UNIVERSITÉ DE RENNES 1

Algèbre et arithmétique 1

Corrigé de l'examen (1e session)

Exercice 1 : Voir le corrigé du partiel. (D'autres rédactions sont possibles.)

Exercice 5

1. Théorème (formule du binôme) : Soit $n \geq 0$ un entier, et soient x, y deux nombres réels ou complexes. On a alors :

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}.$$

En particulier, on a $(1+x)^{2n} = \sum_{i=0}^{2n} \binom{2n}{i} x^i$.

Le coefficient devant x^n dans le développement de $(1+x)^{2n}$ est donc $\boxed{\binom{2n}{n}}$.

2. D'après la formule du binôme, on a

$$(1+x)^n = \sum_{i=0}^{n} \binom{n}{i} x^i,$$

donc

$$\begin{aligned}(1+x)^{2n} &= \left(\sum_{i=0}^{n} \binom{n}{i} x^i\right)\left(\sum_{j=0}^{n} \binom{n}{j} x^j\right) \\ &= \sum_{i=0}^{n}\sum_{j=0}^{n} \binom{n}{i}\binom{n}{j} x^{i+j} \quad \text{(en développant)} \\ &= \sum_{k=0}^{2n}\left[\sum_{(i,j)\in I_k} \binom{n}{i}\binom{n}{j}\right] x^k \quad \text{avec } I_k = \{(i,j)\in\{0,\dots,n\}^2 \,/\, i+j=k\} \\ & \qquad (k\in\{0,\dots,2n\}) \\ &= \sum_{k=0}^{2n} A_k x^k \quad \text{avec } A_k = \sum_{(i,j)\in I_k} \binom{n}{i}\binom{n}{j}.\end{aligned}$$

On a en particulier

$$\begin{aligned}A_n &= \sum_{(i,j)\in I_n} \binom{n}{i}\binom{n}{j} \\ &= \sum_{i=0}^{n} \binom{n}{i}\binom{n}{n-i} \quad \text{car } I_n = \{(i, n-i) \,;\, i\in\{0,\dots,n\}\} \\ &= \sum_{i=0}^{n} \binom{n}{i}^2 \quad \text{car } \binom{n}{n-i} = \binom{n}{i}.\end{aligned}$$

On a démontré :

$$\forall x \in \mathbb{R} \qquad (1+x)^{2n} = \sum_{i=0}^{2n} \binom{2n}{i} x^i = \sum_{i=0}^{2n} A_i\, x^i \quad . \quad (*)$$

On voudrait en déduire que : $\forall i \in \{0,\dots,2n\} \qquad \binom{2n}{i} = A_i$,

ce qui permettrait de conclure (en considérant $i=n$). Pour justifier une telle identification des coefficients, on peut par exemple dériver puis évaluer en $x=0$:

Soit $j \in \{0,\dots,n\}$. En dérivant j fois $(*)$, on trouve :

$$\forall x \in \mathbb{R} \qquad \sum_{i=j}^{2n} \binom{2n}{i} i(i-1)(i-2)\cdots(i-j+1)\, x^{i-j} = \sum_{i=j}^{2n} A_i\, i(i-1)\cdots(i-j+1)\, x^{i-j}.$$

En particulier (pour $x=0$), on a : $\binom{2n}{j} j! = A_j\, j!$, donc $A_j = \binom{2n}{j}$.

On a donc démontré (pour $j=n$) que $A_n = \binom{2n}{n}$,

c'est-à-dire $\boxed{\binom{2n}{n} = \sum_{i=0}^{n} \binom{n}{i}^2}$.

3. Soit $m \in \mathbb{Z}$. Comme m est congru modulo 2 au reste de sa division par 2, on a $m \equiv 0 \pmod 2$ ou $m \equiv 1 \pmod 2$.

- Si $m \equiv 0 \pmod 2$, alors $m^2 \equiv 0 \equiv m \pmod 2$.
- Si $m \equiv 1 \pmod 2$, alors $m^2 \equiv 1 \equiv m \pmod 2$.

On a donc : $\boxed{\forall m \in \mathbb{Z} \quad m^2 \equiv m \pmod 2}$.

4. On a

$$\begin{aligned}
\binom{2n}{n} &= \sum_{k=0}^{n} \binom{n}{k}^2 && \text{d'après la question 2} \\
&\equiv \sum_{k=0}^{n} \binom{n}{k}^2 && \pmod 2 \\
&\equiv \sum_{k=0}^{n} \binom{n}{k} && \pmod 2 \quad \text{d'après la question 3} \\
&\equiv (1+1)^n && \pmod 2 \quad \text{d'après la formule du binôme (question 1)} \\
&\equiv 2^n && \pmod 2 \\
&\equiv 0 && \pmod 2 \quad \text{car } n \geq 1
\end{aligned}$$

donc $\boxed{\binom{2n}{n} \text{ est pair .}}$

5 – On considère l'application $\Phi : \begin{cases} A \longrightarrow B \\ F \longmapsto X \setminus F \end{cases}$ et l'application $\Psi : \begin{cases} B \longrightarrow A \\ F \longmapsto X \setminus F \end{cases}$.

Ces deux applications sont bien définies. En effet, si $F \in A$, on a $x \in F$ donc $x \notin X \setminus F$, et
$$|X \setminus F| = |X| - |F| \quad (\text{car } F \subseteq X)$$
$$= 2n - n$$
$$= n,$$
donc $X \setminus F \in B$.

De même, si $F \in B$, on a $x \notin F$ et $x \in X$ donc $x \in X \setminus F$, et $|X \setminus F| = |X| - |F| = 2n - n = n$, donc $X \setminus F \in A$.

Montrons que $\Phi \circ \Psi = id_B$ et $\Psi \circ \Phi = id_A$:

Soit $F \in B$. On a $(\Phi \circ \Psi)(F) = \Phi(\Psi(F)) = \Phi(X \setminus F) = X \setminus (X \setminus F) = F$.

Soit $F \in A$. On a $(\Psi \circ \Phi)(F) = \Psi(X \setminus F) = X \setminus (X \setminus F) = F$.

Donc Φ et Ψ sont des bijections, et elles sont réciproques l'une de l'autre.

On a donc $|A| = |B|$ (puisque $\Phi : A \longrightarrow B$ est une bijection),

et $A \cap B = \emptyset$ (car si $F \in A \cap B$, alors on aurait $x \in F$ et $x \notin F$, ce qui est impossible)

et $A \cup B$ est l'ensemble des parties de X à n éléments, donc $|A \cup B| = \binom{2n}{n}$ (puisque $|X| = 2n$).

On a $|A \cup B| = |A| + |B|$ car $A \cap B = \emptyset$
$= 2|A|$ car $|A| = |B|$,

donc $\boxed{\binom{2n}{n} = |A \cup B| \text{ est pair}}$.

Exercice 2 :

1. On écrit : $12345 = 12350 + (-5)$

$$= 13 \times 950 - 5$$

$$= 13 \times 949 + 8$$

On a $0 \leq 8 < 13$. 8 est donc le reste cherché.

2. On a : $8 \equiv -5 \mod 13$, donc

$$8^2 \equiv \underbrace{-5 \times 8}_{=-40} \mod 13$$

$$\equiv -1 \mod 13$$

D'où : $8^4 \equiv 1 \mod 13$

3. Par la question 1., il vient :

$$12345 \equiv 8 \mod 13$$

Ainsi, on a : $12345^{12345} \equiv 8^{12345} \mod 13$.

Cherchons le reste de la division euclidienne de 12345 par 4.

On écrit $12340 + 5 = 12345$ et on remarque que $12340 = 12300 + 40$ est divisible par 4 ; donc $12345 \equiv 1 \mod 4$.

1 est le reste de la division de 12345 par 4.

On a donc l'existence de $q \in \mathbb{N}$: $12345 = 4q + 1$.

On en tire : $12345^{12345} \equiv 8^{4q+1} \mod 13 \equiv (8^4)^q \cdot 8 \mod 13 \equiv 8 \mod 13$

Le reste cherché est donc 8.

Exercice 4 :

1. Par définition, $(x,y) \in f^{-1}(\{0\})$ ssi $15x - 8y = 0$
Il s'agit donc de trouver les couples $(x,y) \in \mathbb{Z}^2$ t.q
$15x - 8y = 0$.
Soit $(x,y) \in \mathbb{Z}^2$ t.q $15x - 8y = 0$.
On a : $8 \mid 8y$ et donc $8 \mid 15x$. Or,
$PGCD(15,8) = 1$, car $2 \times 8 - 15 = 1$. Par le
théorème de Gauss, on en déduit que : $8 \mid x$.
Il existe $q \in \mathbb{Z}$ t.q $x = 8q$. Revenant
à l'équation, on en déduit que $15 \times 8q - 8y = 0$
et donc $y = 15q$. Toute solution est donc
de la forme $(x,y) = (8q, 15q)$ avec $q \in \mathbb{Z}$.
Réciproquement, on remarque que ces couples sont
solutions.
Conclusion : $f^{-1}(\{0\}) = \{(8q, 15q),\ q \in \mathbb{Z}\}$.

2. f n'est pas injective. En effet, on a :
$f(0,0) = f(8,15) = 0$ et $(0,0) \neq (8,15)$;
autrement dit 0 admet au moins deux antécédents
par f.

3. Nous avons observé dans la question 1. que :
$$15 \times (-1) - 8 \times (-2) = 1.$$
On pose $(x_0, y_0) = (-1, -2)$. On a : $f(x_0, y_0) = 1$.

4. Montrons que f est surjective.

Soit $n \in \mathbb{Z}$. On a : $f(-1, -2) = 1$ et donc

$$n \times f(-1, -2) = n$$ si bien que :

$$f(-n, -2n) = n.$$

Le couple $(-n, -2n) \in \mathbb{Z}^2$ est un antécédent de n par f.

Tout élément de $\mathbb{Z}$ possède donc au moins un antécédent par f.

Exercice 3

1. Démontrons que $P(n)$ est vraie pour tout $n \in \mathbb{N}$.

Soit $n \in \mathbb{N}$, un entier naturel. Si l'on pose $x \overset{\text{def}}{=} n$, on voit que :

$$n = x \leq y \Rightarrow n \leq y.$$

2

Ceci montre qu'il existe $x \in \mathbb{N}$ (on vient de voir que $x = n$ convient) tel que : $\forall y \in \mathbb{N}$, $(x \leq y \Rightarrow n \leq y)$.

Ainsi $P(n)$ est vraie.

2. Montrons que $Q(0)$ est vraie, et $Q(n)$ fausse si $n \geq 1$

1

D'abord on observe que si $x \in \mathbb{N}$ et $y \in \mathbb{N}$, alors, que l'on ait $x \leq y$ ou non, dans tous les cas il est vrai que $0 \leq y$. Ceci signifie que $Q(0)$ est vraie.

2

Supposons maintenant que n est un entier tel que $n \geq 1$.

1

Posons $x = y = 0$. Alors, $x = 0 \leq y = 0$ mais $n \geq 1 > 0 = y$.

Ceci démontre que :

$$\exists x \in \mathbb{N},\ \exists y \in \mathbb{N},\ x \leq y \text{ et } n > y$$

(on a vu que $x = y = 0$ convient). C'est la négation de $Q(n)$, donc $Q(n)$ est fausse.

Exercice 6

1. Montrons que f est injective si $h \circ f$ l'est.

Soient x, x' dans E tels que $f(x) = f(x')$. Alors $h(f(x)) = h(f(x'))$ c'est-à-dire $(h \circ f)(x) = (h \circ f)(x')$.

Comme $h \circ f$ est supposée injective, on déduit que $x = x'$.

Donc f est injective.

Montrons que h est surjective si $h \circ f$ l'est.
Soit $z \in G$. Comme $h \circ f$ est supposée surjective,
il existe $x \in E$ tel que $(h \circ f)(x) = z$. Posons $y \overset{\text{def}}{=} f(x)$.
1 On calcule : $h(y) = h(f(x)) = (h \circ f)(x) = z$, de sorte
que y est un antécédent pour z par l'application h.
Donc h est surjective.

2. Supposons f injective. Alors, pour $y \in F$ donné, se présentent deux situations :

* si $y \in f(E)$, il existe $x \in E$ tel que $y = f(x)$, et de plus cet élément x est unique par l'hypothèse que f est injective.
* $y \notin f(E)$.

Comme E est supposé non vide, on peut choisir $a \in E$.
Construisons alors une application $g : F \to E$ de la
1 manière suivante : on pose, pour $y \in F$:

$$g(y) = \begin{cases} \text{l'unique } x \text{ tel que } y = f(x) \text{ (voir ci-dessus),} \\ \qquad \text{si } y \in f(E) \\ a, \quad \text{si } y \notin f(E). \end{cases}$$

Pour tout $x \in E$, par définition même de g on a

$$(g \circ f)(x) = g(f(x)) = x$$

puisque $x \in E$ est l'(unique) élément de E tel que $f(x) = f(x)$.
On a construit $g : F \to E$ telle que $g \circ f = \mathrm{id}_E$.

Réciproquement supposons qu'il existe $g : F \to E$ telle que $g \circ f = id_E$. Montrons que f est injective : pour x, x' deux éléments de E tels que $f(x) = f(x')$, on a

$$x = (g \circ f)(x) = g(f(x)) = g(f(x')) = (g \circ f)(x') = x',$$

ce qui conclut à l'injectivité.

3. Supposons f surjective. Construisons $g : F \to E$ de la manière suivante : pour tout $y \in F$, on choisit $x \in E$ tel que $y = f(x)$ (il existe un tel x car f est surjective) et on pose $g(y) = x$.

Par construction de g, on a, pour tout $y \in F$:

$(f \circ g)(y) = f(g(y)) = f(x)$ où x a été choisi tel que $y = f(x)$, ci-dessus,

1

$= y$ par ce choix de x.

Ceci démontre que $f \circ g = id_F$.

Réciproquement supposons qu'il existe $g : F \to E$ telle que $f \circ g = id_F$. Montrons que f est surjective : pour tout $y \in F$, du fait que $y = (f \circ g)(y) = f(g(y))$, on voit que $g(y)$ est un antécédent pour y par f, ce qui conclut à la surjectivité.

4. Supposons qu'il existe une application injective $f : E \to F$. Alors d'après 2. il existe $g : F \to E$ telle que $g \circ f = id_E$. D'après 3. appliquée en échangeant les rôles de f et g, on voit que g est surjective : donc il existe une application surjective de F dans E.

1

Réciproquement supposons qu'il existe une application surjective de F dans E, notée $g : F \to E$.
D'après 3. appliquée en échangeant les rôles de f et g, il existe $f : E \to F$ telle que $g \circ f = id_E$. D'après 2. l'application f est injective, donc il existe une application injective de E dans F.