Corrigé du TD n$^{\text{o}}$ 7

Dénombrement, anneaux et corps

21 décembre 2020

1 Dénombrement

Exercice 1. Soient A et B deux parties de E et F. Soit f une application de E dans F. Déterminer si les propositions suivantes sont vraies ou fausses. Justifier.

1. Si A est une partie finie de E alors $f(A)$ est une partie finie de F.
2. Si $f(A)$ est une partie finie de F alors A est une partie finie de E.
3. Si B est une partie finie de F alors $f^{-1}(B)$ est une partie finie de E.
4. Si $f^{-1}(B)$ est une partie finie de E alors B est une partie finie de F.

---

1. Vrai. Notons n le cardinal de A. On peut alors écrire $A = \{x_1, \dots, x_n\}$. Donc $f(A) = \{f(x_1), \dots, f(x_n)\}$ et $\text{card}(f(A)) \leq n$. Donc $f(A)$ est une partie finie de F.
2. Faux. Il suffit de prendre E une partie infinie, $A = E$ et choisir une fonction constante. Dans ce cas, $f(A)$ est un singleton, de cardinal 1.
   Par exemple, on prend $E = F = \mathbb{N}$ et $f : \mathbb{N} \longrightarrow \mathbb{N}\ ;\ n \longmapsto 0$. Alors $f(E) = \{0\}$ est une partie finie (de cardinal 1) de F mais $\mathbb{N}$ est une partie infinie de $\mathbb{N}$.
3. Faux. Le même contre-exemple qu'à la question précédente convient. On prend $E = F = \mathbb{N}$, $f : \mathbb{N} \longrightarrow \mathbb{N}\ ;\ n \longmapsto 0$ et $B = \{0\} \subset \mathbb{N}$ de cardinal 1. On a $f^{-1}(B) = \mathbb{N}$ qui est une partie infinie de $\mathbb{N}$.
4. Faux. On prend $E = F = \mathbb{N}$, $f : \mathbb{N} \longrightarrow \mathbb{N}\ ;\ x \longmapsto \begin{cases} 1 \text{ si } n = 1 \\ 0 \text{ sinon} \end{cases}$ et $B = \mathbb{N}^*$. Alors $f^{-1}(B) = \{1\}$ est fini (de cardinal 1) et B est une partie infinie de $\mathbb{N}$.
   On pouvait aussi prendre pour f la fonction $n \longmapsto 0$ et $f^{-1}(\mathbb{N}^*) = \emptyset$ qui est une partie finie, de cardinal 0.

Exercice 2.

1. Combien y a-t-il d'anagrammes du mot « ABRACADABRA » ?
2. Soit $(p, q) \in \mathbb{N}^2$. On part du point de coordonnées $(0, 0)$ pour rejoindre le point de coordonnées (p, q) en se déplaçant à chaque étape d'une unité vers la droite ou vers le haut. Combien y a-t-il de chemins possibles ?

---

1. Déterminons le nombre d'anagrammes du mot "ABRACADABRA". Il est constitué de 11 lettres, dont 5 lettres distinctes, A apparaissant 5 fois, B apparaissant 2 fois, R apparaissant 2 fois, C apparaissant 1 fois et D apparaissant 1 fois.
   -1$^{\text{ère}}$ méthode : On choisit la position des lettres A. Il y a $\binom{11}{5}$ positions possibles.
   On choisit ensuite la position des lettres B parmi les $11 - 5 = 6$ positions restantes. Il y a alors $\binom{6}{2}$ positions possibles.
   On choisit ensuite la position des lettres R parmi les $11 - 5 - 2 = 4$ positions restantes. Il y a alors $\binom{4}{2}$ positions possibles.
   On choisit ensuite la position de la lettre C parmi les $11 - 5 - 2 - 2 = 2$ positions restantes. Il y a alors $\binom{2}{1} = 2$ positions possibles.
   Il ne reste plus qu'un choix possible pour la lettre D.
   Au total, il y a donc
   $$\binom{11}{5} \times \binom{6}{2} \times \binom{4}{2} \times \binom{2}{1} = \frac{11!}{5!6!} \times \frac{6!}{2!4!} \times \frac{4!}{2!2!} \times \frac{2!}{1!1!} = \frac{11!}{5!2!2!} = 83160$$
   anagrammes possibles.
   -2$^{\text{ème}}$ méthode : On numérote les lettres de 1 à 11 afin de les discerner. On peut alors former 11! mots avec ces lettres distinctes. Mais chaque anagramme est alors compté plusieurs fois puisqu'il y a des lettres identiques. Chaque anagramme est compté exactement le nombre de fois qu'il y a de façons de permuter les lettres A, les lettres B et les lettres R, c'est-à-dire $5!2!2!$. Il y a donc $\frac{11!}{5!2!2!} = 83160$ anagrammes possibles.

2. Pour rejoindre le point de coordonnées (p,q) à partir du point de coordonnées $(0,0)$, on se déplace à chaque étape d'une unité vers la droite ou d'une unité vers le haut. On va donc devoir se déplacer au total de p unités vers la droite et de q unités vers le haut. *Faire un petit dessin pour visualiser un chemin possible.* On va donc se déplacer de $p+q$ unités, dont p unités vers la droite et q unités vers le haut. Un chemin peut donc être vu comme un mot à $p+q$ lettres, constituées des lettres D (déplacement vers la droite) et H (déplacement vers le haut). On peut donc choisir les positions des p lettres D parmi les $p+q$ positions : $\binom{p+q}{p}$. La position des lettres q est alors imposée.

   Il y a donc $\dbinom{p+q}{p}$ chemins possibles.

Exercice 3. Une urne contient 10 boules rouges numérotées de 1 à 10, 10 boules jaunes numérotées de 1 à 10, 10 boules bleues numérotées de 1 à 10 et 10 boules vertes numérotées de 1 à 10. On tire simultanément sans remise 5 boules dans l'urne. *On ne cherchera pas la valeur numérique des résultats.*

1. Combien y a-t-il de tirages contenant exactement une boule numérotée 1 ?
2. Combien y a-t-il de tirages contenant exactement trois boules rouges ?
3. Combien y a-t-il de tirages contenant exactement deux boules jaunes et deux boules bleues ?
4. Combien y a-t-il de tirages contenant au moins deux boules vertes ?
5. Combien y a-t-il de tirages contenant au moins une boule numérotée 5 et deux boules jaunes ?

Remarquons que le nombre de tirages possibles est $\binom{40}{5}$. En effet, on tire simultanément 5 boules dans l'urne : il n'y a donc pas de répétition et l'ordre n'importe pas. Il s'agit donc d'une 5-combinaison dans $[\![1,40]\!]$.

1. Dans l'urne, il y a 4 boules avec le numéro 1 (une de chaque couleur).
   On prend une boule parmi les 4 boules numérotées 1, puis 4 boules parmi les $40-4=36$ boules qui n'ont pas le numéro 1. Il y a donc
   $$\binom{4}{1}\times\binom{36}{4}$$
   tirages possibles.
2. Dans l'urne, il y a 10 boules rouges.
   On prend 3 boules parmi les 10 boules rouges, puis 2 boules parmi les $40-10=30$ boules qui ne sont pas rouges. Il y a donc
   $$\binom{10}{3}\times\binom{30}{2}$$
   tirages possibles.
3. Dans l'urne, il y a 10 boules jaunes et 10 boules bleues.
   On prend 2 boules parmi les 10 boules jaunes, puis 2 boules parmi les 10 boules bleues, puis 1 boule parmi les $40-10-10=20$ boules qui ne sont ni jaunes, ni bleues. Il y a donc
   $$\binom{10}{2}\times\binom{10}{2}\times\binom{20}{1}$$
   tirages possibles.
4. *Dans cette question, on utilise la formule* $\mathrm{card}(A)=\mathrm{card}(E)-\mathrm{card}(\complement_E A)$ *car il est plus facile de compter le nombre de tirages contenant* 0 *ou* 1 *boule verte.*
   Le nombre de tirages contenant au moins deux boules vertes est donc égal au nombre de tirages total moins le nombre de tirages contenant 0 ou 1 boule verte.
   Le nombre de tirages contenant 0 boule verte est $\binom{30}{5}$ (on choisit 5 boules parmi les $40-10=30$ boules qui ne sont pas vertes).
   Le nombre de tirages contenant 1 boule verte est $\binom{10}{1}\times\binom{30}{4}$ (on choisit 1 boule parmi les 10 boules vertes, puis 4 boules parmi les $40-10=30$ boules qui ne sont par vertes.)
   Le nombre de tirages contenant 0 ou 1 boule verte (on dit aussi, contenant au plus une boule verte) est donc égal à $\binom{30}{5}+\binom{10}{1}\times\binom{30}{4}$.
   Ainsi, le nombre de tirages contenant au moins deux boules vertes est
   $$\binom{40}{5}-\binom{30}{5}-\binom{10}{1}\times\binom{30}{4}.$$
5. Le nombre de boules qui ne sont ni jaunes, ni numérotées 5 est égal à $40-10-3=27$ (on enlève les 10 boules jaunes dont la boule jaune numéro 5, et les 3 autres boules numérotées 5).
   On regarde à nouveau le complémentaire. Les différents cas possibles sont les suivants :
   — 1 boule numéro 5 et 0 boule jaune : on tire 1 boule parmi les $4-1=3$ boules numérotées 5 qui ne sont pas jaunes, puis 4 boules parmi les 27 boules qui ne sont ni 5 ni jaunes, il y a donc $\binom{4}{1}\times\binom{27}{4}$ tirages,
   — 1 boule numéro 5 jaune et pas d'autres boules jaunes : on tire 1 boule parmi la seule boule 5 jaune, puis 4 boules parmi les 27 boules qui ne sont ni 5, ni jaunes, il y a donc $\binom{1}{1}\times\binom{27}{4}$ tirages,
   — 1 boule 5 non jaune et 1 boule jaune non 5 : on tire 1 boule parmi les 3 boules 5 non jaunes, puis 1 boule parmi les 9 boules jaunes non 5, puis 3 boules parmi les boules non 5 et non jaunes, il y a donc $\binom{3}{1}\times\binom{9}{1}\times\binom{27}{3}$,

— 0 boule numéro 5 et 0 boule jaune : on tire 5 boules parmi les 27 boules non jaunes et non 5, il y a donc $\binom{27}{5}$ tirages,

— 0 boule numéro 5 et 1 boule jaune : on tire 1 boule parmi les 9 boules jaunes non 5, puis 4 boules parmi les 27 boules non jaunes non 5, il y a donc $\binom{9}{1} \times \binom{27}{4}$,

— 0 boule numéro 5 et 2 boules jaunes : on tire 2 boules parmi les 9 boules jaunes non 5, puis 3 boules parmi les 27 boules non jaunes non 5, il y a $\binom{9}{2} \times \binom{27}{3}$.

Le nombre de tirages possibles est alors

$$\binom{40}{5} - \binom{4}{1}\binom{27}{4} - \binom{27}{4} - \binom{3}{1}\binom{9}{1}\binom{27}{3} - \binom{27}{5} - \binom{9}{1}\binom{27}{4} - \binom{9}{2}\binom{27}{3}.$$

Exercice 4. Soit E un ensemble à n éléments.

1. (a) Soit X une partie à p éléments de E. Combien y a-t-il de parties Y de E telles que $X \cap Y = \emptyset$?
   (b) Combien y a-t-il de couples (X, Y) formés de parties disjointes de E (ie telles que $X \cap Y = \emptyset$) ?
2. Combien y-a-t-il de couples (X, Y) de parties de E tels que $Y \subset X$?

---

1. (a) Une partie Y de E telle que $X \cap Y = \emptyset$ est une partie de $E \setminus X$ et réciproquement, toute partie Y de $E \setminus X$ vérifie $Y \cap X = \emptyset$. Autrement dit,
   $$\{Y \in \mathcal{P}(E) \mid Y \cap X = \emptyset\} = \mathcal{P}(E \setminus X).$$
   Comme $E \setminus X$ est de cardinal $n - p$, il existe 2^{n-p} parties de $E \setminus X$, donc le cardinal de $\{Y \in \mathcal{P}(E) \mid Y \cap X = \emptyset\}$ est égal à $\text{card}(\text{P}(E \setminus X)) = 2^{n-p}$.
   Il existe donc 2^{n-p} parties Y de E telles que $X \cap Y = \emptyset$.
   (b) Pour construire un couple (X, Y) de parties disjointes de E, on commence par choisir une partie X de E. Cette partie peut être de cardinal $p = 0$, ou $p = 1$, ou ... ou $p = n$.
   Fixons $p \in \{0, \ldots, n\}$. Il existe $\binom{n}{p}$ parties X de cardinal p dans E. Il y a donc $\binom{n}{p}$ possibilités pour le choix de X de cardinal p. Puis, pour chaque partie X fixée de cardinal p, on choisit Y telle que $X \cap Y = \emptyset$. D'après la question a), il y a 2^{n-p} possibilités.
   Au total, il y a donc $\sum_{p=0}^{n} \binom{n}{p} 2^{n-p}$ possibilités. On reconnaît le binôme de Newton avec $a = 1$ et $b = 2$. Donc $\sum_{p=0}^{n} \binom{n}{p} 2^{n-p} = (1 + 2)^n = 3^n$.
   Il y a donc 3^n couples (X, Y) formés de parties disjointes de E.
2. Pour construire un couple (X, Y) de parties de E telles que $Y \subset X$, on commence par choisir une partie X de E. Cette partie peut être de cardinal $p = 0$, ou $p = 1$, ou ... ou $p = n$.
   Fixons $p \in \{0, \ldots, n\}$. Il existe $\binom{n}{p}$ parties X de cardinal p dans E. Il y a donc $\binom{n}{p}$ possibilités pour le choix de X de cardinal p. Puis, pour chaque partie X fixée de cardinal p, on choisit Y telle que $Y \subset X$, autrement dit, Y est une partie de X. X étant de cardinal p, il y a 2^p possibilités pour Y.
   Au total, il y a donc $\sum_{p=0}^{n} \binom{n}{p} 2^p$ possibilités. On reconnaît le binôme de Newton avec $a = 2$ et $b = 1$. Donc $\sum_{p=0}^{n} \binom{n}{p} 2^p = (2 + 1)^n = 3^n$.
   Il y a donc 3^n couples (X, Y) de parties de E tels que $Y \subset X$.

Exercice 5. On note S_n^p le nombre de surjections de $\{1, \ldots, n\}$ sur $\{1, \ldots, p\}$ avec $(n, p) \in \mathbb{N}^{*2}$. Déterminer les nombres suivants :

$$S_n^p \text{ pour } p > n, \quad S_n^n, \quad S_n^1, \quad S_n^2 \quad \text{et} \quad S_{n+1}^n.$$

— Si $p > n$, alors il n'existe pas de surjection de $\{1, \ldots, n\}$ dans $\{1, \ldots, p\}$ donc $S_n^p = 0$.

— Supposons $p = n$. Alors l'ensemble de départ $E = \{1, \ldots, n\}$ et l'ensemble d'arrivée $F = \{1, \ldots, n\}$ sont finis et de même cardinal n. D'après le cours, les applications surjectives sont donc exactement les applications bijectives. Il existe $n!$ applications bijectives de E sur $F = E$. Donc $S_n^n = n!$.

— Si $p = 1$ alors l'ensemble d'arrivée a un unique élément, 1. Donc tout élément de $\{1, \ldots, n\}$ est envoyé sur l'élément 1. Il existe donc une unique application surjective, l'application constante égale à 1. Donc $S_n^1 = 1$.

— Supposons $p = 2$. Soit f une application de $\{1, \ldots, n\}$ dans $\{1, 2\}$. f n'est pas surjective si et seulement si f est constante égale à 1 ($\text{Im}(f) = \{1\}$) ou si f est constante égale à 2 ($\text{Im}(f) = \{2\}$). Or le nombre d'applications surjectives de $\{1, \ldots, n\}$ dans $\{1, 2\}$ est égal au nombre d'applications de $\{1, \ldots, n\}$ dans $\{1, 2\}$ (il y en a 2^n d'après le cours) moins le nombre d'applications NON surjectives.
Donc $S_n^2 = 2^n - 2$.

— Dire que f est une surjection de $\{1, \ldots, n+1\}$ dans $\{1, \ldots, n\}$ est équivalent à dire que deux entiers dans $\{1, \ldots, n+1\}$ ont la même image $k \in \{1, \ldots, n\}$ par f et les autres entiers ont des images distinctes et différentes de k.
Pour construire une surjection de $\{1, \ldots, n+1\}$ dans $\{1, \ldots, n\}$, on peut donc choisir deux entiers dans $\{1, \ldots, n+1\}$, il y a $\binom{n+1}{2}$ possibilités. Puis on choisit la valeur k de l'image commune dans $\{1, \ldots, n\}$ à ces deux entiers, il y a n

possibilités. Enfin, on choisit les images deux à deux distinctes des $n+1-2=n-1$ autres éléments de $\{1,\ldots,n+1\}$ dans $\{1,\ldots,n\}\setminus\{k\}$. Il y a $(n-1)!$ possibilités.

Au total, il y a donc $\binom{n+1}{2}n\times(n-1)!=\dfrac{n(n+1)}{2}\times n!=\dfrac{n(n+1)!}{2}$ possibilités.

D'où $S_{n+1}^{n}=\dfrac{n(n+1)!}{2}$.

2 Anneaux

Exercice 6. Donner l'ensemble G des inversibles de l'anneau $\mathbb{Z}/20\mathbb{Z}$. Montrer que (G,x) est isomorphe à $(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z},+)$

Les inversibles sont obtenus à partir des nombres premiers avec 20

$$G=\{1,3,7,9,11,13,17,19\}$$

3 est un élément d'ordre 4 dans $(G,\times)$ avec

$$\langle 3\rangle=\{1,3,9,7\}$$

et 11 est un élément d'ordre 2 n'appartenant pas à $\langle 3\rangle$. Le morphisme $\varphi:\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}\to G$ donné par

$$\varphi(k,\ell)=11^k\times 3^\ell$$

est bien défini et injectif par les arguments qui précèdent. Par cardinalité, c'est un isomorphisme.

Exercice 7. On pose $j:=e^{\frac{2i\pi}{3}}$. On pose

$$\mathbb{Z}[j]:=\{a+jb\in\mathbb{C}/(a,b)\in\mathbb{Z}^2\}$$

On U l'ensemble des éléments inversibles de $\mathbb{Z}[j]$.

1. Montrer que $1+j+j^2=0$
2. Montrer que $\mathbb{Z}[j]$ est un sous-anneau de $\mathbb{C}$.
3. Soit $z\in\mathbb{Z}[j]$. Montrer que $z\in U\Leftrightarrow |z|=1$
4. Soit $z=a+jb\in\mathbb{Z}[j]$. Montrer que $z\in U\Rightarrow(a,b)\in\{-1,0,1\}^2$
5. En déduire l'ensemble U.

---

1. On a $1+j+j^2=\dfrac{1-j^3}{1-j}=0$ car $j^3=1$ et $j\neq 1$.
2. On sait que $1\in\mathbb{Z}[j]$ car $1=1+0j$. Et pour tous a, b, a', $b'\in\mathbb{Z}$,
$$(a+jb)-(a'+jb')=(a-a')+j(b-b')\in\mathbb{Z}[j]$$
et
$$(a+jb)(a'+jb')=(aa'-bb')+(ab'+ba'-bb')j\in\mathbb{Z}[j].$$
Ce qui montre que $\mathbb{Z}[j]$ est un sous-anneaux de $\mathbb{C}$.
3. On calcule $|a+jb|^2=(a-\dfrac{b}{2})^2+\dfrac{3b^2}{4}=a^2+b^2-ab\in\mathbb{Z}$. On en déduit que si $a+jb$ est inversible dans $\mathbb{Z}[j]$, alors $|a+b|^2$, $|a+jb|^{-2}\in\mathbb{Z}$, d'où $|a+jb|=1$.
Réciproquement, si $|a+jb|=1$, alors $(a+jb)^{-1}=\overline{a+jb}=a+\overline{j}b=a-b-bj\in\mathbb{Z}[j]$, car $\overline{j}=j^2=-1-j$.
4. On doit résoudre $a^2-ab+b^2-1=0$, que l'on considère comme une équation du second degré d'inconnue a. On calcule son discriminant : $\Delta=b^2-4(b^2-1)=4-3b^2$ qui est positif ssi $b\in\{-1,0,1\}$ puisque $b\in\mathbb{Z}$. De même pour a.
5. On a ±1, $\pm j$, $\pm(1+j)=\pm j^2$ inversibles, soit 6 éléments inversibles. $\pm(1-j)$ et 0 ne sont as de modules 1 !

3 Corps

Exercice 8. Soient $A=\{a+b\sqrt{7},\,(a,b)\in\mathbb{Q}^2\}$ et $B=\{a+b\sqrt{11},\,(a,b)\in\mathbb{Q}^2\}$.

1. Démontrer que A et B sont des sous-corps de $(\mathbb{R},+,\times)$.
2. Montrer que l'application de A dans B définie par : $\varphi:a+b\sqrt{7}\longmapsto a+b\sqrt{11}$ est un morphisme de groupes mais n'est pas un morphisme de corps (calculer $\varphi(\sqrt{7}\times\sqrt{7})$).

---

1. On fait la la preuve pour A et on l'admet pour B. On a $A,\ B \subset \mathbb{R}$. Il suffit de montrer que $(A, +)$ sous-groupe et $(A^*, \times)$ sous-groupe, ce qui est immédiat.
2. On doit vérifier $\varphi(x+y) = \varphi(x) + \varphi(y)$ et $\varphi(xy) = \varphi(x)\varphi(y)$. Contrairement aux morphismes d'anneaux, il n'est pas nécessaire de montrer que $\varphi(1) = 1$ qui est une conséquence de ($\varphi : (A^*, \times) \to (B^*, \times)$ morphisme de groupes.

Exercice 9. Soit $M = \{aI_2 + bJ \in \mathcal{M}_2(\mathbb{R}) : a, b \in \mathbb{Q}\}$ où $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $J = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$.

1. Calculer J^2 et montrer que si $a, b \in \mathbb{R}$ et $aI_2 + bJ = O$ alors $a = b = 0$.
2. Montrer que, muni des lois usuelles sur $\mathcal{M}_2(\mathbb{R})$, M est un anneau. Cet anneau est-il commutatif, intègre ?
3. M est-il un corps ?
4. Que peut-on dire si on remplace $\mathbb{Q}$ par $\mathbb{R}$, c'est-à-dire $M = \{aI_2 + bJ \in \mathcal{M}_2(\mathbb{R}) : a, b \in \mathbb{R}\}$

---

1. On calcule facilement que $J^2 = 2I_2$ et on résout $aI_2 + bJ = 0$ implique $a = b = 0$.
2. On a $(aI_2 + bJ) - (a'I_2 + b'J) = (a - a')I_2 + (b - b')J$,
$$(aI_2 + bJ) \times (a'I_2 + b'J) = (aa' + 2bb')I_2 + (ab' + a'b)J$$
et si a et $b \neq 0$, $\left\{ \begin{array}{l} aa' + 2bb' = 1 \\ ab' + a'b = 0 \end{array} \right.$ donne $a' = \dfrac{a}{a^2 - 2b^2}$ et $b' = -\dfrac{b}{a^2 - 2b^2}$ (le dénominateur ne s'annule pas car $\sqrt{2}$ est irrationnel.
La formule du produit montre qu'il est commutatif.
Et si $aI_2 + bJ \neq 0$, alors le produit est nul ssi $(a' + b'J = 0$ (résoudre le système. L'anneau est intègre.
3. On a montré en fait que tout élement non nul est inversible, c'est un corps. On pouvait remarquer que $(a + b\sqrt{2}) \mapsto aI + bJ$ est un isomorphisme d'anneaux, ce qui répondait à toutes les questions d'un coup !
4. Si a et b sont dans $\mathbb{R}$, alors $a^2 - 2b^2 = 0$ a des solutions non triviales : par exemple $a = \sqrt{2}$ et $b = 1$. Et donc tout élément n'est plus inversible ! C'est un anneau.