Mathématiques - CT Algèbre
Corrigé

Exercice 1 : Logique

1. Montrer que les deux propositions suivantes sont équivalentes :
$$(P \Leftrightarrow Q) \Rightarrow (P \Leftrightarrow R) \quad \text{et} \quad (P \wedge (Q \Rightarrow R)) \vee (\neg P \wedge (R \Rightarrow Q)).$$
2. Soit $f : I \to \mathbb{R}$ une fonction réelle. Exprimer en langage formel que f est lipschitzienne. Donner la négation de cet énoncé.
3. Pour deux ensembles X et Y on pose $X \triangle Y = (X \cup Y) \setminus (X \cap Y)$. Montrer que pour deux ensembles A et B on a
$$(A \triangle B) \triangle B = A.$$

Solution.

1. Par table de vérité : Soit $X = (P \Leftrightarrow Q) \Rightarrow (P \Leftrightarrow R)$, $Y = P \wedge (Q \Rightarrow R)$ et $Z = \neg P \wedge (R \Rightarrow Q)$.

P	Q	R	$P \Leftrightarrow Q$	$P \Leftrightarrow R$	X	$Q \Rightarrow R$	Y	$R \Rightarrow Q$	$\neg P$	Z	$Y \vee Z$
V	V	V	V	V	V	V	V	V	F	F	V
F	V	V	F	F	V	V	F	V	V	V	V
V	F	V	F	V	V	V	V	F	F	F	V
F	F	V	V	F	F	V	F	F	V	F	F
V	V	F	V	F	F	F	F	V	F	F	F
F	V	F	F	V	V	F	F	V	V	V	V
V	F	F	F	F	V	V	V	V	F	F	V
F	F	F	V	V	V	V	F	V	V	V	V

Les colonnes X et $Y \vee Z$ étant identiques, les deux énoncés sont équivalents.

2. $\exists\, \lambda \in \mathbb{R}\, \forall x \in I\, \forall y \in I\, |f(x) - f(y)| \leq \lambda\, |x - y|$.
Négation : $\forall\, \lambda \in \mathbb{R}\, \exists x \in I\, \exists y \in I\, |f(x) - f(y)| > \lambda\, |x - y|$.
3. Soit $x \in A$.
1er cas : $x \in B$. Alors $x \in A \cup B$ et $x \in A \cap B$, d'où $x \notin A \triangle B$. Donc $x \in (A \triangle B) \cup B$ but $x \notin (A \triangle B) \cap B$. Ainsi $x \in (A \triangle B) \triangle B$.
2me cas : $x \notin B$. Alors $x \in A \cup B$ et $x \notin A \cap B$, d'où $x \in A \triangle B$. Donc $x \in (A \triangle B) \cup B$ but $x \notin (A \triangle B) \cap B$. Ainsi $x \in (A \triangle B) \triangle B$.
Ainsi $A \subseteq (A \triangle B) \triangle B$.
Réciproquement, soit $x \notin A$.
1er cas : $x \in B$. Alors $x \in A \cup B$ et $x \notin A \cap B$, d'où $x \in A \triangle B$. Donc $x \in (A \triangle B) \cup B$ et $x \in (A \triangle B) \cap B$. Ainsi $x \notin (A \triangle B) \triangle B$.
2me cas : $x \notin B$. Alors $x \notin A \cup B$. Puisque $X \triangle Y \subseteq X \cup Y$, on a $(A \triangle B) \cup B \subseteq A \cup B$ et $x \notin (A \triangle B) \triangle B$.
Ainsi $(A \triangle B) \triangle B \subseteq A$, et on a égalité.

Exercice 2 : Les complexes

1. Réssoudre dans $\mathbb{C}$:
$$z^2 - (12 + i)z + 37 + 9i = 0.$$
2. Soit $f : \mathbb{C}^* \to \mathbb{C}^*$ l'application complexe $z \mapsto 1/\bar{z}$, et L la droite $\{z \in \mathbb{C} : \operatorname{im} z = 1\}$. Identifier $f^{-1}[L]$.

Solution.

1. On calcule le discriminant :

$$\Delta = (12+i)^2 - 4(37+9i) = 144 - 1 + 24i - 148 - 36i = -5 - 12i.$$

On pose $\Delta = \delta^2 = (a+ib)^2 = a^2 - b^2 - i2ab$. De plus, $|\Delta| = |\delta|^2 = a^2 + b^2$. Ceci donne

$$a^2 - b^2 = -5, \qquad 2ab = -12, \qquad a^2 + b^2 = \sqrt{5^2 + 12^2} = \sqrt{169} = 13.$$

Donc $2a^2 = 8$ et $a = \pm 2$, et $2b^2 = 18$ et $b = \pm 3$. Puisque $2ab = -12 < 0$, on a $\delta = \pm(2-3i)$. Ainsi

$$z = \frac{12 + i \pm (2-3i)}{2} \in \{7 - i, 5 + 2i\}.$$

2. Pour $z = x + iy \in f^{-1}[L]$ on a

$$f(x+iy) = \frac{1}{x - iy} = \frac{x+iy}{x^2+y^2} \in L.$$

Donc $\operatorname{im} f(x+iy) = \frac{y}{x^2+y^2} = 1$, et $y = x^2 + y^2$. Ainsi $x^2 + (y - \frac{1}{2})^2 = (\frac{1}{2})^2$, et $f^{-1}[L]$ est le cercle de centre d'affice $i/2$ et de rayon $1/2$, moins l'origine (puisque f n'est pas défini en 0).

Exercice 3 : Arithmétique

1. Résoudre dans $\mathbb{Z}$ l'équation diophantienne $1665x + 1035y = 45$.
2. (a) Montrer par récurrence que pour tout $n \in \mathbb{N}$ et entier $k \geq 1$ on a :

$$2^{2^{n+k}} - 1 = \left(2^{2^n} - 1\right) \prod_{i=0}^{k-1} \left(2^{2^{n+i}} + 1\right).$$

   (b) On pose $F_n = 2^{2^n} + 1$. Montrer que F_n et F_m sont premiers entre eux pour $m \neq n$.

   (c) En déduire qu'il y a une infinité de nombres premiers.

Solution.

1. On divise l'équation par 5, ce qui donne $333x + 207y = 9$. On note que tout est divisible par 9, et la division donne $37x + 23y = 1$. On calcule donc les coefficients de Bézout.

$$\begin{aligned} 37 &= 23 \cdot 1 + 14 \\ 23 &= 14 \cdot 1 + \ \ 9 \\ 14 &= \ \ 9 \cdot 1 + \ \ 5 \\ 9 &= \ \ 5 \cdot 1 + \ \ 4 \\ 5 &= \ \ 4 \cdot 1 + \ \ 1 \\ 4 &= \ \ 1 \cdot 4 + \ \ 0 \end{aligned}$$

Le $\operatorname{pgcd}(37, 23) = 1$, et on remonte le calcul :

$$\begin{aligned} 1 &= 5 - 4 = 5 - (9-5) = 5 \cdot 2 - 9 = (14 - 9) \cdot 2 - 9 = 14 \cdot 2 - 9 \cdot 3 \\ &= 14 \cdot 2 - (23 - 14) \cdot 3 = 14 \cdot 5 - 23 \cdot 3 = (37 - 23) \cdot 5 - 23 \cdot 3 = 37 \cdot 5 - 23 \cdot 8. \end{aligned}$$

On a donc une solution particulière $x_0 = 5$ et $y_0 = -8$. Si (x, y) est une autre solution, on a $37(x - x_0) + 23(y - y_0) = 0$. Puisque $\operatorname{pgcd}(27, 23) = 1$, le lemme de Gauss nous donne que $23 | x - x_0$, et $x = x_0 + 23k = 5 + 23k$ pour $k \in \mathbb{Z}$. Alors $y = y_0 - 37k = -8 - 37k$, et les solutions sont $\{(5 + 23k, -8 - 37k) : k \in \mathbb{Z}\}$.

   (a) On fait une récurrence sur k.
   Initialisation avec $k = 1$. $\left(2^{2^n} - 1\right) \prod_{i=0}^{1-1} \left(2^{2^{n+i}} + 1\right) = \left(2^{2^n} - 1\right)\left(2^{2^n} + 1\right) = \left(2^{2^n}\right)^2 - 1 = 2^{2^{n+1}} - 1$.
   Hypothèse. $2^{2^{n+k}} - 1 = \left(2^{2^n} - 1\right) \prod_{i=0}^{k-1} \left(2^{2^{n+i}} + 1\right)$.
   Hérédité.

$$\begin{aligned} \left(2^{2^n} - 1\right) \prod_{i=0}^{(k+1)-1} \left(2^{2^{n+i}} + 1\right) &= \left(2^{2^n} - 1\right) \prod_{i=0}^{k-1} \left(2^{2^{n+i}} + 1\right)\left(2^{2^{n+k}} + 1\right) \\ &= \left(2^{2^{n+k}} - 1\right)\left(2^{2^{n+k}} + 1\right) = \left(2^{2^{n+k}}\right)^2 - 1 = 2^{2^{n+k+1}} - 1. \end{aligned}$$

   L'énoncé est donc vrai.

(b) On peut supposer $m = n + k$ avec $k > 0$. D'après (a) on a que $F_n | F_m - 2$, et il y a $k \in \mathbb{Z}$ avec $kF_n + 2 = F_m$. Donc $\text{pgcd}(F_m, F_n) = \text{pgcd}(F_n, 2) = 1$, puisque F_n est impair. Ainsi F_n et F_m sont premiers entre eux pour $m \neq n$.

(c) POur toput $n \in \mathbb{N}$ on a $F_n > 1$, et F_n a un diviseur premier p_n. Pour $m \neq n$ on a $p_m \neq p_n$ puisque $\text{pgcd}(F_m, F_n) = 1$. $\{p_n : n \in \mathbb{N}\}$ est donc une infinité de nombres premiers.

Exercice 4 : Polynômes

1. Soit $P \in \mathbb{R}[X]$ un polynôme.
   (a) Définir une racine d'ordre n de P.
   (b) Définir le polynôme dérivé de P.
2. On cherche à montrer la formule de Taylor pour les polynômes, c'est-à-dire pour $a \in \mathbb{R}$ et $n \geq \deg(P)$ on a
$$P(X) = \sum_{k=0}^{n} \frac{(X-a)^k}{k!} P^{(k)}(a).$$
   (a) Montrer que la formule est vrai si $P(X) = X^d$.
   (b) Montrer que si la formule est vrai pour P et Q, alors elle est vraie pour $bP + cQ$, où $b, c \in \mathbb{R}$.
   (c) Conclure.
3. En déduire que a est une racine d'ordre ℓ si et seulement si $P(a) = P'(a) = \cdots = P^{(\ell-1)}(a) = 0$ et $P^{(\ell)}(a) \neq 0$.

Solution.

1. (a) Un réel $r \in \mathbb{R}$ est une racine d'ordre n de P si $(X-r)^n | P$ mais $(X-r)^{n+1} \nmid P$.
   (b) Si $P(X) = \sum_{k=0}^{d} a_k X^k$, alors le polynôme dérivé est $P'(X) = \sum_{k=1}^{d} k a_k X^{k-1}$.
2. (a) Si $P(X) = X^d$ on voit par récurrence que $P^{(k)}(X) = \frac{d!}{(k-d)!} X^{k-d}$ pour $k \leq d$, et $P^{(k)} = 0$ pour $k > d$. Ainsi
$$\begin{aligned}\sum_{k=0}^{n} \frac{(X-a)^k}{k!} P^{(k)}(a) &= \sum_{k=0}^{d} \frac{(X-a)^k}{k!} \frac{d!}{(k-d)!} a^{k-d} \\ &= \sum_{k=0}^{d} \binom{d}{k} (X-a)^k a^{k-d} = \big((X-a)+a\big)^d = X^d = P(X).\end{aligned}$$
   (b) On a $(bP + cQ)^{(k)} = bP^{(k)} + cQ^{(k)}$. Donc
$$\begin{aligned}\sum_{k=0}^{n} \frac{(X-a)^k}{k!} (bP + cQ)^{(k)}(a) &= \sum_{k=0}^{n} \frac{(X-a)^k}{k!} (bP^{(k)}(a) + cQ^{(k)}(a) \\ &= b\sum_{k=0}^{n} \frac{(X-a)^k}{k!} P^{(k)}(a) + c\sum_{k=0}^{n} \frac{(X-a)^k}{k!} Q^{(k)}(a) \\ &= bP(X) + cQ(X) = (bP + cQ)(X).\end{aligned}$$
   (c) Puisque tout polynôme est une combinaison linéaire de ses monômes, le résultat découle des parties (a) et (b).
3. Supposons que $P(a) = P'(a) = \cdots = P^{(\ell-1)}(a) = 0$ et $P^{(\ell)}(a) \neq 0$. Alors pour $n \geq \deg(P)$ on a
$$P(X) = \sum_{k=0}^{n} \frac{(X-a)^k}{k!} P^{(k)}(a) = \sum_{k=\ell}^{n} \frac{(X-a)^k}{k!} P^{(k)}(a) = (X-a)^\ell Q(X)$$
   avec $Q(X) = \sum_{k=\ell}^{n} \frac{(X-a)^{k-\ell}}{k!} P^{(k)}(a)$. On a $Q(a) = \frac{1}{\ell!} P^{(\ell)}(a) \neq 0$. Donc $X - a \nmid Q$. Ainsi $(X-a)^\ell | P$ mais $(X-a)^{\ell+1} \nmid P$, et a est une racine d'ordre ℓ.
   Réciproquement, si $P \neq 0$ et $d = \deg(P)$, alors $P^{(d)}$ est une constante différente de zéro. Il y a donc $\ell' \geq 0$ minimal avec $P^{(\ell')}(a) \neq 0$. Alors a est une racine d'ordre ℓ' d'après la première partie. Ainsi, si a est une racine d'ordre ℓ, alors $\ell = \ell'$, et $P(a) = P'(a) = \cdots = P^{(\ell-1)}(a) = 0$ mais $P^{(\ell)}(a) \neq 0$.