Corrigé de l'examen d'AR1 2e session
juin 2017

Exercice 1

1.a.

On a : $f(0,8) = 8b = 8\times 6 = 48$

$f(6,-7) = 6a - 7b = 6\times 15 - 7\times 6 = 90 - 42 = 48$.

1.b.

Comme $f(0,8) = f(6,-7)$, et $(0,8) \neq (6,-7)$, l'application f n'est pas injective.

1.c.

Quel que soit $(m,n)\in\mathbb{Z}^2$, on a $f(m,n) = am + bn = 15m + 6n = 3(5m+2n)$, donc $3 \mid f(m,n)$.
En particulier, comme $3 \nmid 1$, il n'existe pas de $(m,n)\in\mathbb{Z}^2$ tel que $f(m,n) = 1$,
donc l'application f n'est pas surjective.

2.

Soit $(m,n)\in\mathbb{Z}^2$. On a : $f(m,n)\in\{0\} \iff f(m,n) = 0$

$\iff am + bn = 0$

$\iff am = -bn$.

- Si a et b sont premiers entre eux (i.e. $\operatorname{pgcd}(a,b) = 1$), alors :
  - si $am = -bn$, alors $b \mid am$,
    or $\operatorname{pgcd}(a,b) = 1$, donc $b \mid m$ d'après le lemme de Gauß,
    donc $\exists k\in\mathbb{Z}$ $m = kb$,
    or $am = -bn$, donc $-bn = kab$, donc $(ka+n)b = 0$,
    or $b > 0$ donc en particulier on a $b \neq 0$, donc $ka + n = 0$,
    donc $n = -ka$,
    donc $(m,n) = (kb, -ka)$;
  - réciproquement, si $\exists k\in\mathbb{Z}$ $(m,n) = (kb,-ka)$,
    alors $am = akb = -bn$;

  donc $(m,n)\in f^{-1}(\{0\}) \iff \exists k\in\mathbb{Z}$ $(m,n) = (kb,-ka)$.
- Dans le cas général (i.e. <u>on ne suppose plus</u> que $\operatorname{pgcd}(a,b) = 1$) :
  notons $a' = \frac{a}{d}$ et $b' = \frac{b}{d}$ (avec $d = \operatorname{pgcd}(a,b)$),
  alors $am = -bn \iff (a'm + b'n)d = 0$

  $\iff a'm + b'n = 0$ car $d > 0$,

  et $\operatorname{pgcd}(a',b') = 1$ (car $d\operatorname{pgcd}(a',b')$ est un diviseur de a et de b, donc de d),
  donc on peut appliquer le raisonnement du point précédent (avec a' et b' au lieu de a et b), et on obtient :

  $a'm + b'n = 0 \iff \exists k\in\mathbb{Z}$ $(m,n) = (kb', -ka')$,

  donc $f^{-1}(\{0\}) = \left\{ \left(k\frac{b}{d}, -k\frac{a}{d}\right) ; k\in\mathbb{Z} \right\}$.

Notons que $(0,0) \in f^{-1}(\{0\})$ (avec $k=0$)

et $(b,-a) \in f^{-1}(\{0\})$ (avec $k=d$),

or $(0,0) \neq (b,-a)$, donc f n'est pas injective.

3_a.

D'après la formule de Bézout, $\exists (u,v) \in \mathbb{Z}^2 \quad au+bv=d$,

i.e. $f(u,v)=d$, donc d a un antécédent par f.

Si $d|p$, alors $\left(\frac{p}{d}u, \frac{p}{d}v\right) \in \mathbb{Z}^2$ (car $\frac{p}{d} \in \mathbb{Z}$ et $(u,v) \in \mathbb{Z}^2$),

et $f\left(\frac{p}{d}u, \frac{p}{d}v\right) = a\frac{p}{d}u + b\frac{p}{d}v = \frac{p}{d}(au+bv) = \frac{p}{d}d = p$,

donc p a un antécédent par f.

3_b.

Soit $(m,n) \in \mathbb{Z}^2$, alors $f(m,n) = am+bn$,

or $d = \text{pgcd}(a,b)$ donc $d|a$ et $d|b$, donc $d|(am+bn)$,

donc $d \mid f(m,n)$.

Si $d \nmid p$, on ne peut donc pas avoir $p=f(m,n)$, donc p n'a pas d'antécédent par f.

4_

Si f est surjective, alors $p=1$ a un antécédent par f,

donc $d|1$ d'après 3_b., donc $d=1$ puisque d est un entier naturel.

Réciproquement, si $d=1$, alors d divise tous les entiers relatifs,

donc f est surjective d'après 3_a.

Donc l'application f est surjective si et seulement si a et b sont premiers entre eux.

Exercice 2

1.

On a $\binom{p}{m} = \dfrac{p!}{m!\,(p-m)!}$,

or $p! = p\,(p-1)!$ donc $p \mid p!$,

et $m! = \prod_{i=1}^{m} i$, or $p > m$, donc $\forall i \in \{1, \dots, m\}$ $p \nmid i$,

et p est premier, donc $p \nmid m!$ (puisqu'un nombre premier divise un produit si et seulement s'il divise un des facteurs, d'après le lemme d'Euclide),

et de même $p \nmid (p-m)!$ puisque $p > p-m$,

donc $p \nmid (m!\,(p-m)!)$, donc $p \mid \binom{p}{m}$, d'après le lemme d'Euclide.

2.

D'après la formule du binôme, on a

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

or $\binom{p}{i} \equiv 0 \pmod p$ pour tout $i \in \{1, 2, \dots, p-1\}$, d'après la question 1.,

donc $(x+y)^p \equiv x^p + y^p \pmod p$.

3.

Si $y \equiv 0 \pmod{p^n}$, on a

$$(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^{p-i} y^i \quad \text{d'après la formule du binôme,}$$

et pour tout $i \in \{1, \dots, p\}$:

- si $i < p$, on a $p \mid \binom{p}{i}$, $p^n \mid y$, donc $p^{n+1} \mid \binom{p}{i} y^i$ (puisque $i \geq 1$) ;
- si $i = p$, on a $p^n \mid y$ donc $p^{2n} \mid y^i$ (puisque $i = p \geq 2$), donc $p^{n+1} \mid y^i$ (puisque $n \geq 1$),

donc $\binom{p}{i} x^{p-i} y^i \equiv 0 \pmod{p^{n+1}}$ pour tout $i \in \{1, \dots, p\}$,

donc $(x+y)^p \equiv x^p \pmod{p^{n+1}}$.

4-

Si $n\in\mathbb{N}$, notons $\mathcal{P}(n)$ la propriété : $x^{p^n}\equiv y^{p^n} \pmod{p^{n+1}}$.

- Comme $x\equiv y \pmod p$, la propriété $\mathcal{P}(0)$ est vraie.
- Soit $n\in\mathbb{N}$ tel que $\mathcal{P}(n)$ soit vraie,

  alors $x^{p^n}\equiv y^{p^n} \pmod{p^{n+1}}$, donc $y^{p^n}-x^{p^n}\equiv 0 \pmod{p^{n+1}}$,

  donc $(x^{p^n}+y^{p^n}-x^{p^n})^p\equiv x^{p^{n+1}} \pmod{p^{n+2}}$ d'après la question 3-,

  donc $x^{p^{n+1}}\equiv y^{p^{n+1}} \pmod{p^{n+2}}$, donc $\mathcal{P}(n+1)$ est vraie.

Par récurrence, on a donc : $\forall n\in\mathbb{N}\quad x^{p^n}\equiv y^{p^n} \pmod{p^{n+1}}$.

Exercice 3

1.

Si E et F sont deux ensembles finis, de cardinaux $p = |E|$ et $n = |F|$, alors le cardinal de l'ensemble F^E des applications de E dans F est n^p (avec $0^0 = 1$).

Montrons-le par récurrence sur p. Notons $\mathcal{P}(p)$, pour $p \geq 0$ entier, la propriété : « pour tout ensemble E de cardinal p, et pour tout ensemble fini F, le cardinal de F^E est $|F|^p$.

- Montrons que $\mathcal{P}(0)$ est vraie.

  Soit E un ensemble de cardinal 0, et soit F un ensemble fini.
  Comme $|E| = 0$, l'ensemble E est vide.
  Rappelons qu'une application de E dans F est, par définition, la donnée des ensembles E et F et du graphe G de l'application, qui est une partie de $E \times F$ vérifiant :
  $$\forall x \in E \quad \exists!\, y \in F \quad (x,y) \in G .$$
  Comme $E = \emptyset$, on a $E \times F = \emptyset$, or $G \subseteq E \times F$ donc $G = \emptyset$. On a donc au plus une application de $E = \emptyset$ dans F.
  Réciproquement, comme $E = \emptyset$, la propriété $\forall x \in E \ \exists!\, y \in F \ (x,y) \in \emptyset$ est vraie, donc $G = \emptyset$ donne bien une application de E dans F.
  Donc $|F^E| = 1 = |F|^0$.

- Soit $p \geq 0$ un entier. Supposons que $\mathcal{P}(p)$ est vraie. Montrons que $\mathcal{P}(p+1)$ est vraie.
  Soit E un ensemble de cardinal $p+1$, et soit F un ensemble fini.
  Notons $n = |F|$ le cardinal de F.
  Comme $p+1 \neq 0$, l'ensemble E n'est pas vide. Soit $x \in E$.
  Comme $\{x\}$ et $E \setminus \{x\}$ forment une partition de E (i.e. on a $E = \{x\} \cup (E \setminus \{x\})$ et $\emptyset = \{x\} \cap (E \setminus \{x\})$), on a $|E \setminus \{x\}| = |E| - |\{x\}| = (p+1) - 1 = p$.
  On veut montrer que $|F^E| = n^{p+1}$, c'est-à-dire $|F^E| = n^p \cdot n$.
  Par hypothèse de récurrence, on a $n^p = |F^{E \setminus \{x\}}|$, donc il suffit de montrer qu'il existe une bijection entre F^E et $F^{E \setminus \{x\}} \times F$.
  Considérons les applications
  $$\Phi : \begin{cases} F^E \longrightarrow F^{E\setminus\{x\}} \times F \\ f \longmapsto (f|_{E\setminus\{x\}}, f(x)) \end{cases} \quad \text{et} \quad \Psi : \begin{cases} F^{E\setminus\{x\}} \times F \longrightarrow F^E \\ (g,y) \longmapsto \begin{cases} E \longrightarrow F \\ z \longmapsto \begin{cases} g(z) & \text{si } z \neq x \\ y & \text{si } z = x \end{cases} \end{cases} \end{cases}$$
  Montrons que $\Psi \circ \Phi = id_{F^E}$ et $\Phi \circ \Psi = id_{F^{E\setminus\{x\}} \times F}$.

Soit $f \in F^E$. On a $\Phi(f) = (f|_{E\setminus\{x\}}, f(x))$,

donc $(\Psi \circ \Phi)(f) = \Psi(f|_{E\setminus\{x\}}, f(x))$

$$= \left\{\begin{array}{l} E \longrightarrow F \\ z \longmapsto \begin{cases} f|_{E\setminus\{x\}}(z) & \text{si } z \neq x \\ f(x) & \text{si } z = x \end{cases}\end{array}\right.$$

$$= \left\{\begin{array}{l} E \longrightarrow F \\ z \longmapsto f(z) \end{array}\right.$$

$$= f.$$

Soit $(g, y) \in F^{E\setminus\{x\}} \times F$.

Notons h l'application $\Psi(g,y)$, i.e. $h : \left\{\begin{array}{l} E \longrightarrow F \\ z \longmapsto \begin{cases} g(z) & \text{si } z \neq x \\ y & \text{si } z = x \end{cases}\end{array}\right.$.

On a $(\Phi \circ \Psi)(g,y) = \Phi(h)$

$$= (h|_{E\setminus\{x\}}, h(x))$$

or $h(x) = y$ par définition de h,

et $h|_{E\setminus\{x\}} = g$ car pour tout $z \in E\setminus\{x\}$ on a $h(z) = g(z)$ (par définition de h),

donc $(\Phi \circ \Psi)(g,y) = (g,y)$.

Donc Φ est une bijection (et Ψ aussi, et $\Psi = \Phi^{-1}$),

donc $|F^E| = |F^{E\setminus\{x\}} \times F|$

$$= |F^{E\setminus\{x\}}| \cdot |F|$$

$$= n^p \cdot n$$

$$= n^{p+1}.$$

Donc $\mathcal{P}(p+1)$ est vraie, ce qui conclut la récurrence.

Bien que ce ne soit pas nécessaire dans la preuve (puisqu'on a commencé la récurrence à $p=0$), voici comment démontrer directement que $\mathcal{P}(1)$ est vraie.

Soit E un ensemble de cardinal 1, i.e. un singleton : $E = \{x\}$.

Soit F un ensemble fini.

On veut montrer que $|F^E| = |F|^1 = |F|$. Il suffit pour cela de construire une bijection entre F^E et F.

Soient $\alpha : \begin{cases} F^E \longrightarrow F \\ f \longmapsto f(x) \end{cases}$ et $\beta : \begin{cases} F \longrightarrow F^E \\ y \longmapsto \begin{cases} E \longrightarrow F \\ z \longmapsto y \end{cases} \end{cases}$.

Si $f \in F^E$, on a $\alpha(f) = f(x)$, donc $(\beta \circ \alpha)(f) = \begin{cases} E \longrightarrow F \\ z \longmapsto f(x) \end{cases}$,

or pour tout $z \in E$ on a $z = x$ (car $E = \{x\}$) donc $f(z) = f(x)$,

donc $f = (\beta \circ \alpha)(f)$.

Si $y \in F$, on a $\beta(y) = \begin{cases} E \longrightarrow F \\ z \longmapsto y \end{cases}$, donc $(\alpha \circ \beta)(y) = (\beta(y))(x) = y$.

Donc $\beta \circ \alpha = id_{F^E}$ et $\alpha \circ \beta = id_F$, donc α et β sont des bijections,

et $|F^E| = |F|$.

2.

Une <u>partition</u> d'un ensemble ~~fini~~ E est une famille $(A_i)_{i \in I}$ de sous-ensembles de E (i.e. I est un ensemble, et, pour tout $i \in I$, A_i est une partie de E), telle que :

- $\bigcup_{i \in I} A_i = E$
- les A_i sont deux à deux disjoints, i.e.
  $\forall (i,j) \in I^2 \quad i \neq j \Longrightarrow A_i \cap A_j = \emptyset$.

3.

On a $|\mathcal{P}(E)| = 2^p$.

Pour le démontrer, il suffit de montrer qu'il existe une bijection entre $\mathcal{P}(E)$ et $\{0,1\}^E$ (l'ensemble des applications de E dans $\{0,1\}$). En effet, d'après la question 1., on a $|\{0,1\}^E| = 2^{|E|}$.

Considérons les application

$$\Gamma : \begin{cases} \mathcal{P}(E) \longrightarrow \{0,1\}^E \\ A \longmapsto \chi_A : \begin{cases} E \longrightarrow \{0,1\} \\ x \longmapsto \begin{cases} 0 \text{ si } x \notin A \\ 1 \text{ si } x \in A \end{cases} \end{cases} \end{cases} \quad \text{et} \quad \Delta : \begin{cases} \{0,1\}^E \longrightarrow \mathcal{P}(E) \\ f \longmapsto f^{-1}(\{1\}) \end{cases}$$

Montrons que $\Delta \circ \Gamma = id_{\mathcal{P}(E)}$ et $\Gamma \circ \Delta = id_{\{0,1\}^E}$.

• Soit $A \in \mathcal{P}(E)$. Alors $\Gamma(A) = \chi_A$, où $\chi_A : \begin{cases} E \longrightarrow \{0,1\} \\ x \longmapsto \begin{cases} 0 \text{ si } x \notin A \\ 1 \text{ si } x \in A \end{cases} \end{cases}$,

donc $(\Delta \circ \Gamma)(A) = \Delta(\chi_A) = \chi_A^{-1}(\{1\})$. Montrons que $\chi_A^{-1}(\{1\}) = A$.

Soit $x \in A$. Alors $\chi_A(x) = 1$ par définition de χ_A, donc $x \in \chi_A^{-1}(\{1\})$.

Soit $x \in \chi_A^{-1}(\{1\})$. Alors $\chi_A(x) = 1$, donc $x \in A$ par définition de χ_A.

On a donc $(\Delta \circ \Gamma)(A) = A$.

• Soit $f \in \{0,1\}^E$. On a $\Delta(f) = f^{-1}(\{1\})$, donc $(\Gamma \circ \Delta)(f) = \chi_{f^{-1}(\{1\})}$,

où $\chi_{f^{-1}(\{1\})} : \begin{cases} E \longrightarrow \{0,1\} \\ x \longmapsto \begin{cases} 0 \text{ si } x \notin f^{-1}(\{1\}) \\ 1 \text{ si } x \in f^{-1}(\{1\}) \end{cases} \end{cases}$. Montrons que $\chi_{f^{-1}(\{1\})} = f$.

Soit $x \in E$.

- Si $x \notin f^{-1}(\{1\})$, alors $\chi_{f^{-1}(\{1\})}(x) = 0$,
  et $f(x) \notin \{1\}$ par définition de $f^{-1}(\{1\})$,
  or $f(x) \in \{0,1\}$ par définition de f, donc $f(x) = 0$.
- Si $x \in f^{-1}(\{1\})$, alors $\chi_{f^{-1}(\{1\})}(x) = 1$,
  et $f(x) \in \{1\}$ donc $f(x) = 1$.

Donc $\chi_{f^{-1}(\{1\})} = f$.

Donc on a montré que Γ et Δ sont des bijections (et $\Gamma^{-1} = \Delta$),

donc $|\mathcal{P}(E)| = |\{0,1\}^E| = 2^p$.

4-

Une méthode possible est de montrer que $\left(f^{-1}(\{y\})\right)_{y \in f(E)}$ est une partition de E.

Commençons par démontrer ce lemme.

- On a $\bigcup_{y \in f(E)} f^{-1}(\{y\}) \subseteq E$ par définition de $f^{-1}(\{y\})$.
- Soit $x \in E$, alors $f(x) \in \{f(x)\}$ donc $x \in f^{-1}(\{f(x)\})$,
  et $f(x) \in f(E)$ donc $f^{-1}(\{f(x)\}) \subseteq \bigcup_{y \in f(E)} f^{-1}(\{y\})$ (en prenant $y = f(x)$).

  Donc $E \subseteq \bigcup_{y \in f(E)} f^{-1}(\{y\})$.

On a donc $E = \bigcup_{y \in f(E)} f^{-1}(\{y\})$.

- Soient $y, y' \in f(E)$, tels que $y \neq y'$. Par l'absurde, si $x \in f^{-1}(\{y\}) \cap f^{-1}(\{y'\})$, on aurait $f(x) \in \{y\}$ et $f(x) \in \{y'\}$ donc $y = f(x) = y'$: contradiction.
  Donc $f^{-1}(\{y\}) \cap f^{-1}(\{y'\}) = \emptyset$.

Donc la famille $\left(f^{-1}(\{y\})\right)_{y \in f(E)}$ est une partition de E.

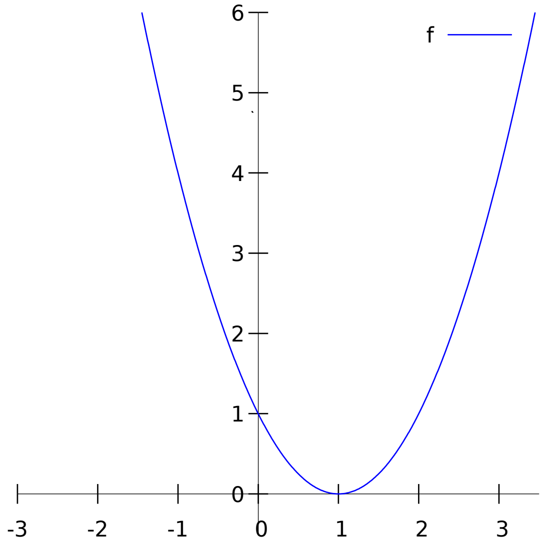
De plus, si $y \in f(E)$, alors $\exists x \in E \quad y = f(x)$, et on a alors $x \in f^{-1}(\{y\})$, donc $f^{-1}(\{y\}) \neq \emptyset$.

On a alors
$$\begin{aligned}
|E| &= \sum_{y \in f(E)} |f^{-1}(\{y\})| && \text{car } \left(f^{-1}(\{y\})\right)_{y \in f(E)} \text{ est une partition de } E \\
&\geq \sum_{y \in f(E)} 1 && \text{car } \forall y \in f(E) \quad |f^{-1}(\{y\})| \geq 1 \\
& && \text{(puisque } f^{-1}(\{y\}) \neq \emptyset \text{)} \\
&\geq |f(E)|.
\end{aligned}$$

On a donc $|f(E)| \leq |E|$.

Exercice 4

1-



2-

Montrons que $f(I) = [0;4]$.

- Soit $x \in I$. On a $f(x) = (x-1)^2 \geq 0$.
  De plus, si $x \geq 1$, on a $0 \leq x-1 \leq 2$ (car $x \leq 3$ puisque $x \in I$),
  donc $f(x) = (x-1)^2 \leq 4$.
  Si $x \leq 1$, on a $-1 \leq x-1 \leq 0$ (car $x \geq 0$ puisque $x \in I$),
  donc $0 \leq 1-x \leq 1$, donc $f(x) = (x-1)^2 = (1-x)^2 \leq 1 \leq 4$.
  On a donc $f(x) \in [0;4]$. On a donc démontré $f(I) \subseteq [0;4]$.
- Soit $y \in [0;4]$. Comme $y \geq 0$, il existe un réel $x' \geq 0$ tel que $x'^2 = y$ (i.e. $x' = \sqrt{y}$)
  (L'existence de la racine carrée d'un réel positif est ici admise. Pour justifier son existence, consultez un cours d'analyse.)
  Si $x' > 2$, on aurait $x'^2 > 4$; or $y \leq 4$, donc $x' \leq 2$.
  Posons $x = x'+1$. On a alors $0 \leq x' \leq 2$ donc $1 \leq x \leq 3$, donc $x \in I$,
  et $f(x) = (x-1)^2 = x'^2 = y$. Donc $y \in f(I)$. On a démontré $[0;4] \subseteq f(I)$.

On a donc $f(I) = [0;4]$.

3-

Montrons que $f^{-1}(I) = [1-\sqrt{3}\,;\, 1+\sqrt{3}]$.

- Soit $x \in [1-\sqrt{3}\,;\, 1+\sqrt{3}]$.
  - Si $x \geq 1$, on a $1 \leq x \leq \sqrt{3}+1$, donc $0 \leq x-1 \leq \sqrt{3}$, donc $0 \leq f(x) \leq 3$.
  - Si $x \leq 1$, on a $1-\sqrt{3} \leq x \leq 1$, donc $-\sqrt{3} \leq x-1 \leq 0$, donc $0 \leq 1-x \leq \sqrt{3}$,
    or $f(x) = (1-x)^2$, donc $0 \leq f(x) \leq 3$.

  Donc $f(x) \in I$.

- Réciproquement, soit $x \in \mathbb{R}$ tel que $f(x) \in I$ (i.e. $x \in f^{-1}(I)$).

  On a $(x-1)^2 \leq 3$.

  - Si $x - 1 > \sqrt{3}$, on aurait $(x-1)^2 > 3$: contradiction.
  - Si $x - 1 < -\sqrt{3}$, alors on aurait $1 - x > \sqrt{3}$ donc $(x-1)^2 = (1-x)^2 > 3$: contradiction.

  On a donc $-\sqrt{3} \leq x - 1 \leq \sqrt{3}$, donc $x \in [1-\sqrt{3}, 1+\sqrt{3}]$

On a donc $f^{-1}(I) = [1-\sqrt{3} ; 1+\sqrt{3}]$.

Exercice 5

Remarquons que cette proposition est équivalente à :

$$\forall x \in \mathbb{R} \quad \exists y \in \mathbb{R} \quad x = y \vee f(x) \neq f(y) .$$

La proposition est vraie. En effet,

soit $x \in \mathbb{R}$, posons $y = x$, alors $x \neq y$ est faux, donc $x \neq y \Rightarrow f(x) \neq f(y)$ est vrai.

Ceci démontre la proposition de l'énoncé.