Colle 16 – Questions de cours

Questions rapides

NB : pour chaque question, une justification claire et concise est attendue. Ces justifications ont été données en classe.

➤ Soient n et p deux entiers naturels, avec $p \leqslant n$. Combien existe t-il d'applications $f : \mathbb{N}_p \longrightarrow \mathbb{N}_n$ strictement croissantes ?

Réponse : $\dbinom{n}{p}$.

➤ Dans le plan, on trace n droites (avec n entier $\geqslant 3$) en position générale (deux à deux non-parallèles, trois à trois non-concourantes). Combien de triangles forme t-on ainsi ?

Réponse : $\dbinom{n}{3}$.

➤ Dans S_5, combien existe t-il de transpositions ?

Réponse : $\dbinom{5}{2} = \dfrac{5 \times 4}{2} = 10$.

➤ Dans S_5, combien existe t-il de 3-cycles ?

Réponse : $\dbinom{5}{3} \times 2 = \dbinom{5}{2} \times 2 = 20$.

➤ Dans S_5, combien existe t-il de produits de 2 transpositions à supports disjoints ?

Réponse : $\dbinom{5}{4} \times 3 = \dbinom{5}{1} \times 3 = 15$.

Question de cours n^{0}1 — **Propriété**. Soit E fini de cardinal n. Alors $\text{Card}(\mathscr{P}(E)) = 2^n$

Pour tout entier $k \in [\![0, n]\!]$, notons $\mathscr{P}_k(E)$ l'ensemble des parties de E de cardinal k.

On a : $\mathscr{P}(E) = \displaystyle\bigcup_{k=0}^{n} \mathscr{P}_k(E)$. Cette union étant disjointe (le cardinal d'une partie de E est unique), on en déduit que :

$$\text{Card}(\mathscr{P}(E)) = \sum_{k=0}^{n} \text{Card}\left(\mathscr{P}_k(E)\right) \qquad \text{Or pour tout } k \in [\![0, n]\!] \text{ on a : } \text{Card}\left(\mathscr{P}_k(E)\right) = \binom{n}{k}^{*}$$

Ainsi : $\text{Card}(\mathscr{P}(E)) = \displaystyle\sum_{k=0}^{n} \binom{n}{k} = (1+1)^n = 2^n$.

Question de cours n^{0}2 — **Propriété**. Soient A et B deux parties d'un même ensemble fini E.
Alors : $\text{Card}(E\backslash A) = \text{Card}(E) - \text{Card}(A)$, et $\text{Card}\,(A \cup B) = \text{Card}\,(A) + \text{Card}\,(B) - \text{Card}(A \cap B)$

Observons que : $E = (E\backslash A) \cup A$. Cette union étant disjointe, on a : $\text{Card}(E) = \text{Card}(E\backslash A) + \text{Card}(A)$. On en déduit la première égalité.

Dans le même registre : $A \cup B = (A\backslash B) \cup B$.
Cette union étant disjointe, on a : $\text{Card}(A \cup B) = \text{Card}\,(A\backslash B) + \text{Card}(B) \qquad (\spadesuit)$.
Par ailleurs : $A = (A\backslash B) \cup (A \cap B)$.
Cette nouvelle union étant disjointe, on a : $\text{Card}(A) = \text{Card}\,(A\backslash B) + \text{Card}(A \cap B)$.
Par suite : $\text{Card}\,(A\backslash B) = \text{Card}(A) - \text{Card}(A \cap B) \qquad (\clubsuit)$.
D'après $(\spadesuit)$ et $(\clubsuit)$: $\text{Card}\,(A \cup B) = \text{Card}\,(A) + \text{Card}\,(B) - \text{Card}(A \cap B)$.

Question de cours n^{0}3 — **Propriété**. Soient E et F deux ensembles finis, et $f : E \longrightarrow F$ une application. On suppose **Card** $(E) =$ **Card** (F). LASSE (les assertions suivantes sont équivalentes) :

1/ f est bijective 2/ f est injective 3/ f est surjective

Montrons $1) \Longrightarrow 2) \Longrightarrow 3) \Longrightarrow 1)$; la boucle sera ainsi bouclée !
Supposons E et F finis de même cardinal $n \in \mathbb{N}^*$.

• $1) \Longrightarrow 2)$: trivial.

• $2) \Longrightarrow 3)$: supposons f injective. On peut commencer par noter que $f(E)$ est une partie de F, ça ne mange pas de pain. En outre, puisque f est injective, $f(E)$ est un ensemble fini, de cardinal égal à celui de E (cours). Or $\text{Card}\,(E) = \text{Card}\,(F)$ (par hypothèse). Donc l'ensemble $f(E)$ est une partie de F, de cardinal égal à celui de F ; il s'ensuit que $f(E) = F$ (question de cours 7). Donc f est surjective, ce qui prouve l'implication.

• $3) \Longrightarrow 1)$: supposons à présent f surjective. Alors $f(E) = F$, donc $\text{Card}\,(f(E)) = \text{Card}\,(F)$, et par conséquent $\text{Card}\,(f(E)) = \text{Card}\,(E)$ (puisque $\text{Card}\,(E) = \text{Card}\,(F)$ par hypothèse). On en déduit (cours) que f est injective, et donc bijective. Ce qui prouve l'implication, et achève la preuve de la propriété.

∗. Par définition même des coefficients binomiaux.

Question de cours n⁰4 — **Théorème**. Si E est un ensemble fini de cardinal n, alors $(S_E, \circ)$ est un groupe fini de cardinal $n!$.

Un élément de S_E est une bijection de E dans E. En vertu de la question de cours 3, il existe autant de bijections de E dans E que d'injections de E dans E (puisque E est fini). Or le nombre d'injections de E dans E est : $\dfrac{n!}{(n-n)!} = n!$.[†]

Par suite, il existe $n!$ bijections de E dans E, ce qui assure déjà que : $\boxed{\text{Card}\,(S_E) = n!}$

En outre, la loi de composition ("o") est une *loi de composition interne* dans S_E (la composée de deux bijections est une bijection). Cette lci est *associative* car plus généralement la composition des applications l'est. Elle possède un *élément neutre* qui est l'identité de E. Enfin, tout élément f de S_E est *inversible* (pour la loi "o") dans S_E, car si f est bijective de E dans E, sa réciproque f^{-1} est elle aussi une bijection de E dans E.

Ce qui prouve que $(S_E, \circ)$ est un groupe, de cardinal $n!$.

Question de cours n⁰5 — **Lemme "fondamental"**. Soient n et m deux entiers naturels. S'il existe une injection de $\mathbb{N}_n$ dans $\mathbb{N}_m$, alors $n \leqslant m$.

Raisonnons par récurrence sur l'entier naturel n en posant :

$$\mathscr{P}(n) : \text{“s'il existe une injection de } \mathbb{N}_n \text{ dans } \mathbb{N}_m \text{, alors } n \geqslant m\text{”}$$

➥ Initialisation $(n = 0)$: OK.[‡]

➥ Hérédité : supposons la propriété établie jusqu'à un certain entier naturel n, et montrons que $\mathscr{P}(n+1)$ est vraie.

Considérons $f : \mathbb{N}_{n+1} \longrightarrow \mathbb{N}_m$ une application injective. Deux cas peuvent alors se présenter ; soit $f\,(n+1) = m$, soit $f\,(n+1) \neq m$.

Premier cas — Si $f\,(n+1) = m$: on introduit alors la restriction de f à $\mathbb{N}_n$, que nous noterons g. Pour mémoire, il s'agit de l'application $g = f_{|\mathbb{N}_n} : \mathbb{N}_n \longrightarrow \mathbb{N}_m$ définie en posant : $\forall\, k \in \mathbb{N}_n,\ g(k) = f(k)$.[§]

L'application g est encore injective, puisque f l'est et que la restriction d'une application injective l'est encore.
En outre g est à valeurs dans $\mathbb{N}_{m-1}$, puisque m ne peut avoir d'antécédent par g. En effet, s'il existait un entier $k \in \mathbb{N}_n$ tel que $g(k) = m$, alors on aurait $f(k) = m$ (par définition de g) et $f(n+1) = m$ (par hypothèse). L'injectivité de f impliquerait alors $k = n+1$, ce qui est absurde puisque $k < n+1$.

En résumé, l'application g induit une application injective de $\mathbb{N}_n$ dans $\mathbb{N}_{m-1}$. Par hypothèse de récurrence, on en déduit que $\boxed{n \leqslant m-1, \text{ d'où } n+1 \leqslant m}$.

Second cas — Si $f\,(n+1) \neq m$: on introduit alors l'application (c'est une transposition) :

$$\begin{array}{rcl} \tau : \mathbb{N}_m & \longrightarrow & \mathbb{N}_m \\ m & \longmapsto & f\,(n+1) \\ f\,(n+1) & \longmapsto & m \\ k & \longmapsto & k \text{ si } k \neq f\,(n+1) \text{ et } k \neq m \end{array}$$

L'application τ est bijective, car c'est clairement une involution (Toronto est l'identité de $\mathbb{N}_m$, ah, ah, ah !).

Cette remarque faite, on introduit l'application : $F = \tau \circ f : \mathbb{N}_n \longrightarrow \mathbb{N}_m$. L'application F est injective, car c'est la composée de τ (injective car bijective) et de f (injective par hypothèse).

De plus, $F\,(n+1) = \tau\,(f\,(n+1)) = m$. On est ainsi ramenés au premier cas, et on peut conclure que $n+1 \leqslant m$.

Dans les deux cas, on a établi (sous l'hypothèse que $\mathscr{P}(n)$ est vraie) que s'il existe une application injective de $\mathbb{N}_{n+1}$ dans $\mathbb{N}_m$, alors $n+1 \leqslant m$. Ce qui prouve que la propriété $\mathscr{P}(n+1)$ est vraie. La propriété est donc initialisée et héréditaire, et on peut donc conclure.

Conclusion. S'il existe une injection de $\mathbb{N}_n$ dans $\mathbb{N}_m$, alors $n \leqslant m$.

---

†. Plus généralement, le nombre d'applications injectives de E dans F est $\dfrac{n!}{(n-p)!}$ si $\text{Card}(E) = p \leqslant n = \text{Card}(F)$.

‡. On pourra puissamment observer que tout entier naturel est supérieur ou égal à zéro.

§. "g est définie par la même formule que f, sur un ensemble de définition plus petit".

Question de cours n^{0}6 — **Théorème 1**. Toute partie A d'un ensemble fini E est elle-même un ensemble fini, et $\text{Card}(A) \leqslant \text{Card}(E)$. De plus, $A = E \Longleftrightarrow \text{Card}(A) = \text{Card}(E)$.

Prouvons par récurrence sur n que toute partie d'un ensemble fini à n éléments est elle-même finie, en posant :

$\mathscr{P}(n)$: "si E est fini de cardinal n, alors toute partie A de E est finie et $\text{Card}(A) \leqslant \text{Card}(E)$".

➥ Initialisation $(n = 0)$: OK. [¶]

➥ Hérédité : supposons la propriété établie jusqu'à un certain entier naturel n, et montrons que $\mathscr{P}(n+1)$ est vraie.

Soit E un ensemble à $n+1$ éléments, et a un élément de E.

Soit A une partie de E. Deux cas peuvent alors se présenter : soit $a \in A$, soit $a \notin A$.

Premier cas — Si $a \in A$: alors l'ensemble $A \backslash \{a\}$ est une partie de l'ensemble $E \backslash \{a\}$. D'après le cours : $\text{Card}\,(E \backslash \{a\}) = \text{Card}\,(E) - 1 = n$. Ainsi $A \backslash \{a\}$ est une partie d'un ensemble à n éléments. Par hypothèse de récurrence, elle est donc finie, et : $\text{Card}\,(A \backslash \{a\}) \leqslant n$. Il s'ensuit que : $\text{Card}\,(A) \leqslant n+1$.

Second cas — Si $a \notin A$: alors l'ensemble A est une partie de l'ensemble $E \backslash \{a\}$, qui possède n éléments. Il s'ensuit, par hypothèse de récurrence, que A est finie, et que $\text{Card}\,(A) \leqslant n$. Puisque qui peut le plus peut le moins, on a aussi : $\text{Card}\,(A) \leqslant n+1$.

Dans les deux cas, on a établi que toute partie d'un ensemble à $n+1$ éléments est finie, de cardinal au plus égal à $n+1$, ce qui établit l'hérédité de la propriété.

Conclusion. Toute partie A d'un ensemble fini E est elle-même un ensemble fini, et $\text{Card}(A) \leqslant \text{Card}(E)$.

Cas d'égalité : montrons l'implication $[\text{Card}(A) = \text{Card}(E)] \Longrightarrow [A = E]$, en établissant la contraposée. Si $A \neq E$, alors il existe $x \in E \backslash A$. On a donc $A \subset E \backslash \{x\}$, et par suite : $\text{Card}(A) \leqslant (n-1)$, d'où en particulier : $\text{Card}(A) \neq \text{Card}(E)$. En résumé : $[A \subsetneq E] \Longrightarrow [\text{Card}(A) \neq \text{Card}(E)]$, ce qui équivaut à : $[\text{Card}(A) = \text{Card}(E)] \Longrightarrow [A = E]$. Comme il est par ailleurs clair que : $[A = E] \Longrightarrow [\text{Card}(A) = \text{Card}(E)]$, on peut conclure : $\boxed{[A = E] \Longleftrightarrow [\text{Card}(A) = \text{Card}(E)]}$.

Question de cours n^{0}7 — **Théorème**. Soit n un entier naturel supérieur ou égal à 2, et soit $\sigma \in S_n$. Il existe un entier $k \leqslant n$, et k transpositions $\tau_1, \ldots, \tau_k$ de S_n tels que : $\sigma = \displaystyle\prod_{i=1}^{k} \tau_i$.

Raisonnons par récurrence sur l'entier naturel n en posant pour tout $n \in \mathbb{N} \backslash \{0,1\}$:

$\mathscr{P}(n)$: "Pour tout $\sigma \in S_n$ il existe un entier $k \leqslant n$ et k transpositions $\tau_1, \ldots, \tau_k$ de S_n tels que : $\sigma = \displaystyle\prod_{i=1}^{k} \tau_i$"

➥ Initialisation $(n = 2)$: les permutations de S_2 sont l'identité (produit de 0 transposition… ou de deux !) et (12) (produit d'une transposition), ce qui assure que $\mathscr{P}(2)$ est vraie.

➥ Hérédité : supposons la propriété établie jusqu'à un certain entier naturel n, et montrons que $\mathscr{P}(n+1)$ est vraie.

Soit $\sigma \in S_{n+1}$. On peut distinguer deux cas : $\sigma\,(n+1) = n+1$ et $\sigma\,(n+1) \neq n+1$.

Premier cas — Si $\sigma\,(n+1) = n+1$: dans ce cas, la restriction $\sigma_{|\mathbb{N}_n}$ est une permutation de $\mathbb{N}_n$. Par hypothèse de récurrence, il existe un entier $k \leqslant n$ et k transpositions $\tau_1, \ldots, \tau_k$ de S_n tels que : $\sigma_{|\mathbb{N}_n} = \displaystyle\prod_{i=1}^{k} \tau_i$.

Il reste à voir qu'une transposition dans S_n est aussi une transposition dans S_{n+1} ; en effet, une transposition de S_n s'écrit (ab) avec a et b deux entiers distincts dans $\mathbb{N}_n$; ce sont donc naturellement deux entiers distincts dans $\mathbb{N}_{n+1}$. Et puisque $\sigma\,(n+1) = n+1$, on a donc : $\sigma = \displaystyle\prod_{i=1}^{k} \tau_i$ (égalité dans S_{n+1}). Ainsi, sous l'hypothèse $\sigma\,(n+1) = n+1$, il existe un entier $k \leqslant n$ (en particulier $k \leqslant n+1$) et k transpositions $\tau_1, \ldots, \tau_k$ de S_{n+1} tels que : $\sigma = \displaystyle\prod_{i=1}^{k} \tau_i$.

Second cas — Si $\sigma\,(n+1) \neq n+1$: dans ce cas, on introduit la permutation $\rho = (\sigma\,(n+1)\;\; n+1)\,\sigma$. [‖]

ρ est un élément de S_{n+1}, qui vérifie : $\rho\,(n+1) = n+1$. En vertu de l'étude faite dans le premier cas : il existe un entier $k \leqslant n$ et k transpositions $\tau_1, \ldots, \tau_k$ de S_{n+1} tels que : $\rho = \displaystyle\prod_{i=1}^{k} \tau_i$. Par suite, on a : $\sigma = (\sigma\,(n+1)\;\; n+1) \displaystyle\prod_{i=1}^{k} \tau_i$. La permutation σ est ainsi écrite comme produit de $k+1$ transpositions (et $k+1 \leqslant n+1$).

Synthèse : dans les deux cas, on a montré que $\sigma \in S_{n+1}$ peut s'écrire comme produit de K transpositions, avec $K \leqslant n+1$. Ce qui assure que $\mathscr{P}\,(n+1)$ est vraie, et achève la preuve de l'hérédité.

¶. La description des parties de l'ensemble vide étant relativement rapide.

‖. La permutation ρ est le produit de σ, et de la transposition échangeant $\sigma\,(n+1)$ et $n+1$.

Conclusion. Pour tout entier naturel $n \geqslant 2$, et pour toute permutation $\sigma \in S_n$ il existe un entier $k \leqslant n$ et k transpositions $\tau_1, \ldots, \tau_k$ de S_n tels que : $\sigma = \prod_{i=1}^{k} \tau_i$. En d'autres termes, les transpositions engendrent le groupe symétrique.

Hors-programme de colle — **Exercice**. Deux permutations à supports disjoints commutent.

➤ On commence par prouver que si un entier k appartient au support d'une permutation σ, alors $\sigma(k)$ appartient également au support de σ.

Considérons donc un entier $k \in \text{supp}(\sigma)$. Par l'absurde, supposons que $\sigma(k)$ n'appartienne pas au support de σ. Alors :

$$\sigma(\sigma(k)) = \sigma(k) \text{ d'où } (\sigma \text{ étant injective}) : \sigma(k) = k$$

Ce qui contredit l'hypothèse "$k \in \text{supp}(\sigma)$". Donc $\sigma(k) \in \text{supp}(\sigma)$.

En résumé : $\forall \sigma \in S_n, \forall k \in \mathbb{N}_n, \ [k \in \text{supp}(\sigma)] \Longrightarrow [\sigma(k) \in \text{supp}(\sigma)]$ $\quad (\spadesuit)$

➤ La preuve du lemme est à présent une formalité. Soient φ et ρ deux éléments de S_n, à supports disjoints.

Soit k un entier de $\mathbb{N}_n$. Puisque $\text{supp}(\varphi) \cap \text{supp}(\rho) = \emptyset \quad (\clubsuit)$, on peut distinguer 3 cas :

➣ *Premier cas :* $k \in \text{supp}(\varphi)$. Alors on a : $k \notin \text{supp}(\rho)$ (selon $(\clubsuit)$), et $\varphi(k) \in \text{supp}(\varphi)$ (selon $(\spadesuit)$), donc $\varphi(k) \notin \text{supp}(\rho)$ (re-$(\clubsuit)$).

On en déduit que : $\quad \varphi(\rho(k)) = \varphi(k)$ et $\rho(\varphi(k)) = \varphi(k)$. Donc : $\varphi(\rho(k)) = \rho(\varphi(k))$.

➣ *Second cas :* $k \in \text{supp}(\rho)$. D'après le premier cas : $\varphi(\rho(k)) = \rho(\varphi(k))$.

➣ *Troisième cas :* $k \notin (\text{supp}(\rho) \cup \text{supp}(\varphi))$. Alors : $\varphi(\rho(k)) = \rho(\varphi(k)) = k$.

➣ *Conclusion :* $\forall k \in \mathbb{N}_n, \ \varphi(\rho(k)) = \rho(\varphi(k)) = k$. Ainsi : $\varphi \circ \rho = \rho \circ \varphi$.

Conclusion. Deux permutations à supports disjoints commutent.