \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right)$$

(b) D'après la proposition précédente, il s'agit dans un premier temps de décomposer les nombres proposés en facteurs premiers :

$$\star 105 = 3 \times 5 \times 7 \text{ d'où } \varphi(105) = \varphi(3)\varphi(5)\varphi(7) = 2 \times 4 \times 6 = 48.$$

$$\star 120 = 2^3 \times 3 \times 5 \text{ d'où } \varphi(120) = \varphi(2^3)\varphi(3)\varphi(5) = 4 \times 2 \times 4 = 32.$$

$$\star 1000 = 2^3 \times 5^3 \text{ d'où } \varphi(1000) = \varphi(2^3)\varphi(5^3) = 4 \times (5^3 - 5^2) = 4 \times 100 = 400.$$

Récapitulons :

$\varphi(105)$	$=$	48
$\varphi(120)$	$=$	32
$\varphi(1000)$	$=$	400

(c) Réutilisons la formule suivante qui a été vue au cours de la démonstration de la question 5.(a) :

$$\varphi(n) = \prod_{i=1}^r (p_i^{\alpha_i} - p_i^{\alpha_i-1}) = \prod_{i=1}^r p_i^{\alpha_i-1} (p_i - 1).$$

Il y a deux cas à distinguer :

★ S'il existe $i \in \llbracket 1, r \rrbracket$ tel que p_i soit impair alors $p_i - 1$ est pair et la formule ci-dessus montre que $\varphi(n)$ est pair.

★ Dans le cas contraire $n = 2^\beta$ où $\beta \geq 2$, ainsi $\varphi(n) = 2^{\beta-1}$ est pair.

On a montré que :

$\forall n \geq 3, \varphi(n) \text{ est pair}$
