Mathématiques - CF Algèbre 1

Corrigé

Exercice 1 : Logique.

1. Est-ce que les deux propositions suivantes sont équivalentes ? Justifier la réponse.

$$(a) \quad P \to (Q \to R) \qquad \text{et} \qquad (b) \quad (P \to Q) \to R.$$

2. Écrire en langage formel l'énoncé suivant :

   Pour tout nombre premier il existe un nombre premier strictement plus grand.

   Ensuite, écrire la négation de cet énoncé.
   Attention : Il faut traduire *premier* en n'utilisant que l'addition et la multiplication.

3. On cherche à calculer la somme $S_n = \sum_{k=1}^{n^2} E(\sqrt{k})$, où $E(x)$ est la partie entière de x.
   (a) Montrer que
   $$S_n = n + \sum_{i=1}^{n-1} \sum_{k=i^2}^{(i+1)^2-1} E(\sqrt{k}).$$
   (b) Conclure.

Solution.

1. On écrit la table de vérité.

P	Q	R	$Q \to R$	$P \to (Q \to R)$	$P \to Q$	$(P \to Q) \to R$
V	V	V	V	V	V	V
V	V	F	F	F	V	F
V	F	V	V	V	F	V
V	F	F	V	V	F	V
F	V	V	V	V	V	V
F	V	F	F	V	V	F
F	F	V	V	V	V	V
F	F	F	V	V	V	F

   La 5me et la 7me colonne étant différentes, les deux propositions ne sont pas équivalentes.

2. On note que p est premier ssi p satisfait $p > 1 \wedge \forall x \forall y\, [xy = p \to (x = 1 \vee y = 1)]$. L'énoncé est donc :
$$\forall p\, [(p > 1 \wedge \forall x \forall y\, [xy = p \to (x = 1 \vee y = 1)]) \to \exists q\, (q > p \wedge \forall x \forall y\, [xy = q \to (x = 1 \vee y = 1)])].$$
   La négation est :
$$\exists p\, [(p > 1 \wedge \forall x \forall y\, [xy = p \to (x = 1 \vee y = 1)]) \wedge \forall q\, (q \leq p \vee \exists x \exists y\, [xy = q \wedge x \neq 1 \wedge y \neq 1])].$$

3. (a) On a $E(\sqrt{n^2}) = n$, et donc
$$S_n = \sum_{k=1}^{n^2} E(\sqrt{k}) = \sum_{k=1^2}^{2^2-1} E(\sqrt{k}) + \sum_{k=2^2}^{3^2-1} E(\sqrt{k}) + \cdots + \sum_{k=(n-1)^2}^{n^2-1} E(\sqrt{k}) + E(\sqrt{n^2}) = n + \sum_{i=1}^{n-1} \sum_{k=i^2}^{(i+1)^2-1} E(\sqrt{k}).$$
   (b) Pour $i^2 \leq k \leq (i+1)^2 - 1$ on a $E(\sqrt{k}) = i$. Ainsi
$$\begin{aligned} S_n &= n + \sum_{i=1}^{n-1} \sum_{k=i^2}^{(i+1)^2-1} i = n + \sum_{i=1}^{n-1} [(i+1)^2 - i^2] i = n + \sum_{i=1}^{n-1} (2i+1) i = n + \sum_{i=1}^{n-1} (2i^2 + i) \\ &= n + 2\frac{(n-1)n(2n-1)}{6} + \frac{(n-1)n}{2} = \frac{n}{6}\,[6 + (n-1)(2(2n-1)+3)] \\ &= \frac{n}{6}\,[6 + (n-1)(4n+1)] = \frac{n}{6}\,[4n^2 - 3n + 5]. \end{aligned}$$

Exercice 2 : Relations et Applications.

1. Soient E un ensemble et $f : E \to E$ une application. On suppose que $f \circ f = f$ et que f est injective ou surjective. Montrer que $f = \mathrm{id}_E$.
2. Soient E et F deux ensembles, $f : E \to F$ une application, $A \subseteq E$ et $B \subseteq F$. Montrer que

$$f[A \cap f^{-1}[B]] = f[A] \cap B.$$

3. Soient E un ensemble et $A \subseteq E$. On note f l'application $X \mapsto X \cap A$ de $\mathcal{P}(E)$ dans $\mathcal{P}(E)$.
   (a) Montrer que $X \sim X'$ ssi $f(X) = f(X')$ est une relation d'équivalence.
   (b) Montrer que $\mathcal{P}(A)$ est un ensemble de représentants des classes d'équivalence de $\sim$.

Solution.

1. Si f est injective, il y a une fonction réciproque à gauche f', avec $f' \circ f = \mathrm{id}_E$. Alors

$$f = \mathrm{id}_E \circ f = (f' \circ f) \circ f = f' \circ (f \circ f) = f' \circ f = \mathrm{id}_E.$$

   Si f est surjective, il y a une fonction réciproque à droite f'', avec $f \circ f'' = \mathrm{id}_E$. Alors

$$f = f \circ \mathrm{id}_E = f \circ (f \circ f'') = (f \circ f) \circ f'' = f \circ f'' = \mathrm{id}_E.$$

2. Soit $y \in f[A \cap f^{-1}[B]]$. Donc il y a $a \in A \cap f^{-1}[B]$ avec $f(a) = y$. Puisque $a \in f^{-1}[B]$ on a $y = f(a) \in B$. Donc $y \in f[A] \cap B$.
   Réciproquement, soit $y \in f[A] \cap B$. Donc il y a $a \in A$ avec $f(a) = y \in B$, et donc $a \in f^{-1}[B]$. Ainsi $a \in A \cap f^{-1}[B]$, et $y = f(a) \in f[A \cap f^{-1}[B]]$.
   Donc $f[A \cap f^{-1}[B]] = f[A] \cap B$.
3. (a) On a $f(X) = f(X)$, d'où $X \sim X$ et $\sim$ est réflexive. Si $X \sim X'$, alors $f(X) = f(X')$, d'où $f(X') = f(X)$ et $X' \sim X$: La relation $\sim$ est symétrique. Enfin, si $X \sim X'$ et $X' \sim X''$, on a $f(X) = f(X')$ et $f(X') = f(X'')$, d'où $f(X) = f(X'')$. Ainsi $X \sim X''$ et $\sim$ est transitive. Il sagot bien d'une relation d'équivalence.
   (b) On a $X \cap A = (X \cap A) \cap A$, d'où $X \sim X \cap A \in \mathcal{P}(A)$. De plus, si $Y, Y' \in \mathcal{P}(A)$ avec $Y \sim Y'$, alors $Y = f(Y) = f(Y') = Y'$. Ainsi tout $X \in \mathcal{P}(E)$ est $\sim$-équivalent à un unique $Y \in \mathcal{P}(A)$, à savoir $Y = f(X) = X \cap A$. Donc $\mathcal{P}(A)$ est un système de représentants des classes modulo $\sim$.

Exercice 3 : Les complexes.

1. Soit $a \in \mathbb{C} \setminus \mathbb{U}$. On note f la fonction $z \mapsto \frac{z-a}{\bar{a}z-1}$. Montrer que f est définie sur $\mathbb{U}$, à valeurs dans $\mathbb{U}$, et que $f : \mathbb{U} \to \mathbb{U}$ est bijective. (Rappel : $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$.)
2. Résoudre algébriquement dans $\mathbb{C}$ l'équation $2z^2 + (8 - 5i)z + (4 - 13i) = 0$.

Solution.

1. Si $z \in \mathbb{U}$ on a $|\bar{a}z| = |\bar{a}|\,|z| = |\bar{a}| \neq 1$ puisque $a \notin \mathbb{U}$. Donc $\bar{a}z \neq 1$, et $f(z)$ est bien défini. De plus, $z\bar{z} = 1 = |z|$ et donc

$$\left|\frac{z-a}{\bar{a}z-1}\right| = \frac{|z-a|}{|\bar{a}z-1|\,|\bar{z}|} = \frac{|z-a|}{|\bar{a}-\bar{z}|} = \frac{|z-a|}{|\overline{a-z}|} = \frac{|z-a|}{|a-z|} = 1$$

   et $f(z) \in \mathbb{U}$.
   Si $y = f(z) = \frac{z-a}{\bar{a}z-1}$, on a $y(\bar{a}z-1) = z-a$, soit $z(\bar{a}y-1) = y-a$ et $z = \frac{y-a}{\bar{a}y-1} = f(y)$. Donc f est sa propre fonction réciproque, et donc bijective.
2. On calcule le déterminant

$$\Delta = (8-5i)^2 - 4 \cdot 2 \cdot (4-13i) = 64 - 25 - 80i - 32 + 104i = 7 + 24i.$$

   On pose $\delta = a + ib$ avec $\Delta = \delta^2 = a^2 - b^2 + 2abi$. En prenant la partie réelle et la partie imaginaire, on obtient

$$a^2 - b^2 = 7, \quad 2ab = 24, \quad \text{et} \quad a^2 + b^2 = |\delta|^2 = |\Delta| = \sqrt{7^2 + 24^2} = \sqrt{625} = 25.$$

   Ainsi $2a^2 = 32$ et $a = \pm 4$, ce qui donne $b = \pm 3$ et $\delta = \pm(4+3i)$. Donc

$$z \in \frac{-(8-5i) \pm (4+3i)}{4} = \{-1+2i, -3+\frac{i}{2}\}.$$

Exercice 4 : Arithmétique.

1. Montrer que pour tous $n \in \mathbb{N}^*$ et $a, b \in \mathbb{Z}$, si $a \equiv b \mod n$ alors $a^n \equiv b^n \mod n^2$.
   Indication : $a^n - b^n = (a-b)\left(a^{n-1} + \cdots + b^{n-1}\right)$.
2. Donner toutes les solutions dans $\mathbb{Z}$ du système de congruences
$$x \equiv 1 \mod 597 \quad et \quad x \equiv 2 \mod 322.$$
3. Montrer que si $x^3 + y^3 + z^3$ est divisible par 7, xyz l'est aussi.

Solution.

1. Puisque $a \equiv b \mod n$ on a
$$a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1} \equiv a^{n-1} + \cdots + a^{n-1} = n \cdot a^{n-1} \equiv 0 \mod n.$$
   Ainsi $n \mid a - b$ et $n \mid a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}$, d'où
$$n^2 \mid (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}) = a^n - b^n,$$
   et $a^n \equiv b^n \mod n^2$.
2. On effectue l'algorithme d'Euclide.
$$\begin{aligned} 597 &= 322 \cdot 1 + 275 \\ 322 &= 275 \cdot 1 + 47 \\ 275 &= 47 \cdot 5 + 40 \\ 47 &= 40 \cdot 1 + 7 \\ 40 &= 7 \cdot 5 + 5 \\ 7 &= 5 \cdot 1 + 2 \\ 5 &= 2 \cdot 2 + 1. \end{aligned}$$
   Ainsi $597 \wedge 322 = 1$ et $1 \mid 2 - 1$. Il y a donc des solutions. On remonte.
$$\begin{aligned} 1 &= 5 - 2 \cdot 2 = 5 - (7-5) \cdot 2 = 5 \cdot 3 - 7 \cdot 2 = (40 - 7 \cdot 5) \cdot 3 - 7 \cdot 2 = 40 \cdot 3 - 7 \cdot 17 \\ &= 40 \cdot 3 - (47 - 40) \cdot 17 = 40 \cdot 20 - 47 \cdot 17 = (275 - 47 \cdot 5) \cdot 20 - 47 \cdot 17 = 275 \cdot 20 - 47 \cdot 117 \\ &= 275 \cdot 20 - (322 - 275) \cdot 117 = 275 \cdot 137 - 322 \cdot 117 = (597 - 322) \cdot 137 - 322 \cdot 117 \\ &= 597 \cdot 137 - 322 \cdot 254. \end{aligned}$$
   Si x_0 est une solution, il y a des entiers relatifs y_0, z_0 tel que $1 + 597y_0 = x = 2 + 322z_0$. Ceci donne l'équation diophantienne
$$597y_0 - 322z_0 = 2 - 1 = 1$$
   ce qui donne une solution particulière $(y_0, z_0) = (137, 254)$, et $x_0 = 1 + 597y_0 = 81790$. Si (x, y) est une autre solution, $597(y - y_0) = 322(z - z_0)$. Puisque $597 \wedge 322 = 1$, on a $322 \mid y - y_0$ et $y = y_0 + 322k$ pour $k \in \mathbb{Z}$, ce qui donne $x = 1 + 597\,(137 + 322k) = 81790 + 597 \cdot 322k$, pour $k \in \mathbb{Z}$. Puisque $81790 + 597 \cdot 322k \equiv 81790$ modulo 597 et modulo 322, ce sont toutes les solutions.
3. On calcule les cubes modulo 7 :
$$0^3 = 0, \quad (\pm 1)^3 = \pm 1, \quad (\pm 2)^3 = \pm 8 \equiv \pm 1 \mod 7, \quad (\pm 3)^3 = \pm 27 \equiv \mp 1 \mod 7.$$
   Si aucun de x, y, z est divisible par 7, alors $x^3 + y^3 + z^3 \equiv \pm 1 \pm 1 \pm 1 \in \{\pm 1, \pm 3\} \mod 7$, et $x^3 + y^3 + z^3$ ne serait pas divisible par 7. Donc au moins un de x, y, z est divisible par 7, et xyz l'est aussi.

Exercice 5 : Polynômes.

1. Résoudre l'équation polynômiale $(X^2 + 1)P'' = P$, pour $P \in \mathbb{C}[X]$.
   Indication : Poser $P(X) = \sum_{k=0}^{d} a_k X^k$, et obtenir des conditions sur les a_k.
2. Soient $P \in \mathbb{R}[X]$ de degré $d > 0$ et $a \in \mathbb{R}$. On suppose $P(a) > 0$ et $P^{(k)}(a) \geq 0$ pour tout $k \in [\![1, d]\!]$. Montrer que P n'a pas de racine dans $[a, \infty[$.

Solution.

1. On pose $P(X) = \sum_{k=0}^d a_k X^k$, où $d = \deg(P)$. Alors $P''(X) = \sum_{k=2}^d a_k k(k-1)X^{k-2}$, et on a

$$\sum_{k=0}^{d} a_k X^k = P(X) = (X^2+1)P''(X) = (X^2+1)\sum_{k=2}^{d} a_k k(k-1)X^{k-2}$$
$$= \sum_{k=2}^{d} a_k k(k-1)X^k + \sum_{k=0}^{d-2} a_{k+2}(k+2)(k+1)X^k.$$

   En comparant les coefficients de X^k, on obtient $a_k = a_k k(k-1) + a_{k+2}(k+2)(k+1)$ pour tout k (où $a_k = 0$ pour $k > d$). Notamment on a $a_d = a_d d(d-1)$. Si $d = 0$ ou $d = 1$ on a $a_d = 0$; si $d > 1$ on a $d(d-1)$ est un entier > 1, ce qui implique $a_d = 0$. Dans tous les cas $P = 0$, ce qui est la seule solution.

2. D'après la formule de Taylor on a pour $x \geq a$ que

$$P(x) = \sum_{k=0}^{d} \frac{P^{(k)}(a)}{k!}(x-a)^k = P(a) + \sum_{k=1}^{d} \frac{P^{(k)}(a)}{k!}(x-a)^k \geq P(a) > 0.$$