Exercice 1 - Différence d'arctangente (⋆⋆)

1. Démontrer que $\displaystyle\int_0^{+\infty} \arctan(t+1) - \arctan(t)\,dt$ est convergente.

Tout d'abord la fonction intégré étant continue sur $[0, +\infty[$ il n'y a pas de problème de définition en 0.

Pour $+\infty$ on utilise le théorème des accroissement finie. Soit donc $x \in \mathbb{R}_+$, comme arctan est continue et dérivable sur $]x, x+1[$ on en déduit qu'il existe $a \in]x, x+1[$ tel que $\arctan(x+1) - \arctan(x) = \frac{1}{1+a^2}$. Dès lors en multipliant par x^2 on obtient :

$$x^2\left[\arctan(x+1) - \arctan(x)\right] = \frac{x^2}{1+a^2} \leq \frac{x^2}{1+x^2} \leq 1$$

On en déduit alors que notre fonction est dominé par $t \mapsto \frac{1}{t^2}$ qui est intégrable, donc elle est intégrable.

2. Déterminer la limite de $\displaystyle\int_x^{x+1} \arctan(t)\,dt$ quand x tend vers $+\infty$.

Soit $x \in \mathbb{R}$, on remarque que la fonction arctan est croissante et on en déduit pour $t \in [x, x+1]$ l'encadrement :

$$\arctan(x) \leq \arctan(t) \leq \arctan(x+1)$$

Puis en intégrant sur $[x, x+1]$ on obtient :

$$\arctan(x) \leq \int_x^{x+1} \arctan(t)\,dt \leq \arctan(x+1)$$

On conclut en invoquant le théorème d'encadrement, ce qui permet d'affirmer que $\lim\limits_{x\to+\infty} \displaystyle\int_x^{x+1} \arctan(t)\,dt = \frac{\pi}{2}$.

3. En déduire la valeur de $\displaystyle\int_0^{+\infty} \arctan(t+1) - \arctan(t)\,dt$.

On raisonne dans un premier temps à l'aide d'une borne, soit donc $x \in \mathbb{R}$ on a :

$$\begin{aligned}
\int_0^x \arctan(t+1) - \arctan(t)\,dt &= \int_0^x \arctan(t+1)\,dt - \int_0^x \arctan(t)\,dt \\
&= \int_1^{x+1} \arctan(t)\,dt - \int_0^x \arctan(t)\,dt \\
&= -\int_0^1 \arctan(t)\,dt + \int_x^{x+1} \arctan(t)\,dt \\
&= \left[t\arctan(t)\right]_1^0 - \int_1^0 \frac{t}{1+t^2}dt + \int_x^{x+1} \arctan(t)\,dt \\
&= -\frac{\pi}{4} + \left[\frac{1}{2}\ln\left(1+t^2\right)\right] + \int_x^{x+1} \arctan(t)\,dt \\
&= -\frac{\pi}{4} + \ln\left(\sqrt{2}\right) + \int_x^{x+1} \arctan(t)\,dt
\end{aligned}$$

D'après la première question le terme de gauche converge, et pour le terme à droite il s'agit de la question précédente. Finalement on obtient :

$$\int_0^{+\infty} \arctan(t+1) - \arctan(t)\, dt = -\frac{\pi}{4} + \ln\left(\sqrt{2}\right) + \frac{\pi}{2} = \frac{\pi}{4} + \ln\left(\sqrt{2}\right)$$

Exercice 2 - Changements de variables $(\star)$

1. Montrer que pour $a > 0$ l'intégrale $\displaystyle\int_0^{+\infty} \frac{\ln(t)}{a^2+t^2} dt$ est convergente.

Tout d'abord la fonction $t \mapsto \frac{\ln(t)}{a^2+t^2}$ est continue sur $]0, +\infty[$, et au voisinage de 0 on a :

$$\frac{\ln(t)}{a^2+t^2} \underset{t\to 0}{\sim} \frac{\ln(t)}{a}$$

Or la fonction ln est intégrable en 0. De même on remarque que :

$$t^{\frac{3}{2}} \times \frac{\ln(t)}{a^2+t^2} = \frac{\ln(t)}{\sqrt{t}\left(\frac{a^2}{t^2}+1\right)} \underset{t\to+\infty}{\longrightarrow} 0$$

On en déduit alors que $\displaystyle\frac{\ln(t)}{a^2+t^2} = o\left(\frac{1}{t^{\frac{3}{2}}}\right)$, ce qui assure la convergence en $+\infty$.

2. En effectuant le changement de variable $u = \frac{1}{t}$, calculer $\displaystyle\int_0^{+\infty} \frac{\ln(t)}{1+t^2} dt$.

Soient $B \geq A > 0$ on effectue le changement de variable sur $[A, B]$, on obtient :

$$\begin{aligned}
\int_A^B \frac{\ln(t)}{1+t^2} dt &= \int_{\frac{1}{A}}^{\frac{1}{B}} \frac{\ln\left(\frac{1}{u}\right)}{1+\left(\frac{1}{u}\right)^2} \times \left(-\frac{1}{u^2}\right) du \\
&= \int_{\frac{1}{B}}^{\frac{1}{A}} \frac{\ln\left(\frac{1}{u}\right)}{u^2+1} du \\
&= -\int_{\frac{1}{B}}^{\frac{1}{A}} \frac{\ln(u)}{u^2+1} du
\end{aligned}$$

Comme on a montrer la converge à la première question, on en déduit par passage à la limite que :

$$\int_0^{+\infty} \frac{\ln(t)}{1+t^2} dt = -\int_0^{+\infty} \frac{\ln(t)}{1+t^2} dt \Longrightarrow \int_0^{+\infty} \frac{\ln(t)}{1+t^2} dt = 0$$

3. En déduire la valeur de $\displaystyle\int_0^{+\infty} \frac{\ln(t)}{a+t^2} dt$.

On effectue le changement de variable $t = au$ et l'on obtient :

$$\begin{aligned}\int_0^{+\infty} \frac{\ln(t)}{a^2+t^2}dt &= \int_0^{+\infty} \frac{\ln(au)}{a^2+a^2u^2}adu \\ &= \int_0^{+\infty} \frac{\ln(a)}{a\left(1+u^2\right)}du + \int_0^{+\infty} \frac{\ln(t)}{a\left(1+u^2\right)}du \\ &= \frac{\ln(a)}{a} \times \left[\arctan(u)\right]_0^{+\infty} + \frac{1}{a} \times 0 \\ &= \frac{\pi \ln(a)}{2a}\end{aligned}$$

Exercice 3 - Anneaux des décimaux ($\star\star$)

Soit $\mathbb{D}$ l'ensemble des nombres décimaux :

$$\mathbb{D} = \left\{ \frac{n}{10^k} /\ n \in \mathbb{Z},\ k \in \mathbb{N} \right\}$$

Démontrer que $(\mathbb{D}, +, \times)$ est un anneau et déterminer ses éléments inversibles.

On va prouver que $\mathbb{D}$ est un sous-anneau de $\mathbb{Q}$, tout d'abord $\mathbb{D} \subset \mathbb{Q}$ et $1 \in \mathbb{D}$. De plus soient $x = \frac{n}{10^k}$ et $y = \frac{m}{10^l}$ deux éléments de $\mathbb{D}$ alors :

$$x - y = \frac{10^l n - 10^k m}{10^{k+l}} \text{ et } xy = \frac{nm}{10^{k+l}}$$

Sont clairement des éléments de $\mathbb{D}$ qui est alors bien un sous-anneau de $\mathbb{Q}$, et donc lui-même un anneau.

Déterminons à présent les éléments inversibles de $\mathbb{D}$, pour cela on procède par analyse en considérant $x = \frac{n}{10^k}$ inversible d'inverse $y = \frac{m}{10^l}$ on obtient la condition :

$$nm = 10^{k+l}$$

On en déduit que les seuls diviseurs de n et m sont 2 et 5, autrement dit $n = \pm 2^p 5^q$. Réciproquement soit $x = \frac{\pm 2^p 5^q}{10^k}$, et posons $y = \frac{\pm 10^k}{2^p 5^q}$, il suffit alors de montrer que $y \in \mathbb{D}$ mais on a :

$$y = \frac{\pm 10^k}{2^p 5^q} = \frac{\pm 10^k 2^q 5^p}{2^{p+q} 5^{p+q}} = \frac{\pm 10^k 2^q 5^p}{10^{p+q}} \in \mathbb{D}$$

Finalement les éléments inversibles de $\mathbb{D}$ sont ceux de la forme $\frac{\pm 2^p 5^q}{10^k}$.

Exercice 4 - Anneau $\mathbb{Z}\left[\sqrt{2}\right)$ ($\star\star\star$)

On note $\mathbb{Z}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} /\ (a,b) \in \mathbb{Z}^2\right\}$.

1. Montrer que $\left(\mathbb{Z}\left[\sqrt{2}\right], +, \times\right)$ est un anneau commutatif.

On va montrer que c'est un sous-anneau de $(\mathbb{R}, +, \times)$. Mais $\mathbb{Z}\left[\sqrt{2}\right]$ est :

— stable par la loi + : $\left(a + b\sqrt{2}\right) + \left(a' + b'\sqrt{2}\right) = (a + a') + (b + b')\sqrt{2}$.

— stable pa la loi $\times$: $\left(a + b\sqrt{2}\right) \times \left(a' + b'\sqrt{2}\right) = (aa' + 2bb') + (ab' + a'b)\sqrt{2}$.

— stable par passage à l'opposé : $-\left(a + b\sqrt{2}\right) = -a + (-b)\sqrt{2}$.

De plus $1 \in \mathbb{Z}\left[\sqrt{2}\right]$, ainsi $\mathbb{Z}\left[\sqrt{2}\right]$ est bien un anneau et il est commutatif au vu de la formule du produit.

2. On note $N\left(a + b\sqrt{2}\right) = a^2 - 2b^2$. Montrer que pour tout $x, y \in \mathbb{Z}\left[\sqrt{2}\right]$ on a $N(xy) = N(x)\,N(y)$.

Si $x = a + b\sqrt{2}$ on remarque que $N(x) = \left(a + b\sqrt{2}\right)\left(a - b\sqrt{2}\right)$, on note alors $\overline{x} = a - b\sqrt{2} \in \mathbb{Z}\left[\sqrt{2}\right]$ la quantité conjugué de x. On a dès lors :

$$\begin{aligned} N(xy) &= (xy)\,\overline{(xy)} \\ &= xy\overline{x}\,\overline{y} \\ &= x\overline{x}y\overline{y} \\ &= N(x)\,N(y) \end{aligned}$$

D'où le résultat.

3. En déduire que $x \in \mathbb{Z}\left[\sqrt{2}\right]$ est inversible si, et seulement si, $N(x) = \pm 1$.

Si x est inversible on a :

$$N(x) \times N\left(x^{-1}\right) = N\left(xx^{-1}\right) = N(1) = 1$$

Or $N(x)$ et $N\left(x^{-1}\right)$ sont des entiers, dès lors $N(x) = \pm 1$. Réciproquement si $N(x) = \pm 1$, en notant $x = a + b\sqrt{2}$ on a dans $\mathbb{R}$:

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \pm\left(a - b\sqrt{2}\right) \in \mathbb{Z}\left[\sqrt{2}\right]$$

ce qui montre que $x = a + b\sqrt{2}$ est inversible dans $\mathbb{Z}\left[\sqrt{2}\right]$

Exercice 5 - Produit et Somme d'Idéaux ($\star\star$)

Soit $(A, +, \times)$ un anneau commutatif. Si I et J sont deux idéaux de A, on note

$$\begin{aligned} I + J &= \{i + j /\ i \in I,\ j \in J\} \\ I.J &= \{i_1 j_1 + \cdots + i_n j_n /\ n \geq 1,\ \forall k \in [\![1, n]\!],\ i_k \in I,\ j_k \in J\} \end{aligned}$$

1. Montrer que $I + J$ et $I.J$ sont encore des idéaux de A.

Soit $a \in A$ on a pour $i + j \in I + J$ par distributivité de la multiplication sur la somme $a\,(i + j) = ai + aj$ or I et J étant des idéaux on en déduit que $ai \in I$ et $aj \in J$ donc $a\,(i + j) \in I + J$.

De plus on a :

$$a\left(\sum_{k=1}^{n} i_k j_k\right) = \sum_{k=0}^{n} (ai_k)\, j_k$$

Or $ai_k \in I$ et donc $I.J$ est aussi un idéal.

2. Montrer que $I.J \subset I \cap J$.

soit $x = \sum_{k=0}^{n} i_k j_k \in I.J$ comme I est un idéal $i_k j_k \in I$ et donc par somme $x \in I$ de même on montre que $x \in J$ d'où $x \in I \cap J$.

3. Montrer que $(I + J)\,.\,(I \cap J) \subset I.J$.

Soit $x \in (I + J)\,.\,(I \cap J)$ alors :

$$x = \sum_{k=0}^{n} a_k b_k$$

Avec $a_k \in I+J$ et $b_k \in I \cap J$. dès lors on peut écrire $a_k = i_k + j_k$ et on a :

$$x = \sum_{k=0}^{n} i_k b_k + j_k b_k$$

Il s'agit bien d'un élément de $I.J$ car $i_k \in I$ et $b_k \in J$ mais aussi $b_k \in I$ et $j_k \in J$ d'où le résultat.

4. Si I et J sont étranger (*i.e* $I+J=A$) montrer que $I.J = I \cap J$.

D'après ce qui précède on a $I.J \subset I \cap J$. Réciproquement comme $A.(I \cap J) \subset I.J$ on a pour $x \in I \cap J,\ x = 1_A \times x \in A.(I \cap J) \subset I.J$ d'où l'inclusion réciproque et l'égalité.

Exercice 6 - Radical d'un idéal ($\star\star\star$)

Soit A un anneau commutatif unitaire. SI I est un idéal de A, on appelle radical de I l'ensemble :

$$\sqrt{I} = \{x \in A/\ \exists n \in \mathbb{N}^*,\ x^n \in I\}$$

1. Montrer que $\sqrt{I}$ est un idéal de A.

Montrons qu'il s'agit dans un premier temps bien d'un groupe. Comme pour $n=1$ on a $I \subset \sqrt{I}$ on en déduit que $0 \in \sqrt{I}$. De plus si $x \in \sqrt{I}$ alors pour soit $n \in \mathbb{N}^*,\ x^n \in I$, on a $(-x)^n = (-1)^n \times x^n \in I$ car I est un idéal. Enfin pour $y \in \sqrt{I}$ on considère alors $m \in \mathbb{N}^*$ tel que $y^m \in I$ dès lors on a :

$$(x+y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k \times y^{n+m-k}$$

Si $k < n$ alors $n+m-k \geq m$ et donc $y^{n+m-k} \in I$, sinon de façon immédiate $x^k \in I$ ainsi chaque terme de la somme est le produit d'un élément de I avec un élément de A, cette somme est donc un élément de I et on peut alors affirmer que $x+y \in \sqrt{I}$.

Pour montrer qu'il s'agit alors bien d'un idéal on considère $a \in A$ on a $(ax)^n = a^n \times x^n \in I$ d'où $ax \in \sqrt{I}$, il s'agit donc bien d'un idéal.

2. Montrer que l'on a $\sqrt{\sqrt{I}} = \sqrt{I}$

Comme on a remarquer que $I \subset \sqrt{I}$ et que d'après la question précédente $\sqrt{I}$ est un idéal on a déjà $\sqrt{I} \subset \sqrt{\sqrt{I}}$. Réciproquement si $x \in \sqrt{\sqrt{I}}$ alors il existe $n \in \mathbb{N}^*$ tel que $x^n \in \sqrt{I}$ et donc il existe $m \in \mathbb{N}^*$ tel que $(x^n)^m = x^{nm} \in I$ donc $x \in \sqrt{I}$, d'où l'inclusion réciproque.

3. Soient I et J deux idéaux de A, montrer que :

$$\sqrt{I.J} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$$

SI $x \in \sqrt{I.J}$ il existe $n \in \mathbb{N}^*$ tel que $x^n \in I.J$ ainsi il existe $(a_k, b_k) \in I \times J$ tel que :

$$x^n = \sum_{k=0}^{m} a_k b_k$$

Ainsi $x^n \in I$ car I est un idéal, mais aussi $x^n \in J$ ainsi $x^n \in I \cap J$ et donc $x \in \sqrt{I \cap J}$.

Soit à présent $x \in \sqrt{I \cap J}$ alors il existe $n \in \mathbb{N}^*$ tel que $x^n \in I \cap J$ ainsi $x^n \in I$ d'où $x \in \sqrt{I}$ et de même $x \in \sqrt{J}$ d'où $x \in \sqrt{I} \cap \sqrt{J}$.

Soit finalement $x \in \sqrt{I} \cap \sqrt{J}$, il existe $n, m \in \mathbb{N}^*$ tels que $x^n \in I$ et $x^m \in J$ ainsi $x^{n+m} = x^n \times x^m \in I.J$ donc $x \in \sqrt{I.J}$. D'où les trois égalités.

Exercice 7 - Involution (⋆⋆)

Soit G un groupe fini tel que pour tout x de G on ai $x^2 = e$.

1. Montrer que G est commutatif.

Soient $x, y \in G$ on a :

$$(xy)^2 = xyxy = e \qquad x^2 = e \qquad y^2 = e$$

Et donc $x\,(xy)^2\,y = x^2yxy^2 = yx$ mais aussi $x\,(xy)^2\,y = xy$ d'où la commutativité !

2. Soit H est un sous-groupe de G et $x \notin H$, déterminer le cardinal du sous-groupe engendré par H et x.

Il suffit de remarque que $xH \cap H = \varnothing$ en effet dans le cas contraire on obtient immédiatement que $x \in H$. Dès lors $|H \cup xH| = |H| + |xH|$. Mais comme nous sommes dans un groupe, l'application $h \mapsto xh$ de H dans xH est bijective, en particulier elle préserve le cardinal ainsi $|H \cup xH| = 2\,|H|$

3. En déduire que $|G|$ est une puissance de 2.

On pose $H_1 = \{e\} \subset G$ il s'agit d'un sous-groupe de G, si $G = H_1$ alors $|G| = 1 = 2^0$, sinon on peut considérer $x_1 \notin H_1$, et l'on pose $H_2 = H_1 \cup x_1H_1$ d'après ce qui précède H_2 et de cardinal 2, soit $H_2 = G$ au quel cas on a le résultat, soit $H_2 \neq G$ et dans ce cas on recommence en considérant $x_2 \notin H_2$. Enfin comme G est de cardinal fini, on peut affirmer que par récurrence fini $|G|$ est une puissance de 2.

4. <u>Bonus :</u> En déduire que dans un groupe d'ordre $2p$, avec p un nombre premier impair, il existe un élément d'ordre p.

Soit $x \in G$, où G est un groupe d'ordre $2p$ comme dans l'énoncé. On sait d'après le théorème de Lagrange que l'ordre de x divise $2p$, ainsi son ordre peut être $1, 2, p$ ou $2p$.

- Comme G est de cardinale $2p$ on peut choisir $x \neq e$ et donc x n'est pas d'ordre 1.
- Si x est d'ordre p on a le résultat.
- Si x est d'ordre p alors x^2 est d'ordre p d'où le résultat.
- Mais x peut être d'ordre 2, en revanche d'après ce qui précède, si tous les éléments de G étaient d'ordre 2 *i.e* $x^2 = e$, alors $|G| = 2p$ serait une puissance de 2 ce qui n'est pas le cas. Ainsi on est assuré qu'il existe $x \in G$ tel que $x \neq e$ et x n'est pas d'ordre 2, d'où le résultat.

Exercice 8 - Commutatif (⋆⋆)

Montrer que tout groupe de cardinal au plus 5 est commutatif.

On procède par analyse en supposant que G est un groupe fini non-commutatif. Ainsi il existe $x, y \in G^2$, $xy \neq yx$, on suppose alors que $xy \in \{x, y, e\}$.

- Si $xy = e$ alors $xyx = x$ et donc $xyxy = xy$ et en simplifiant on trouve $yx = e$.

— Si $xy = x$ alors $y = e$ et donc $yx = x = xy$.

— le raisonnement s'applique si $xy = y$.

On en déduit que $xy \notin \{x, y, e\}$ et de même on trouve que $yx \notin \{x, y, e\}$, dès lors $|G| \geq 5$.

Si $|G| = 5$ soit $x \in G,\ x \neq e$ par le théorème de Lagrange on sait que l'ordre de x divise 5 et comme $x \neq e$ on en déduit que l'ordre de x est 5. Ainsi G est cyclique (engendré par x) et donc abélien (commutatif).

Exercice 9 - Carré de $\mathbb{Z}/n\mathbb{Z}$ (⋆⋆⋆)

On s'intéresse au nombre de solutions de l'équation $x^2 = 1$ dans $\mathbb{Z}/n\mathbb{Z}$, où $n \geq 2$.

1. Quel est le nombre de solutions lorsque $n = p^\alpha$ avec p un nombre premier impair et $\alpha \geq 1$?

De façon immédiate, 1 et -1 sont deux solutions distinctes. D'autre part si m est un entier solution en notant x sa classe dans $\mathbb{Z}/p^\alpha\mathbb{Z}$, on a $x^2 = 1 \iff x^2 - 1 = 0$ ainsi $p^\alpha | (m-1)(m+1)$ ainsi il existe $k, l \in \mathbb{Z}$ ainsi que $u, v \in \mathbb{Z}$ tel que :

$$m - 1 = kp^u \qquad m + 1 = lp^v$$

Avec $u + v \geq \alpha$ et k, l premier avec p dès lors par différence on trouve :

$$2 = lp^v - kp^u$$

Si $u \neq 0$ et $v \neq 0$ alors $p | lp^v - kp^u$ ce qui implique que p divise 2 ce qui est absurde. Ainsi $u = 0$ ou $v = 0$, sans perte de généralité si $u = 0$ on a $v \geq \alpha$ et donc $x = -1$. En supposant $v = 0$ on trouve $x = 1$. Finalement il n'y a que deux solutions.

2. Quel est le nombre de solutions pour $n = 2, 4$?

Une étude exhaustive montre que pour $n = 2$ il n'y a qu'une solution, alors que pour $n = 4$ il y en a 2 à savoir 1 et -1.

3. On admet que si $n = 2^\alpha$ avec $\alpha \geq 3$ il y a exactement 4 solutions distinctes. En déduire le nombre de solutions dans le cas général.

On note $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ avec $p_1 = 2$ d'après le théorème chinois on a :

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}$$

Et de plus l'isomorphisme est donné par $x \mapsto (x_1, \dots, x_r)$ où x_i désigne la classe de x modulo $p_i^{\alpha_i}$. Dès lors on remarque que l'application carré commute avec l'application précédente, ainsi $x^2 = 1$ si, et seulement si, $x_i^2 = 1$ pour tout $i \in [\![1, r]\!]$. Finalement il y a :

— 2^{r-1} solutions si $\alpha_1 = 0, 1$

— 2^r solutions si $\alpha_1 = 2$

— 2^{r+1} solutions si $\alpha_1 \geq 3$.

Exercice 10 - Théorème $\frac{5}{8}$ (⋆⋆)

Soit G un groupe finis non-commutatif, on considère X et Y deux variables aléatoire suivant la loi uniforme sur G. Démontrer que $\mathbb{P}(XY = YX) \leq \frac{5}{8}$, et interpréter ce résultat.

Commençons par écrire simplement cette probabilité à l'aide de la formule des probabilités totales on obtient :

$$\mathbb{P}(XY = YX) = \frac{1}{|G|^2} \sum_{(x,y)\in G^2} \begin{cases} 1 \text{ si } xy = yx \\ 0 \text{ sinon.} \end{cases}$$

Pour $x \in G$ on note alors C_x l'ensemble des éléments qui commute avec x. On note également $Z(G)$ le *centre* de G, c'est-à-dire, l'ensemble des éléments de G qui commute avec tous les éléments de G. Il est assez facile de montrer que $\forall x \in G,\ C_x$ est un sous-groupe de G. De plus on remarque que l'on a :

$$\begin{aligned} \frac{1}{|G|^2} \sum_{(x,y)\in G^2} \begin{cases} 1 \text{ si } xy = yx \\ 0 \text{ sinon.} \end{cases} &= \frac{1}{|G|^2} \sum_{x\in G} \sum_{y\in G} \begin{cases} 1 \text{ si } xy = yx \\ 0 \text{ sinon.} \end{cases} \\ &= \frac{1}{|G|^2} \sum_{x\in G} |C_x| \end{aligned}$$

Or on remarque que si $x \in Z(G)$ alors $C_x = G$, car par définition x commute avec tous les éléments de G. Et si $x \in G \setminus Z(G)$ alors d'une part $C_x \neq G$ et d'autre part $|C_x|$ divise $|G|$, dès lors on peut en déduire que $|C_x| \leq \frac{1}{2}|G|$ on en déduit alors :

$$\begin{aligned} \mathbb{P}(XY = YX) &= \frac{1}{|G|^2} \sum_{x\in G} |C_x| \\ &= \frac{1}{|G|^2} \left(\sum_{x\in Z(G)} |C_x| + \sum_{x\in G\setminus Z(G)} |C_x| \right) \\ &\leq \frac{1}{|G|^2} \left(\sum_{x\in Z(G)} |G| + \sum_{x\in G\setminus Z(G)} \frac{1}{2}|G| \right) \\ &\leq \frac{1}{|G|^2} \left(|Z(G)| \times |G| + |G \setminus Z(G)| \times \frac{1}{2}|G| \right) \\ &\leq \frac{1}{|G|^2} \left(|Z(G)| \times |G| + (|G| - |Z(G)|) \times \frac{1}{2}|G| \right) \\ &\leq \frac{1}{|G|} \left(|Z(G)| + \frac{1}{2}(|G| - |Z(G)|) \right) \\ &\leq \frac{1}{|G|} \left(\frac{1}{2}|Z(G)| + \frac{1}{2}|G| \right) \\ &\leq \frac{1}{2} + \frac{1}{2} \times \frac{|Z(G)|}{|G|} \end{aligned}$$

Afin de conclure il ne reste alors plus qu'à montrer que $|Z(G)| \leq \frac{1}{4}|G|$, or comme G est non commutatif, il existe $x \in G \setminus Z(G)$, dès lors on a :

$$Z(G) \subset C_x \subset G$$

De plus on remarque chacune des inclusions précédente, en effet $x \in G \setminus Z(G)$ implique que $C_x \neq Z(G)$, mais aussi $C_x \neq G$ comme on l'a vu précédemment. Enfin comme $Z(G) \subset C_x$ on peut affirmer qu'il s'agit en fait d'un sous-groupe de C_x, dès lors on en déduit d'après le théorème de Lagrange que :

$$|Z(G)| \leq \frac{1}{2}|C_x| \leq \frac{1}{4}|G|$$

D'où le résultat.