Corrigé RMS 2024

Alex6oko L. Mai 2025

Note sur les intitulés des exercices :
Les lettres qui précèdent les énoncés indiquent la provenance de l'exercice :

- **X** : École polytechnique
- **U** : ENS Ulm
- **L** : ENS Lyon
- **S** : ENS Paris-Saclay
- **R** : ENS Rennes

Corrigé personnel qui retrace l'évolution de la pensée du narrateur au cours de sa résolution, le narrateur le juge "solide" (sans laisser de définition de solidité). S'il te semble friable à certains endroits, fais-le moi savoir, mais sache que... : alexislcrd@gmail.com. *Le narrateur a délibérément enlevé les étoiles de difficulté.* Clique ici pour avoir tout les énoncés RMS

Exercice – ULSR

On étend de façon naturelle la valuation 2-adique v_2 à $\mathbb{Q}$. Pour un entier N, soit :

$$H_N = \sum_{k=1}^{N} \frac{1}{k}$$

Calculer $v_2(H_N)$.

Proposition de corrigé :

Premièrement, pour tout $N \in \mathbb{N}^*$, on a :

$$H_N = \sum_{k=1}^{N-1} \frac{1}{k} + \frac{1}{N} = H_{N-1} + \frac{1}{N}$$

Notons $H_{N-1} = \frac{p}{q}$ écrit en fraction irréductible, ainsi on peut réécrire H_{N-1} sous la forme $\frac{a}{2^b d}$, avec :

$$\gcd(a,2) = 1, \quad \gcd(2,d) = 1, \quad b = -v_2(H_{N-1}) \in \mathbb{Z} \text{ à priori.}$$

Toutefois si l'on avait b entier naturel, alors $H_N = \frac{aN+2^b d}{2^b dN}$. Ainsi en supposant ensuite N impair, on aurait $2 \nmid aN + 2^b d$, car
$\gcd(a,2) = 1$, ainsi dans ce cas $v_2(H_N) = v_2(H_{N-1})$, car $gcd(2,d) = 1$. En calculant pour quelques valeurs $v_2(H_N)$, on "sent" que b est un entier naturel.
Montrons alors par récurrence sur l'entier N que $v_2(H_N) \leq 0$ (**Lemme 1**).
Initialisation en N=1 : jugée triviale

Hérédité : Soit N ≥ 2, supposons le résultat vrai au rang N-1, montrons le au rang N.
En gardant l'écriture qu'on avait précédement, $H_N = \frac{aN+2^b d}{2^b dN}$ (avec N impair ou pair ici parcontre). Par "extension" de v_2 de $\mathbb{Z}$ à $\mathbb{Q}$, $v_2(H_N) = v_2(\frac{aN+2^b d}{2^b dN}) = v_2(aN+2^b d) - v_2(2^b dN)$, si N est impair alors le résultat est trivial. Si N est pair, le calcul donne $v_2(H_N) = v_2(aN+2^b d) - v_2(2^b dN) = min(v_2(N), b) - (v_2(N) + b))$.
Si $min(v_2(N), b) = b$ alors $v_2(H_N) = -v_2(N) \leq 0$, car N $\in \mathbb{N}$.
Sinon si $min(v_2(N), b) = v_2(N)$ alors $v_2(H_N) = -b \leq 0$, par hypothèse de récurrence.

Conclusion : Ok !
Donc on a établi par le **Lemme 1** que si N est impair, $v_2(H_N) = v_2(H_{N-1})$. On sait alors que $(v_2(H_N))$ est une suite par paliers (de taille au moins 2 quand n est plus grand que 2). En calculant les valuations 2-adiques pour plusieurs valeurs, on conjecture le résultat suivant :

$$v_2(H_n) = -k \quad \text{pour } n = \sum_{i=0}^{k-1} 2^i + 1 = 2^{k-1} + 1 \text{ à } \sum_{i=0}^{k} 2^i = 2^k \text{ occurrences consécutives.}$$

C'est-à-dire $v_2(H_n) = -\lfloor \log_2(n) \rfloor$, pour tout entier naturel n.

Montrons le résultat par récurrence (on ne fait que l'hérédité mes frères). Soit n un entier naturel non nul, On a $H_{n+1} = H_n + \frac{1}{n+1}$ donc $v_2(H_{n+1}) = min(v_2(H_n), v_2(\frac{1}{n+1})) =$ min(-$\lfloor \log_2(n) \rfloor, v_2(\frac{1}{n+1})$) (par hypothèse de récurrence).

Or $v_2(\frac{1}{n+1}) = -v_2(n+1) \geq -\lfloor \log_2(n+1) \rfloor$.
Et si n+1 n'est pas une puissance de 2, alors $\lfloor \log_2(n+1) \rfloor = \lfloor \log_2(n) \rfloor$.
Sinon si $n+1 = 2^k$, alors $v_2(n+1) = k = \log_2(n+1)$, donc : $v_2\left(\frac{1}{n+1}\right) = -k = -\lfloor \log_2(n+1) \rfloor \leq -\lfloor \log_2(n) \rfloor$
Donc dans tout les cas, $v_2(\frac{1}{n+1}) \leq -\lfloor \log_2(n) \rfloor$. Donc $v_2(H_{n+1}) = -\lfloor \log_2(n+1) \rfloor$
CQFD

Exercice – ULSR

Soit $(m, n, p) \in (\mathbb{N}^*)^3$, avec p premier supérieur ou égal à 5, m et p premiers entre eux.

a) Montrer que
$$\binom{np}{m} \equiv 0 \pmod{p}.$$

b) Montrer que
$$\binom{np}{mp} = \sum_{k=0}^{p} \binom{p(n-1)}{mp-k}\binom{p}{k}.$$

c) Montrer que
$$\binom{np}{mp} \equiv \binom{n}{m} \pmod{p^2}.$$

L'objectif de la suite est de montrer que
$$\binom{2p}{p} \equiv 2 \pmod{p^3}.$$

d) Montrer que $\forall k \in [\![1, p]\!]$,
$$\binom{p-1}{k-1} \equiv \pm 1 \pmod{p}.$$

e) Montrer que
$$\sum_{k=1}^{p-1} \left(\frac{(p-1)!}{k}\right)^2 \equiv 0 \pmod{p}.$$

f) Conclure.

Proposition de corrigé :

a) Premièrement, on élague tout les cas pathologiques (qui sont triviaux car p|0) en prenant m dans $[\![1, np]\!]$. Ensuite, un exo classique, que l'on nommera **Lemme uno**, consiste à montrer que si $\gcd(m, p) = 1$, alors $p \mid \binom{p}{m}$. Le narrateur le laisse en guise d'exercise, il suffit d'appliquer la Formule du pion + le lemme de Gauss. Avec le **Lemme uno**, on a gratuitement (si vous savez le montrer) le cas n=1.

Pour $n \geq 2$. Il suffit d'observer que $\binom{p}{m} \mid \binom{np}{m}$ (développer les coefficients binomiaux pour s'en convaincre). Donc p divise $\binom{np}{m}$.

b) Par un raisonnement combinatoire :
On veut prendre mp élements d'un ensemble E à np élements, soit. Considérons F un sous -ensemble de E à p élements. Prendre mp élements de E, revient à prendre k élements de F (pour $k \in [\![0, p]\!]$), puis à compléter indépendamment avec mp-k élements dans $E \backslash F$ de cardinal pn-p.

D'où :
$$\binom{np}{mp} = \sum_{k=0}^{p} \binom{p(n-1)}{mp-k}\binom{p}{k} \quad (\textbf{"Analogue" à l'identité de Vandermonde})$$

c) 6oko a trimé... En utilisant b), puisque on montre aisément (lecteur [...])

que p divise $\binom{p}{k}$ et p divise $\binom{p(n-1)}{mp-k}$, pour k $\in [\![1, p-1]\!]$. Alors $\binom{np}{mp} \equiv \binom{p(n-1)}{p(m-1)} + \binom{p(n-1)}{mp} \; mod\, p^2$.

Maintenant, si l'on suppose par récurrence (l'initialisation uniquement pour le lecteur) que la formule qu'on veut montrer est vraie au rang n-1 et m premier avec p, on a :
$\binom{p(n-1)}{p(m-1)} \equiv \binom{n-1}{m-1} \; mod\, p^2$ et $\binom{p(n-1)}{mp} \equiv \binom{n-1}{m} \; mod\, p^2$.

Donc $\binom{np}{mp} \equiv \binom{n-1}{m-1} + \binom{n-1}{m} \; mod\, p^2$, i.e (Formule de Pascal) $\binom{np}{mp} \equiv \binom{n}{m} \; mod\, p^2$.

d) Montrons le résultat par récurrence.

Initialisation : Triviale.

Hérédité : Supposons le résultat vrai jusqu'au rang $k \in [\![2, p-1]\!]$.
Alors d'après la formule de Pascal $\binom{p-1}{k-1} + \binom{p-1}{k} = \binom{p}{k} \equiv 0 \; mod\, p$, d'après le **Lemme uno**.
Donc $\binom{p-1}{k} \equiv -\binom{p-1}{k-1} \equiv \pm 1 \; mod\, p$ (par hypothèse de récurrence).

Conclusion : Ok !

e) Le "(p-1) ! mod p" fait évidemment penser au **Théorème de Wilson** :

$\forall p \in \mathbb{P}, \quad (p-1)! \equiv -1 \pmod{p}$. (Le narrateur a le coeur sur la main et va vous donner une preuve de ce classique). Rapidement, on se place dans $\mathbb{Z}/p\mathbb{Z}$, (p-1) ! est le produit de tout les éléments (non nuls) de $\mathbb{Z}/p\mathbb{Z}$. Or $\mathbb{Z}/p\mathbb{Z}$ est un corps (p est premier), donc tout ses élements non nuls sont inversibles. Donc vu que $\mathbb{Z}/p\mathbb{Z}$ est commutatif, les élements se simplifie avec leur inverses dans le produit, si p-1 avait son inverse k représenté dans $[\![2, p-2]\!]$, alors (p-1)k=1 alors p-1=k, ce qui est absurde ! Donc p-1 est son propre inverse ainsi que 1 et aucun autre (sinon si $k^2 = 1 \; alors \; (k-1)(k+1) = 0 \; alors$ k-1=0 ou k+1=0 i.e k=1 ou k=p-1).
Il restera alors 1.(p-1)= -1 mod p.

Ainsi, on réécrit la somme $\sum_{k=1}^{p-1} \left(\frac{(p-1)!}{k}\right)^2 \equiv \sum_{k=1}^{p-1} (k^{-1})^2 \pmod{p}$. Sauf que $\mathbb{Z}/p\mathbb{Z}$ est un corps, sommer sur les inverses au lieu des élements en soi ne change rien. Cette somme vaut alors (modulo p) $\sum_{k=1}^{p-1} k^2 = \frac{p(p-1)(2p-1)}{6}$. Or 6|(p-1)(2p-1) (6oko invite le lecteur a montrer cela, c'est vite fait technique (penser à 6=2x3)). On a alors montré que $\sum_{k=1}^{p-1} \left(\frac{(p-1)!}{k}\right)^2$ était divisible par p. CQFD

f) On a d'après b),

$$\binom{2p}{p} = \sum_{k=0}^{p} \binom{p}{k}^2 = \sum_{k=1}^{p-1} \binom{p}{k}^2 + 2 = 2 + \sum_{k=1}^{p-1} \frac{p^2}{k^2} \binom{p-1}{k-1}^2 \; (Form.\; du\; pion)$$

Or d'après d), $\forall k \in [\![1, p]\!], \quad \binom{p-1}{k-1} \equiv \pm 1 \pmod{p}$. Alors ce coefficient binomial ± 1 est un multiple de p. Il restera alors modulo p^3 : $2 \pm p^2 \sum_{k=1}^{p-1} \frac{1}{k^2} = 2 \pm \frac{p^2}{((p-1)!)^2} \sum_{k=1}^{p-1} \frac{((p-1)!)^2}{k^2}$. Or d'après e), $\sum_{k=1}^{p-1} \frac{((p-1)!)^2}{k^2}$ est un multiple de p. Ainsi il ne restera que le 2 modulo p^3.

Exercice – L

On considère l'équation :

$$2^a + 3^b = 5^c \quad \text{où } (a, b, c) \in \mathbb{N}^3.$$

(a) Résoudre l'équation dans le cas où $a = b = c$.

(b) Traiter le cas où b est impair.

(c) Traiter le cas où c est impair.

(d) Traiter le cas général.

Proposition de corrigé :

a) 6oko a d'abord essayé de mettre des coups de valuation p-adique, mais ça n'aboutit jamais ici. Car, par exemple on aura : $v_5(2^a + 3^a) = a$, on a ensuite envie de dire, comme dans l'exercise 1, que $v_5(2^a + 3^a) = min(v_5(2^a), v_5(3^a)) = 0 = a$; or la formule du min n'a plus de sens, si les élements ne sont pas divisibles par 5 (car ça découle d'une factorisation).

Toutefois cet exercice, se ramène à l'exercice trivial suivant :
Etant donné n entier, trouver tout les couples (x,y) $\in \mathbb{R}^{+*}, x \neq y$, tels que,
$(x + y)^n = x^n + y^n$.
Pour le résoudre, en binômiant de Newton, comme x,y>0, on a $(x + y)^n > x^n + y^n$ sauf si n=1. Donc on a aucune solution, sauf si n=1.

Donc a=1 obligatoirement si on a une solution, or ça marche, donc a=1 est la seule solution.

b) En supposant b impair (b>1), on a $3^b \equiv 1 \ mod\ 4$. Or $2^a \equiv 0 \ mod\ 4$ et $5^c \equiv 1 \ mod\ 4$.
Donc on a aucune solution si b est impair.

c) A tâtons, modulo 8 on a une contradiction, en calculant toutes les combinaisons possibles.

d) Si on a une solution, alors c et b sont pairs (d'après b) et c)). De plus en raisonnant modulo 3, on a nécessairement c et a qui ont même parité. Donc a,b et c sont pairs.
L'équation se réécrit ainsi : $2^{2l} + 3^{2m} = 5^{2n}$, où $(l, m, n) \in \mathbb{N}$. En faisant passer 2^{2l} de l'autre côté, on a 25-4=21 qui divise 3^{2m}, ce qui est impossible. Donc la seule solution c'est quand a=b=c=1 (d'après a)).

Exercice – ULSR

(a) Montrer que les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont cycliques.

(b) Alice et Barbara jouent à un jeu. Elles choisissent à tour de rôle un élément de $\mathbb{Z}/n\mathbb{Z}$ sans remise qu'elles ajoutent à un ensemble S. Le jeu s'arrête quand S engendre $\mathbb{Z}/n\mathbb{Z}$ et la joueuse ayant tiré le dernier numéro perd. Selon n, y a-t-il une stratégie gagnante pour la première joueuse ?

(c) Même question avec le groupe S_n.

Proposition de corrigé :

a) Il est classique de savoir montrer que tout les sous groupes d'un groupe cyclique sont

cycliques. C'est exactement ce qu'on nous demande, car tout groupe cyclique est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Une preuve de la cyclicité des sous-groupes ? Allez !

Soit H un sous-groupe de G=$\mathbb{Z}/n\mathbb{Z}$, H est fini car G est fini.

Montrons maintenant que H est monogène (partie délicate) :
Puisque G est monogène, G s'écrit en extension $\{1, p, p^2, ..., p^{n-1}\}$, avec p premier avec n. Si p ∈ H alors H=G et H est monogène, sinon il existe un plus petit élement j ∈ $[\![2, n-1]\!]$ tel que $p^j \in H$. Montrons que $H = \langle p^j \rangle$.

L'inclusion réciproque est évidente. L'inclusion directe moins. Soit h ∈ H, $h = p^a$, où $a \in [\![2, n-1]\!]$ (à *priori*). Par division euclidienne, il existe v ∈ $\mathbb{N}$ et r ∈ $[\![0, j-1]\!]$, tels que a=jv + r. Alors $h = p^{jv+r} = p^r(p^j)^v$ (car H est commutatif car G l'est). En multipliant à droite par l'inverse de $(p^j)^v$, on a $p^r \in H$ donc r=0 (car j est le plus petit exposant, n'oublions pas). Donc $h \in \langle p^j \rangle$

b) Prend un élement p premier avec n et c'est fini. La preuve c'est du cours (lecteur utilise bézout). Toutefois si n=2, elle perd forcément.

c) S_n n'est pas monogène. Car il est engendré par les transpositions, donc s'il était monogène, un produit de transpositions engendrerait le groupe, mais alors une transposition donnée ne pourrait pas être engendrée par le groupe engendré par cet élement (preuve avec les mains). Il n'y a pas de stratégie gagnante, sauf dans les cas triviaux.

Exercice – U

Soient G un groupe, A une partie finie non vide de G. Montrer que $|A| = |AA|$ si et seulement si $A = xH$ avec $x \in G$ et H sous-groupe de G tel que $x^{-1}Hx = H$.

Proposition de corrigé :

Soit $(x, y) \in A^2$ avec $x \neq y \neq e_G$, nous avons $xA \subset AA$ et $yA \subset AA$, donc $xA \cup yA \subset AA$. Ainsi, $|xA \cup yA| \leq |AA|$. Or, $|xA \cup yA| = |xA| + |yA| - |xA \cap yA| \leq |AA|$, et étant donné que $xA \cong A$, on a $|xA \cup yA| = 2|A| - |xA \cap yA| = 2|AA| - |xA \cap yA| \leq |AA|$.
D'où : $|AA| \leq |xA \cap yA|$. Or $xA \cap yA \subset xA$, et on a vu que |xA|=|A|, alors on a $|AA| \leq |xA \cap yA| \leq |A| = |AA|$. Ainsi $|AA| = |A| = |xA \cap yA|$.
Mais |xA|=|A|, et $xA \cap yA \subset xA$, donc on a $xA \cap yA = xA$. Ainsi (encore ? - oui), xA=AA(=Ax) car $xA \subset AA$ (et ont le même cardinal, par ce qu'on a fait juste avant).

Et là, on a quasiment fini. Pourquoi ? Attends !
Car en posant $H = x^{-1}A$, on a définit un groupe, car pour h_1 et h_2 dans H, alors $xh_1 \in A$ et $h_2x \in A$, d'où $xh_1h_2x \in AA = Ax$, donc $xh_1h_2 \in A$, donc $h_1h_2 \in H$.
Enfin $e_G \in H$ (car $x \in A$). H est stable par passage à l'inverse, car $x^{-1}A = Ax^{-1}$.
Merci à @Valentin9912, @Jakobus et @Gillianseed pour le coup de pouce.
Puis trivialement A=xH, et $x^{-1}Hx = x^{-1}x^{-1}Ax = x^{-1}A = H$.

La réciproque est triviale, AA=xHxH=xxHH=x^2H, or |xH|=$|x^2H|$, CQFD.

Exercice – ULSR

Soit

$$A = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \in M_3(\mathbb{F}_3).$$

On admet que $A^{13} = -I_3$.

a) Quels calculs auriez-vous fait pour justifier que $A^{13} = -I_3$?

b) Montrer que $A \in \mathrm{GL}_3(\mathbb{F}_3)$ et que A est d'ordre 26 dans ce groupe.

c) On note G le sous-groupe de $\mathrm{GL}_3(\mathbb{F}_3)$ engendré par A, et on pose

$$V = G \cup \{0\}.$$

Montrer que $V = \mathrm{Vect}(I_3, A, A^2)$.

d) On pose $W = \mathrm{Vect}(I_3, A)$. Montrer que, pour tout $M \in G$, il existe $N, P \in W \setminus \{0\}$ telles que

$$M = P^{-1}N.$$

e) On note H le sous-groupe de $\mathrm{GL}_3(\mathbb{F}_3)$ engendré par A^2. Montrer que H est isomorphe à $\mathbb{Z}/13\mathbb{Z}$, puis que

$$|H \cap W| = 4.$$

Proposition de corrigé :

a) C'est quoi cette question ? ! Non, en vrai on comprends, en vrai on nous demande d'être astucieux. 6oko aurait prouver que A est diagonalisable, puis mis à la puissance 13 PDP^{-1}.

b) D'après a), $A^{-1} = -A^{12}$. Ainsi

$$A^{-1} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 0 & 0 \end{pmatrix} \in \mathrm{M}_3(\mathbb{F}_3)$$

Enfin, d'après a), $A^{26} = I_3$. Donc d'après la déf du min, ordre(A)|26. On les testes tous aucun convient sauf 26, voilà (c'est du calcul pour le lecteur assidue).

c) D'après les résultats précédents, G est monogène fini donc cyclique, il s'écrit en extension : G=$\{I_3, A, A^2, ..., A^{25}\}$. Donc G est évidemment
stable par produit, et on montre aisément que si B$\in G$, alors $\alpha B \in G \cup \{0\}$, où $\alpha \in \mathbb{F}_3$.
Et étant donné que I_3 est une puissance A, il suffit de prouver maintenant que :
$\forall \alpha, \beta, \gamma \in \mathbb{F}_3$, avec au plus un coeff.nul, $\alpha I_3 + \beta A + \gamma A^2 \in G$ (et là, pas plus d'idée que simplement tester toute les 12 combinaisons...mais, faites-le avec python). En faisant cela, on a $\mathrm{Vect}(I_3, A, A^2) \subset V$.

Mais aussi, la famille (I_3, A, A^2) est libre sur $\mathbb{F}_3$ (le lecteur le montrera), donc |Vect(I_3, A, A^2)|=3^3 =27=|V|.
Ainsi V=Vect(I_3, A, A^2)

d) Soit $M = \alpha I_3 + \beta A + \gamma A^2 \in G$, cherchons P=$aI_3+bA$ dans $W\setminus\{0\}$ telle que, PM=cI_3+dA.
Cela revient à résoudre le système :

$$\begin{cases} a \cdot \alpha = c \\ a \cdot \beta + b \cdot \alpha = d \\ (\beta + \gamma) \cdot b + a \cdot \gamma = 0 \end{cases}$$

Si $\beta + \gamma = 0$ alors a=c=0, et $b\alpha = d$. Donc on peut trouver une solution.
Si $\beta + \gamma \neq 0$, alors b=$\dfrac{-a\gamma}{\beta+\gamma}$ et on détermine alors a, et donc c.
En conclusion, on a toujours une solution au système. Donc la factorisation existe.

e) H est cyclique (en tant que sous-groupe du groupe cyclique G (voir exo 4, pour la preuve)), et de cardinal $\frac{26}{2}$=13. Donc $H \cong \mathbb{Z}/13\mathbb{Z}$. Puis en calculant les différents élements de H et de W, on trouve que $|H \cap W|$=4. C'est pas très long.

Exercice – L

(a) Montrer que toute rotation du plan complexe est composée de deux symétries orthogonales par rapport à des droites.

(b) Montrer que toute permutation d'un ensemble fini non vide X est produit de deux éléments d'ordre au plus 2 du groupe des permutations de X.

(c) Le résultat de la question précédente subsiste-t-il si X est infini ?

Proposition de corrigé :
(a)

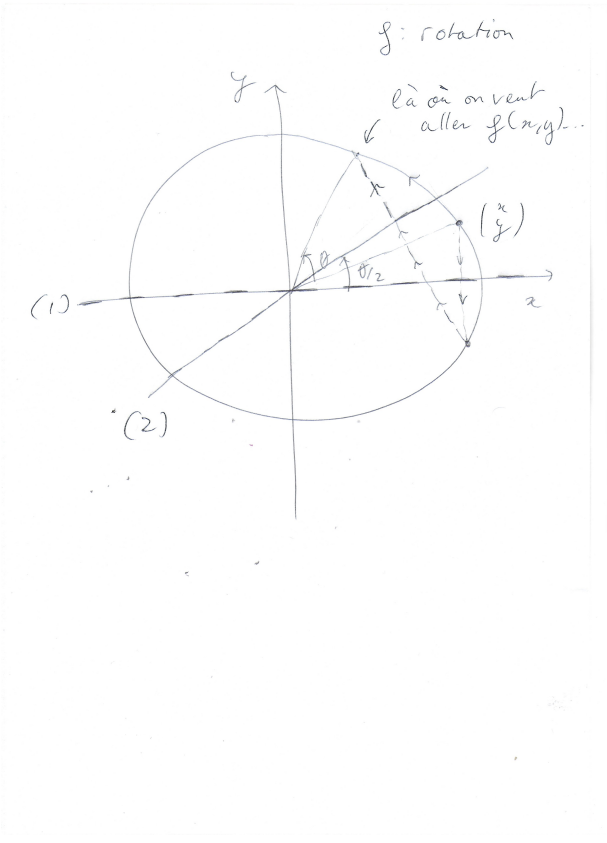

FIGURE 1 – Rotation comme composition de deux symétries orthogonales.

Le narrateur n'arrivait pas (a t-il essayé ?) à faire ce schéma en lateX. Maintenant, il va vous expliquer son idée :
En partant du point du cercle de l'axe réel, on peut écrire une rotation d'angle θ, comme la reflexion par rapport à la droite passant par l'origine d'angle $\dfrac{\theta}{2}$. Mais comment faire si le point est ailleurs sur le cercle ? Et en regardant bien, ce qu'on avait fait au point particulier

c'est deux refléxions, mais dont l'une était sur une droite sur lequel reposait le point (la droite des x). Et pour un autre point, pas sur la droite (voir schéma), la composée des symétries orthogonales par rapport à la droite des x et l'autre droite formant un angle de $\frac{\theta}{2}$ avec la droite des x, donne le bon résultat aussi. En Grèce Antique, ma preuve aurait été évidemment accepted. J'ai convaincu tout les grecs ici. Tout barbare osant m'envoyer un mail n'aura aucune réponse.
Plus sérieusement, je ne vois pas comment écrire cela matriciellement, je suis ouvert à une proposition, je suis toujours ouvert.

(b) Soit σ une permutation de X, on sait qu'elle s'écrit comme produit de cycles à **supports disjoints**. Il nous suffit alors de raisonner sur un cycle. Or un cycle $c = (c_0, c_1, ..., c_p)$ peut se représenter par les racines p-ième de l'unité (c'est un groupe cyclique).

Et en appliquant a), la rotation d'angle $\frac{2\pi}{p}$ s'écrit comme la composée de deux symétries orthogonales (d'ordre 2 maximium de fait). Ainsi, en retournant par bijetion sur c, c est le produit de deux élements d'ordre au plus 2 du groupe des permutation de X. Donc vue que les supports sont disjoints, on pourra regrouper les élements de telle sorte qu'on ait deux élements d'ordre 2, et ainsi σ est le produit de deux éléments d'ordre au plus 2 du groupe des permutations de X.

(c) Dans le cas infini, exemple $X = \mathbb{Z}$, il apparait des cycles infinis dans la décomposition d'une permutation de X. Le seul moyen, de recouvrir une partie infinie de $\mathbb{Z}$ par une involution, est de faire serpenter symétriquement l'involution sur une infinité d'élements (ex : n associe -n (symétrie autour de 0)) de $\mathbb{Z}$.
Maintenant, si l'on prend une permutation de type décalage de n en n+1, où n$\in \mathbb{Z}$, on ne peut trouver une telle décompositon car deux transformations symétriques ne peuvent pas donner un décalage de 1 sur tout élement de $\mathbb{Z}$
(avec les mains, désolé).

Exercice – L

Soit $(a_n) \in (\mathbb{R}^*)^{\mathbb{N}}$. On suppose qu'il existe $C > 0$ tel que

$$\forall n \in \mathbb{N}, \quad |a_n| \in \left[\frac{1}{C}, C\right].$$

Pour $n \in \mathbb{N}$, on pose

$$P_n(X) = \sum_{k=0}^{n} a_k X^k = a_n \prod_{k=1}^{n} (X - x_{k,n}),$$

où l'on a noté $x_{k,n}$ les racines complexes de P_n.

(a) Montrer que l'ensemble $\{x_{k,n}\,;\, n \in \mathbb{N}^*,\ k \in [\![1, n]\!]\}$ est borné.

(b) Montrer que

$$\sum_{k=1}^{n} x_{k,n}^2 = \frac{a_{n-1}^2 - 2a_{n-2}a_n}{a_n^2}, \quad \text{pour tout } n \geq 2.$$

(c) Montrer que, pour n suffisamment grand, P_n n'est pas scindé sur $\mathbb{R}$.

Proposition de corrigé :

(a) $\{x_{k,n}\,;\, n \in \mathbb{N}^*,\ k \in [\![1, n]\!]\} = Rac(P_n)$, si, il existe une racine x de P_n de

module arbitrairement grand, disons plus grand que 1, alors par inégalité triangulaire :
$|x|^n \leq \frac{1}{C}\sum_{k=0}^{n-1}|a_k||x|^k \leq \frac{1}{C}\sum_{k=0}^{n-1}C|x|^k \leq \sum_{k=0}^{n-1}|x|^k$

En divisant alors par $|x|^{n-1}$, on obtient : $|x| \leq \frac{1-\frac{1}{|x|^n}}{1-\frac{1}{|x|}}$.

Donc on peut majorer |x| par $\frac{1-(-1)}{1-\frac{1}{|x|}}$ (on rappele qu'on a pris une racine de module plus grand que 1). Donc $|x| \leq 3$. Donc dans tout les cas |x| est majoré.

(b) Raisonnons par récurrence sur n. L'initialisation ne semble pas triviale, faisons-là !

Initialisation n=2 : D'après les relations coefficients racines : $x_{1,2} + x_{2,2} = -\frac{a_1}{a_2}$
donc $x_{1,2}^2 + x_{2,2}^2 + 2x_{1,2}x_{2,2} = \frac{a_1^2}{a_2^2}$ Or, toujours d'après les relations coeffs-racines,
$x_{1,2} + x_{2,2} = \frac{a_0}{a_2}$. Donc $x_{1,2}^2 + x_{2,2}^2 = \frac{a_1^2}{a_2^2} - 2\frac{a_0}{a_2} = \frac{a_1^2 - 2a_0a_2}{a_2^2}$
Et bien finalement on a pas besoin de faire d'hérédité, si on copie-colle la preuve avec les relations coefficients-racines, on a le cas n>2.

(c) Si, par l'absurde, pour tout n entier P_n est scindé sur $\mathbb{R}$ alors pour tout entier n plus grand que 2, $\sum_{k=1}^{n} x_{k,n}^2 \leq K,\ K \in \mathbb{R}^{+*}$ et les $x_{k,n}$ sont tous réels. Par ailleurs le polynome $X^nP_n(1/X)$ est le polyôme "symetrique" de P, il admet pour racines les $(\frac{1}{x_{k,n}})_k$ donc il est scindé sur $\mathbb{R}$.
D'apres b), on a alors $\sum_{k=1}^{n}\frac{1}{x_{k,n}^2} = \frac{a_1^2 - 2a_2a_0}{a_0^2}$.
Donc d'apres Cauchy-Schwarz :
$n = \sum_{k=1}^{n} 1 \leq \sqrt{\sum_{k=1}^{n} x_{k,n}^2}\sqrt{\sum_{k=1}^{n}\frac{1}{x_{k,n}^2}} \leq \sqrt{\sum_{k=1}^{n} x_{k,n}^2}\frac{(C^2 - \frac{2}{C^2})^2}{C^{-4}}$.
Ce qui est absurde, car alors $\sqrt{\sum_{k=1}^{n} x_{k,n}^2}$ n'est plus bornée pour n assez grand
(Le narrateur n'a jamais mis aurant de temps pour résoudre un exercise...).

Exercice – ULSR

Soient $A, B, C \in \mathbb{C}[X]$ non tous constants et premiers entre eux deux à deux.

(a) On veut montrer que si $A + B = C$ alors :

$$\max(\deg(A), \deg(B), \deg(C)) \leq M(ABC) - 1$$

où $M(P)$ est le nombre de racines distinctes du polynôme P.
Si $P, Q \in \mathbb{C}[X]$, on note $W_{P,Q} = PQ' - P'Q$.

(i) Montrer que $W_{A,B} = W_{C,B} = W_{A,C} \neq 0$.

(ii) Montrer que :

$$\deg(A \wedge A') + \deg(B \wedge B') + \deg(C \wedge C') \leq \deg(W_{A,B}).$$

(iii) Conclure.

(b) Soit $d \in \mathbb{N}^*$. Donner un exemple de $(A, B, C) \in \mathbb{C}[X]^3$ avec $\deg(A) = d$ et pour lequel :

$$\max(\deg(A), \deg(B), \deg(C)) = M(ABC) - 1.$$

(c) Soient $A, B, C \in \mathbb{C}[X]$ premiers entre eux dans leur ensemble et tels que :

$$A^n + B^n = C^n$$

avec $n \in \mathbb{N}^*$. Montrer que $n \leq 2$. Montrer qu'il existe des solutions pour $n = 2$.

Proposition de corrigé :

(a) (i) On raisonne que sur A et B, car les autres combinaisons se déduisent par le même raisonnement. En effet, si par l'absurde, $W_{A,B} = A'B - B'A = 0$, alors vue que A' et B' sont non nuls alors PGCD(A,B) divise 0, donc $PGCD(A, B) = 0 \neq 1$, ce qui est absurde.

Enfin, $W_{A,B}$=AB'-A'B=A(C'-A')-A'(C-A)=AC'-A'C=$W_{A,C}$ et ainsi de suite...

(ii) $A \wedge A' \,|W_{A,B}$, $B \wedge B' \,|W_{A,B}$ et $C \wedge C' \,|W_{A,C} = W_{A,B}$ d'après (i).
Donc $A \wedge A' + B \wedge B' + C \wedge C' \,|W_{A,B}$
Donc $deg(A \wedge A') \leq deg(W_{A,B})$, $deg(B \wedge B') \leq deg(W_{A,B})$, et $deg(C \wedge C') \leq deg(W_{A,B})$
Or étant donné que A,B et C sont premiers entre eux, alors $A \wedge A', B \wedge B'$ et $C \wedge C'$ sont premiers entre eux.

Ainsi $\deg((A \wedge A').(B \wedge B').(C \wedge C')) = \deg(A \wedge A') + \deg(B \wedge B') + \deg(C \wedge C') \leq deg(W_{A,B})$
car $(A \wedge A').(B \wedge B').(C \wedge C')$ divise $W_{A,B}$.

(iii) $\deg(A \wedge A') = deg(A) - M(A)$, c'est de la mécanique les gars ! En effet :
$\deg(\gcd(A, A')) = \sum_{i=1}^{r}(m_i - 1) = (\sum_{i=1}^{r} m_i) - r = \deg(A) -$nombre de racines distinctes de A
en notant (m_i) la multiplicité des r racines de A.

Donc, $\deg(A \wedge A') + \deg(B \wedge B') + \deg(C \wedge C') \leq \deg(W_{A,B})$

$\Leftrightarrow deg(A) + deg(B) + deg(C) \leq M(A) + M(B) + M(C) + deg(W_{A,B})$
Or A,B et C sont premiers entre eux donc M(ABC)=M(A)+M(B)+M(C).
Donc, ici, $deg(A) + deg(B) + deg(C) \leq M(ABC) + deg(W_{A,B})$. Maintenant, sans perdre en généralité, en supposant que max(deg(A),deg(B),deg(C))=deg(A), on a :

$$\begin{aligned}\max(\deg(A),\deg(B),\deg(C)) &\leq M(ABC)-\deg(B)-\deg(C)+\deg(W_{B,C}) \ (car\ W_{B,C}=W_{A,B})\\ &\leq M(ABC)+\max(\deg(B'C),\deg(BC'))-\deg(B)-\deg(C)\\ &\leq M(ABC)+\max(\deg(B')+\deg(C),\deg(B)+\deg(C'))-\deg(B)-\deg(C)\\ &\leq M(ABC)+\max(\deg(B)-1+\deg(C),\deg(B)+\deg(C)-1)-\deg(B)-\deg(C)\\ &\leq M(ABC)-1\end{aligned}$$

(b) $A=X^d, B=-X, C=X^d-X$ (c)Si A, B et C sont tous constants, alors on utilise le **théorème de Fermat–Wiles** pour savoir que $n\leq 2$.
Puis, si $n=2$, on prend $A=3$, $B=4$, $C=5$ (triplet pythagoricien).
Sinon, d'après (a), on a :

$$\max\left(\deg(A^n),\deg(B^n),\deg(C^n)\right)\leq M(A^nB^nC^n)-1$$

Or $\deg(A^n)=n\deg(A)$, donc :

$$n\cdot\max(\deg(A),\deg(B),\deg(C))\leq M(A^n)+M(B^n)+M(C^n)-1$$

Car $A^n\wedge B^n\wedge C^n=1$, et :

$$\begin{aligned}M(A^n)+M(B^n)+M(C^n)-1 &= M(A)+M(B)+M(C)-1\\ &= M(ABC)-1\end{aligned}$$

Donc :

$$\begin{aligned}n\cdot\max(\deg(A),\deg(B),\deg(C)) &\leq M(ABC)-1\\ &\leq \deg(ABC)-1\\ &= \deg(A)+\deg(B)+\deg(C)-1\\ &\leq 3\cdot\max(\deg(A),\deg(B),\deg(C))-1\end{aligned}$$

i.e.

$$n-3\leq -1.$$

EXCELLENT, NEXT !

Exercice – U

Soient $P,Q\in\mathbb{R}[X]$ des polynômes unitaires. On dit que P et Q sont **entrelacés** lorsqu'entre deux racines consécutives de l'un (en tenant compte des multiplicités), il y a exactement une racine de l'autre.
On suppose que :

- $\deg(Q)=\deg(P)-1$,
- Q est scindé à racines simples sur $\mathbb{R}$,
- P et Q n'ont aucune racine commune.

On pose :

$$F=\frac{P}{Q},\qquad H=\{z\in\mathbb{C}\mid \Im(z)>0\}.$$

Montrer l'équivalence entre :

(i) P est scindé sur $\mathbb{R}$ et P et Q sont entrelacés.

(ii) $F(\mathbb{H})\subset\mathbb{H}$, c'est-à-dire : F envoie le demi-plan supérieur dans lui-même.