

DM09
Pour le lundi 08/01
ou avant, via cahier-de-prépa (cf. mail de vacances)

Formules possibles.

1. Formule 1, « bases » : faire le problème 1, bonne révision de ce chapitre d'algèbre (2h30)
2. Formule 2, « plus avancée en algèbre » : faire le problème 1 et le problème 2, plus dur que le précédent (5h)
3. Formule 3, « je n'ai pas fait assez d'analyse » : faire le problème 1 et le problème 3, qui mélange un peu d'algèbre et de l'analyse (4h30)
4. Formule 4, complète : faire les problèmes 1, 2 et 3

Précisez en début de DM la formule choisie. Je ne corrigerai que les exercices associés à la formule choisie.

Problème 1. Ordre d'un élément dans un groupe

Notations. Soit (G, \star) un groupe. On note e son élément neutre. On note, pour tout x dans G , x^{-1} l'inverse de x pour la loi \star . On rappelle que l'on note, pour tout x dans G et pour tout n dans \mathbb{N}^* ,

$$x^n = \underbrace{x \star x \star \dots \star x}_{n \text{ fois}} \text{ et } x^{-n} = \underbrace{x^{-1} \star x^{-1} \star \dots \star x^{-1}}_{n \text{ fois}}.$$

Par convention, $x^0 = e$. On rappelle que toutes les règles de calcul usuel sur les puissances s'appliquent ici. Pour tous m et n dans \mathbb{Z} , pour tout x dans G : $x^m x^n = x^{m+n}$, $(x^{-1})^m = x^{-m}$, $(x^m)^n = x^{mn}$. En particulier, pour tout x dans G et n dans \mathbb{Z} , x^n est inversible d'inverse x^{-n} .

Définitions. Soit x un élément de G . On dit que x **admet un ordre fini** s'il existe un entier naturel **non nul** n tel que $x^n = e$. On note alors \mathcal{P}_x l'ensemble $\mathcal{P}_x = \{k \in \mathbb{N}^*, x^k = e\}$.

Si x admet un ordre fini, on nomme **ordre de** x et on note $\omega(x)$ la quantité $\omega(x) = \min(\mathcal{P}_x)$.

On rappelle que si G est un ensemble fini, on appelle **cardinal** de G le nombre d'éléments de G , et on le note $|G|$.

Un résultat à utiliser. On n'hésitera pas à utiliser l'argument suivant (et on pourra le nommer « principe des tiroirs » lorsqu'on l'utilise) : si E est un ensemble à n éléments ($n \in \mathbb{N}^*$) et si x_1, \dots, x_{n+1} sont $n+1$ éléments de E , alors il existe $(i, j) \in \llbracket 1, n+1 \rrbracket^2$ tels que $i \neq j$ et $x_i = x_j$.

A. Premières manipulations

1. Soit x dans G tel que x admet un ordre fini. Justifier l'existence de $\omega(x)$.

Correction

On a supposé que x admettait un ordre fini, donc on dispose de n dans \mathbb{N}^* tel que $x^n = e$. La partie \mathcal{P}_x est donc une partie non vide de

\mathbb{N} , elle admet donc un plus petit élément, non nul car appartenant à \mathbb{N}^* . Donc $\omega(x)$ existe.

2. Démontrer que si (G, \star) est **fini**, alors tout élément de G admet un ordre.
On pourra considérer, si n est le cardinal de G et $x \in G$, x^0, x^1, \dots, x^n , et utiliser le principe des tiroirs.

Correction

Soit n le cardinal de G et x dans G . Alors x^0, \dots, x^n sont $n+1$ éléments de G donc, d'après le principe des tiroirs, on dispose de i et j dans $\llbracket 0, n \rrbracket$ tels que $i \neq j$ et $x^i = x^j$. Si l'on suppose $i < j$, on en déduit que $x^{j-i} = e$, donc $j-i \in \mathcal{P}_x$. Donc x admet un ordre.

3. Soit x dans G . Démontrer que si x est d'ordre p dans G (où $p \in \mathbb{N}^*$), alors x^0, \dots, x^{p-1} sont deux à deux distincts. *On raisonnera par l'absurde et on contredira la minimalité de p .*

Correction

Supposons qu'il existe i et j dans $\llbracket 0, p-1 \rrbracket$ tels que $x^i = x^j$. Sans perte de généralité, on peut supposer que $i < j$. Alors $x^{j-i} = e$, avec $j-i > 0$ et $j-i < p$, ce qui contredit la minimalité de p . Donc les éléments x^0, \dots, x^{p-1} sont deux à deux distincts.

4. Dans cette question, on suppose que tous les éléments de G différents de e sont d'ordre 2. Exprimer, pour tout x dans G , l'inverse de x en fonction de x , et en déduire que G est abélien.

Correction

Soit x dans G . Alors $x^2 = e$, donc $x \star x = e$, donc $x^{-1} = x$.

Soient alors x et y dans G . Alors, comme tout élément est égal à son inverse,

$$x \star y = (x \star y)^{-1} = y^{-1} \star x^{-1} = y \star x,$$

donc G est abélien.

B. Théorème de Lagrange faible

5. **Un Lemme préliminaire.** Démontrer le lemme préliminaire suivant :

$$\text{Si } x \text{ est dans } G, \text{ si } n \in \mathbb{N}^* \text{ et } x^n = e, \text{ alors } \omega(x) \text{ divise } n. \quad (1)$$

On pourra effectuer la division euclidienne de n par $\omega(x)$.

Correction

Soit x dans G et n dans \mathbb{N}^* tel que $x^n = e$. Effectuons la division euclidienne de n par $\omega(x)$: $n = \omega(x)q + r$, avec $0 \leq r < \omega(x)$. Si on avait $r \neq 0$, alors on aurait

$$x^n = x^{\omega(x)q+r} = (x^{\omega(x)})^q x^r = e^q x^r = x^r,$$

donc r serait dans \mathcal{P}_x et $r < \omega(x)$, absurde ! Donc $r = 0$, donc $\omega(x)$ divise n .

Dans cette partie, on va démontrer le résultat suivant :

Si G est fini et de cardinal n , alors pour tout x dans G , $\omega(x)$ divise n . (2)

On ne prouve ce résultat que dans le cas suivant : on suppose G **abélien**, c'est-à-dire commutatif.

Soit x dans G . On définit l'application φ :

$$\varphi : \begin{cases} G \rightarrow G \\ y \mapsto x * y \end{cases}$$

6. Démontrer que φ est une bijection de G dans G .

Correction

Soit z dans G , y dans G . Alors

$$\varphi(y) = z \Leftrightarrow x * y = z \Leftrightarrow y = x^{-1} * z,$$

donc $\forall z \in G, \exists ! y \in G, \varphi(y) = z$. Donc φ est bijective, de bijection réciproque

$$y \mapsto x^{-1} * y.$$

7. En calculant de deux manières différentes $\prod_{y \in G} \varphi(y)$, démontrer que $x^n = e$ et en déduire que $\omega(x)$ divise n .

Correction

Déjà, comme φ est une bijection de G dans G , et **comme G est abélien**, $\prod_{y \in G} \varphi(y) =$

$$\prod_{y \in G} y.$$

Ensuite,

$$\prod_{y \in G} \varphi(y) = \prod_{y \in G} (x * y) = x^n \prod_{y \in G} y \text{ car } G \text{ est abélien}$$

Donc $x^n \prod_{y \in G} y = \prod_{y \in G} y$, donc $x^n = e$.

On en déduit, par le lemme (1), que $\omega(x)$ divise n .

C. Un exemple dans \mathcal{S}_n . – PARTIE SUPPRIMÉE !

Soit n un entier naturel supérieur ou égal à 2. Soit p dans $\llbracket 2, n \rrbracket$.

8. Définir ce qu'est un p -cycle, et donner, en justifiant brièvement, l'ordre d'un p -cycle.

Correction

Un p -cycle est une permutation ρ telle qu'il existe p entiers i_1, i_2, \dots, i_p tels que

$$\rho(i_1) = i_2, \rho(i_2) = i_3, \dots, \rho(i_{p-1}) = i_p \text{ et } \rho(i_p) = i_1,$$

et $\forall x \notin \{i_1, \dots, i_p\}, \rho(x) = x$.

L'ordre d'un p -cycle est p : $\rho^p = \text{Id}$ et si $k < p, \rho^k(i_1) = i_{k+1} \neq i_1$, donc $\rho^k \neq \text{Id}_{\llbracket 1, n \rrbracket}$.

9. Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 4 & 9 & 6 & 5 & 2 & 8 & 1 \end{pmatrix}$.

(a) Donner la décomposition en produit de cycles à supports disjoints, une décomposition en produit de transpositions, et la signature de σ .

Correction

La décomposition en produit de cycles à supports disjoints de σ est :

$$\sigma = (1 \ 3 \ 4 \ 9) \circ (2 \ 7) \circ (5 \ 6),$$

donc une décomposition en produit de transpositions de σ est

$$\sigma = (1 \ 3) \circ (3 \ 4) \circ (4 \ 9) \circ (2 \ 7) \circ (5 \ 6).$$

Donc $\varepsilon(\sigma) = (-1)^5 = -1$.

(b) Donner, sans justification, l'ordre de σ .

Correction

L'ordre de σ est égal à 4.

10. Donner, en expliquant brièvement mais sans justifier précisément, l'ordre d'une permutation en fonction de sa décomposition en cycles à supports disjoints.

Correction

Si $\sigma = \rho_1 \circ \dots \circ \rho_N$ où ρ_1 est un p_1 -cycle, ρ_2 un p_2 -cycles, ..., ρ_N un p_N -cycle, avec $(p_1, \dots, p_N) \in \llbracket 2, n \rrbracket^N$, à supports disjoints, alors on sait que pour tout k dans \mathbb{N} ,

$$\sigma^k = \rho_1^k \circ \rho_2^k \circ \dots \circ \rho_N^k,$$

car deux cycles à supports disjoints commutent. Donc $\sigma^k = \text{Id}$ ssi pour tout $i, \rho_i^k = \text{Id}$, donc ssi k est multiple de tous les ordres des ρ_i , donc, par minimalité de l'ordre,

$$\omega(\sigma) = \text{ppcm}(p_1, \dots, p_N).$$

Exercice 1. Exercice remplaçant la partie précédente. On note $\mathbb{Q}[\sqrt{2}] = \{a + \sqrt{2}b, (a, b) \in \mathbb{Q}^2\}$ et $\mathbb{Q}[\sqrt{3}] = \{a + \sqrt{3}b, (a, b) \in \mathbb{Q}^2\}$.

1. Démontrer que $\mathbb{Q}[\sqrt{2}]$ est un sous-corps de $(\mathbb{R}, +, \times)$.

Correction

Corrigé dans les exercices corrigés en classe.

On admet que, de même, $\mathbb{Q}[\sqrt{3}]$ est un sous-corps de $(\mathbb{R}, +, \times)$. On va démontrer qu'il n'existe pas de morphisme de corps de $(\mathbb{Q}[\sqrt{2}], +, \times)$ dans $(\mathbb{Q}[\sqrt{3}], +, \times)$. On suppose, par l'absurde, qu'il existe un tel morphisme φ .

2. Démontrer que pour tout x dans \mathbb{Q} , $\varphi(x) = x$.

Correction

Soit déjà k dans \mathbb{N} . Alors, par récurrence immédiate,

$$\varphi(k) = \varphi(1 + 1 + \dots + 1) = k, \text{ comme } \varphi(1) = 1.$$

Ensuite, comme φ est un morphisme de corps,

$$\varphi(-k) = -\varphi(k) = -k.$$

Donc, pour tout k dans \mathbb{Z} , $\varphi(k) = k$.

Enfin, si $r \in \mathbb{Q}$, $r = \frac{p}{q}$, alors

$$\varphi(qr) = \varphi(q)\varphi(r) = q\varphi(r) \text{ et, en même temps, } \varphi(qr) = \varphi(p) = p,$$

donc

$$\varphi(r) = \frac{p}{q} = r,$$

d'où le résultat attendu.

3. Démontrer que $\varphi(\sqrt{2}) = \pm\sqrt{2}$.

Correction

Comme φ est un morphisme de corps,

$$\varphi(\sqrt{2})^2 = \varphi(\sqrt{2}^2) = 2,$$

donc $\varphi(\sqrt{2}) = \pm\sqrt{2}$.

4. Démontrer que $\sqrt{2} \notin \mathbb{Q}[\sqrt{3}]$ et conclure.

Correction

On devrait avoir $\varphi(\sqrt{2}) \in \mathbb{Q}[\sqrt{3}]$. Or, si c'était le cas, on disposerait de (a, b) dans \mathbb{Q} tels que $\varphi(\sqrt{2}) = a + b\sqrt{3}$. En supposant, sans perte de généralité, que $\varphi(\sqrt{2}) = \sqrt{2}$,

on obtient

$$\sqrt{2} = a + b\sqrt{3}.$$

En passant l'égalité au carré,

$$2 = a^2 + 3b^2 + 2ab\sqrt{3},$$

donc, si $ab \neq 0$, $\sqrt{3} = \frac{2 - a^2 - 3b^2}{2ab} \in \mathbb{Q}$, absurde!

Donc $a = 0$ ou $b = 0$.

- si $a = 0$, alors $b = \frac{\sqrt{2}}{\sqrt{3}}$. Si on écrit $b = \frac{u}{v}$, où u et v sont entiers, alors $3u^2 = 2v^2$, ce qui est absurde en regardant les valuations 2-adiques.
- si $b = 0$, donc $\sqrt{2} = a \in \mathbb{Q}$, absurde!

Il n'existe donc pas de morphisme de corps de $\mathbb{Q}[\sqrt{2}]$ dans $\mathbb{Q}[\sqrt{3}]$!

Problème 2. Théorème de Lagrange fort

Cet exercice a pour but de prouver un très joli théorème de théorie des groupes (dont vous verrez une version faible en spé) :

Théorème 1 (Lagrange)

Soit $(G, *)$ un groupe fini et H un sous-groupe de G . Alors $\text{Card}(H)$ divise $\text{Card}(G)$.

Soit donc G un groupe fini, H un sous-groupe de G . On définit la relation \mathcal{R} suivante sur G

$$\forall (x, y) \in G^2, (x\mathcal{R}y) \Leftrightarrow (x * y^{-1} \in H).$$

1. Montrer que \mathcal{R} définit bien une relation d'équivalence sur G .

Correction

Montrons que \mathcal{R} est bien une relation d'équivalence sur G .

- (a) (réflexivité) Soit x dans G . Alors $x * x^{-1} = 1_G$, élément neutre de G . Or H est un sous-groupe de G donc $1_G \in H$. Donc $x\mathcal{R}x$.
- (b) (symétrie) Soient x et y dans G tels que $x\mathcal{R}y$. Alors $x * y^{-1} \in H$. Or H est un sous-groupe de G donc $(x * y^{-1})^{-1} \in H$. Donc $(y^{-1})^{-1} * x^{-1} \in H$. Donc $y * x^{-1} \in H$. Donc $y\mathcal{R}x$.
- (c) (transitivité) Soient x, y et z dans G tels que $x\mathcal{R}y$ et $y\mathcal{R}z$. Alors $x * y^{-1} \in H$ et $y * z^{-1} \in H$. Or H est un sous-groupe de G donc $(x * y^{-1}) * (y * z^{-1}) \in H$, i.e. $x * z^{-1} \in H$. Donc $x\mathcal{R}z$.

2. Soit y dans G . Montrer que la classe d'équivalence de y est

$$Hy = \{h * y, h \in H\}.$$

Correction

Montrons que la classe d'équivalence de y est incluse dans Hy . Soit x tel que $x\mathcal{R}y$. Alors $x * y^{-1} \in H$. Posons $h = x * y^{-1}$. Alors $x = h * y$, avec $h \in H$. Donc $x \in Hy$. Réciproquement, si $x \in Hy$, on dispose de h dans H tel que $x = h * y$. Donc $x * y^{-1} = h$, i.e. $x * y^{-1} \in H$. Donc $x\mathcal{R}y$.

Soient alors (y_1, y_2, \dots, y_p) les représentants des différentes classes d'équivalence Hy_1, Hy_2, \dots, Hy_p .

3. Soit φ_i l'application définie par

$$\varphi_i : \begin{cases} H \rightarrow Hy_i \\ h \mapsto h * y_i \end{cases}$$

Montrer que φ_i est une bijection de H sur Hy_i .

Correction

Deux méthodes pour montrer que φ_i est bijective.

Méthode par injection/surjection.

- (a) Montrons que φ_i est injective. Soient h et h' dans H tels que $\varphi(h) = \varphi(h')$. Alors $h * y_i = h' * y_i$. Donc, en multipliant par y_i^{-1} des deux côtés, on obtient $h * y_i * y_i^{-1} = h' * y_i * y_i^{-1}$, i.e. $h = h'$. Donc φ_i est injective.
- (b) Montrons que φ_i est surjective. Soit x dans Hy_i . Alors on dispose de h dans H tel que $x = h * y_i$. Donc $x = \varphi(h)$. Donc φ_i est surjective.

Injective et surjective, φ_i est bijective.

Méthode par détermination d'une bijection réciproque.

Posons ψ_i définie comme suit :

$$\psi_i : \begin{cases} Hy_i \rightarrow H \\ x \mapsto x * y_i^{-1} \end{cases}$$

Déjà, ψ_i est bien à valeurs dans H , car si $x \in Hy_i$, on dispose de h dans H tel que $x = h * y_i$, donc $\psi_i(x) = h * y_i * y_i^{-1} = h \in H$.

Ensuite, si $x \in Hy_i$, $\varphi_i \circ \psi_i(x) = \varphi_i(x * y_i^{-1}) = x * y_i^{-1} * y_i = x$, et si $x \in H$, $\psi_i \circ \varphi_i(x) = \psi_i(x * y_i) = x * y_i * y_i^{-1} = x$. Donc $\varphi_i \circ \psi_i = \text{Id}_{Hy_i}$ et $\psi_i \circ \varphi_i = \text{Id}_H$. Donc φ_i est une bijection.

4. En déduire que $p \times \text{Card}(H) = \text{Card}(G)$, et conclure.

Correction

S'il existe une bijection d'un ensemble fini dans un autre ensemble fini, alors leurs cardinaux sont égaux. Donc $\text{Card}(H) = \text{Card}(Hy_i)$. Ensuite, on sait que les $(Hy_i)_{1 \leq i \leq p}$ forment une partition de G , donc

$$\text{Card}(G) = \sum_{i=1}^p \text{Card}(Hy_i).$$

Or, $\text{Card}(Hy_i) = \text{Card}(H)$, donc

$$\text{Card}(G) = \sum_{i=1}^p \text{Card}(H) = p \times \text{Card}(H).$$

Donc $\text{Card}(H)$ divise $\text{Card}(G)$. Le théorème est donc démontré.

On va maintenant donner quelques conséquences de ce théorème.

5. Soit G un groupe fini, x un élément de G . On définit le sous-groupe engendré par x , noté $\langle x \rangle$, par

$$\langle x \rangle = \{x^k, k \in \mathbb{Z}\}.$$

On note ordre de x l'entier $\omega(x) = \min\{k \in \mathbb{N}^*, x^k = e\}$.

- (a) Montrer que $\langle x \rangle$ est un sous groupe de G .

Correction

$\langle x \rangle$ est non vide car il contient x . Soient ensuite a et b deux éléments de $\langle x \rangle$. Montrons que $a * b^{-1} \in \langle x \rangle$. On dispose de k et ℓ deux entiers relatifs tels que $a = x^k$ et $b = x^\ell$. Donc $b^{-1} = x^{-\ell}$, donc

$$a * b^{-1} = x^k * x^{-\ell} = x^{k-\ell},$$

et $k - \ell \in \mathbb{Z}$. Donc $a * b^{-1} \in \langle x \rangle$. Donc $\langle x \rangle$ est un sous-groupe de G .

(b) Montrer qu'il s'agit du plus petit sous-groupe de G contenant x .

Correction

Soit H un sous groupe contenant x . On montre que $\langle x \rangle$ est inclus dans H : montrons le par récurrence. Montrons par récurrence que H contient x^n pour tout entier naturel n .

Initialisation. H est un groupe donc $x^0 = 1_G \in H$.

Hérédité. Supposons que $x^n \in H$ pour un certain n . Alors comme $x \in H$ et H est un sous-groupe de G , $x^n * x \in H$, i.e. $x^{n+1} \in H$.

Conclusion. Héréditaire et vraie au rang 0, la proposition est vraie pour tout entier naturel n par le principe de récurrence.

De plus, si $k \in \mathbb{Z}_-$, on sait que $x^{-k} \in H$ (par la proposition précédente), et donc, comme G est un groupe, $(x^{-k})^{-1} \in H$, donc $x^k \in H$.

Donc H contient $\langle x \rangle$. Le résultat est donc démontré.

(c) Montrer que $\omega(x)$ est bien défini et que $\omega(x) | \text{Card}(G)$.

Correction

Déjà, G est un groupe fini, donc par la même construction qu'au problème 1, $\omega(x)$ est bien défini.

Ensuite, par les mêmes raisonnements qu'au problème 1, encore, on peut dire que $e_G, x, \dots, x^{\omega(x)-1}$ sont deux à deux distincts. Ainsi, $\langle x \rangle$ possède $\omega(x)$ éléments (par le même argument de division euclidienne qu'au problème 1).

Donc, comme, par le théorème de Lagrange, $|\langle x \rangle|$ divise $|G|$, on peut dire que $\omega(x)$ divise $|G|$.

6. Supposons maintenant que G est fini de cardinal p , p premier. Montrer que G est cyclique, et en déduire qu'il est isomorphe à \mathbb{U}_p .

Correction

Si $G = \{1_G\}$, c'est gagné. Sinon, soit x dans G tel que $x \neq 1_G$. Alors le cardinal de $\langle x \rangle$ est supérieur ou égal à 2 (car $1_G \neq x$) et divise p premier. Donc $\langle x \rangle$ est de cardinal p . Donc $\langle x \rangle = G$. Donc G est cyclique, engendré par x .

Ensuite vient une des questions les plus dures du sujet : montrer que G est isomorphe à \mathbb{U}_p . On a envie de poser $\varphi : x^k \mapsto e^{\frac{2ik\pi}{p}}$. Problème : qui nous dit que cette fonction est

bien définie, i.e. que si $x^k = x^\ell$, alors $e^{\frac{2ik\pi}{n}} = e^{\frac{2i\ell\pi}{n}}$?

Commençons déjà par montrer que $G = \{e, x, \dots, x^{p-1}\}$.

On sait que G est fini, de cardinal p , donc, parmi les $p + 1$ éléments e, x, \dots, x^p , deux sont égaux, i.e. il existe $k < \ell$ tels que $x^k = x^\ell$. En particulier $x^{\ell-k} = e$.

Considérons alors $A = \{k \in \mathbb{Z}, x^k = e\}$. A est clairement un sous-groupe de $(\mathbb{Z}, +)$.

Donc on dispose de $q \in \mathbb{N}$ tel que $A = q\mathbb{Z}$. De plus, A contient $\ell - k$ donc $A \neq \{0\}$, donc $q > 0$. Ainsi, $x^q = e$, et $G = \{x^k, k \in \mathbb{Z}\} = \{e, x, \dots, x^{q-1}\}$.

Donc $q = p$. Ainsi, $x^p = e$!

Posons alors

$$\varphi : \begin{cases} G \rightarrow \mathbb{U}_p \\ x^k \mapsto e^{\frac{2ik\pi}{p}} \end{cases}.$$

- Il faut déjà vérifier que φ est bien définie. Soient k et k' tels que $x^k = x^{k'}$. Alors $x^{k-k'} = e$, donc $k - k' \in A$, donc $k \equiv k' [p]$. Ainsi, $e^{\frac{2ik\pi}{p}} = e^{\frac{2ik'\pi}{p}}$. Donc φ est bien définie.
- Vérifions que φ est un morphisme. Soient a et b dans G , k et ℓ dans \mathbb{Z} tels que $a = x^k$ et $b = x^\ell$. Alors

$$\varphi(a * b^{-1}) = \varphi(x^k * x^{-\ell}) = \varphi(x^{k-\ell}) = e^{\frac{2i(k-\ell)\pi}{p}} = \frac{e^{\frac{2ik\pi}{p}}}{e^{\frac{2i\ell\pi}{p}}},$$

donc φ est un morphisme.

- Enfin, soit $a \in \ker(\varphi)$, $a = x^k$. Alors $\varphi(a) = 1$, i.e. $e^{\frac{2ik\pi}{p}} = 1$, donc $k \equiv 0 [p]$. Donc $x^k = e$, donc $a = e$. Donc $\ker(\varphi) = e$, donc φ est injective. Injective, entre deux ensembles de même cardinal, φ est bijective.

Finalement, \mathbb{U}_p et G sont bien isomorphes. Ouf !

7. Montrer que si p n'est pas premier, il peut exister des groupes finis de cardinal p non cycliques.

Correction

Déjà, si on pense à \mathcal{S}_3 , \mathcal{S}_3 n'est pas abélien donc ne peut pas être cyclique.

Sinon, considérons $\mathbb{U}_2 \times \mathbb{U}_2 = \{(-1, -1), (-1, 1), (1, -1), (1, 1)\}$. Alors ce groupe n'est pas cyclique : tous les éléments ont leur carré égal à $(1, 1)$, donc ne peuvent engendrer tout le groupe.

On va maintenant montrer que tout groupe fini de cardinal p^2 (p premier) est abélien. Soit G un groupe fini de cardinal p^2 . Soit, pour $h \in G$, $\varphi_h : x \mapsto h * x * h^{-1}$.

8. Vérifier que φ_h est un isomorphisme de G , i.e. un morphisme de groupes bijectif.

Correction

φ_h est bien un morphisme :

- $\varphi_h(1_G) = h * 1_G * h^{-1} = 1_G$.
- pour tous x et y , $\varphi_h(x) * \varphi_h(y) = h * x * h^{-1} * h * y * h^{-1} = h * (x * y) * h^{-1} = \varphi_h(x * y)$.

- pour tout x , $(\varphi_h(x))^{-1} = (h * x * h^{-1})^{-1} = (h^{-1})^{-1} * x^{-1} * h^{-1} = h * x * h^{-1}$.
- La bijectivité est immédiate en remarquant que $\varphi_h^{-1} = \varphi_{h^{-1}}$.

9. Soit $x \in G$. On appelle orbite de x par l'action de G par automorphismes l'ensemble

$$\mathcal{O}(x) = \{\varphi_h(x), h \in G\}.$$

Montrer, en considérant la relation d'équivalence \sim définie par $g \sim h$ ssi $\varphi_g(x) = \varphi_h(x)$, que le cardinal de l'orbite d'un élément divise le cardinal de G .

Correction

On considère la relation d'équivalence \sim sur G définie par $g \sim h$ ssi $\varphi_g(x) = \varphi_h(x)$. Si l'on prend deux classes d'équivalence $\overline{h_1}$ et $\overline{h_2}$, alors $x \mapsto h_2 * h_1^{-1}$ est une bijection de $\overline{h_1}$ dans $\overline{h_2}$: si $a \in \overline{h_1}$, alors

$$\begin{aligned} (h_2 * h_1^{-1} * a) * x * (h_2 * h_1^{-1} * a)^{-1} &= h_2 * h_1^{-1} * (\varphi_a(x)) * h_1 * h_2^{-1} \\ &= h_2 * h_1^{-1} * (\varphi_{h_1}(x)) * h_1 * h_2^{-1} \\ &= h_2 * x * h_2^{-1}, \end{aligned}$$

et réciproquement. Et le caractère bijectif a déjà été démontré.

Donc toutes les classes d'équivalence ont le même cardinal c . De plus, chaque élément de $\mathcal{O}(x)$ est un **représentant d'une classe d'équivalence**.

Comme elles forment une partition de G , le cardinal de G est de $c \times \text{Card}(\mathcal{O}(x))$.

10. On appelle centre de G l'ensemble $Z(G) = \{x \in G, \forall y \in G, x * y = y * x\}$.

(a) Démontrer que $Z(G)$ n'est pas trivial (i.e. réduit au neutre). On s'intéressera au cardinal des orbites.

Correction

Le cardinal de l'orbite d'un élément de $Z(G)$ est 1, car tout élément de $Z(G)$ commute avec tous les éléments de G .

Or, on remarque que l'ensemble des orbites forme une partition de G , donc, si l'on note $\mathcal{O}_1, \mathcal{O}_2, \dots, \mathcal{O}_r$ les r orbites de G , on a

$$\begin{aligned} \text{Card}(G) &= \sum_{i=1}^r \text{Card}(\mathcal{O}_i) = \sum_{\substack{1 \leq i \leq r \\ \text{Card}(\mathcal{O}_i)=1}} 1 + \sum_{\substack{1 \leq i \leq r \\ \text{Card}(\mathcal{O}_i) \neq 1}} \text{Card}(\mathcal{O}_i) \\ &= \text{Card}(Z(G)) + \sum_{\substack{1 \leq i \leq r \\ \text{Card}(\mathcal{O}_i) \neq 1}} \text{Card}(\mathcal{O}_i). \end{aligned}$$

Or, on a vu à la question précédente que le cardinal de toute orbite divise le cardinal de G . Donc le cardinal de toute orbite est égal à 1, p ou p^2 . Donc, en particulier, p divise $\sum_{\substack{1 \leq i \leq r \\ \text{Card}(\mathcal{O}_i) \neq 1}} \text{Card}(\mathcal{O}_i)$. Donc, comme p divise $\text{Card}(G)$, p divise $\text{Card}(Z(G))$,

qui est > 0 donc $Z(G)$ n'est pas trivial.

(b) En déduire que G est abélien.

Correction

Pour montrer que G est abélien, il suffit de montrer que $Z(G)$ est de cardinal p^2 . Si ça n'était pas le cas, on aurait $Z(G)$ de cardinal p . Mais alors si x n'était pas dans $Z(G)$, l'ensemble $H = \{g \in G, g * x = x * g\}$ est un sous-groupe de G contenant $Z(G)$ et x , donc de cardinal $> p$, et, d'après le théorème de Lagrange, son cardinal divise $\text{Card}(G)$. Donc H serait de cardinal p^2 , donc x commuterait avec tous les éléments de H , absurde ! Donc $Z(G) = G$, donc G est abélien.

Problème 3. Sous-groupes de $S(\mathbb{R})$

On note G l'ensemble des bijections continues de \mathbb{R} dans \mathbb{R} , muni de la loi \circ . On rappelle que (G, \circ) est un groupe, de neutre $\text{Id}_{\mathbb{R}}$. Si $f \in G$ et $n \in \mathbb{N}^*$, on note

$$f^n = \underbrace{f \circ \dots \circ f}_{n \text{ fois}}.$$

Par convention, $f^0 = \text{Id}_{\mathbb{R}}$. Et, comme f est bijective, on note aussi $f^{-n} = f^{-1} \circ \dots \circ f^{-1}$.

A. Généralités

1. Que peut-on dire de la monotonie des éléments de G ?

Correction

Les éléments de G sont des bijections, donc des **injections continues** de \mathbb{R} dans \mathbb{R} , donc elles sont strictement monotones.

2. On note, pour $a \in \mathbb{R}^*$ et $b \in \mathbb{R}$, $f_{a,b} : x \mapsto ax + b$. On appelle $\text{Aff} = \{f_{a,b}, (a,b) \in \mathbb{R}^* \times \mathbb{R}\}$ leur ensemble. Démontrer que Aff est un sous-groupe de G .

Correction

. Déjà, Aff est inclus dans G . En effet, si $a \in \mathbb{R}^*$ et $b \in \mathbb{R}$, $f_{a,b}$ est clairement continue et on remarque que pour $(x, y) \in \mathbb{R}^2$,

$$\begin{aligned} f_{a,b}(x) = y &\Leftrightarrow ax + b = y \\ &\Leftrightarrow x = \frac{y - b}{a} \\ &\Leftrightarrow x = f_{\frac{1}{a}, -\frac{b}{a}}(y). \end{aligned}$$

Ainsi, $f_{a,b}$ est une bijection, de bijection réciproque $f_{\frac{1}{a}, -\frac{b}{a}}(y)$.

Ceci permet de démontrer que Aff est inclus dans G **et** que cet ensemble est stable par passage à l'inverse !

. Ensuite, $\text{Id}_{\mathbb{R}} = f_{1,0}$ est bien dans Aff .

. Enfin, si $(a, b) \in \mathbb{R}^* \times \mathbb{R}$ et $(c, d) \in \mathbb{R}^* \times \mathbb{R}$, si $x \in \mathbb{R}$, alors

$$\begin{aligned} f_{a,b} \circ f_{c,d}(x) &= f_{a,b}(cx + d) \\ &= a(cx + d) + b \\ &= acx + ad + b = f_{ac, ad+b}(x), \end{aligned}$$

donc $f_{a,b} \circ f_{c,d} \in \text{Aff}$, donc Aff est bien stable par \circ .

B. Sous-groupes finis de G

Soit désormais H un sous-groupe fini de G .

3. Si H est de cardinal 1, qui est H ?

Correction

Si H est de cardinal 1, comme H contient au moins $\text{Id}_{\mathbb{R}}$, alors $H = \{\text{Id}_{\mathbb{R}}\}$.

Soit désormais f dans H .

4. Démontrer qu'il existe $p \in \mathbb{N}^*$ tel que $f^p = \text{Id}_{\mathbb{R}}$.

Correction

On sait que pour tout n dans \mathbb{N} , $f^n \in H$. Mais, comme H est fini, les f^n , pour n dans \mathbb{N} , ne peuvent être deux à deux distinctes.

Ainsi, on dispose de n, m différents tels que $f^n = f^m$. Sans perte de généralité, on peut supposer que $n > m$. Ainsi, $f^{n-m} = \text{Id}_{\mathbb{R}}$, et $n - m \in \mathbb{N}^*$. D'où le résultat souhaité !

B-I. Cas où f est strictement croissante

5. Dans cette question, on suppose f strictement croissante. Démontrer, par l'absurde que $f = \text{Id}_{\mathbb{R}}$.

Correction

Si $f \neq \text{Id}_{\mathbb{R}}$, alors on dispose de $x \in \mathbb{R}$ tel que $f(x) \neq x$.

. Si $f(x) < x$, comme f est strictement croissante, $f^2(x) < f(x) < x$ et

$$f^p(x) < f^{p-1}(x) < \dots < f(x) < x,$$

soit $x < x$, absurde !

. Si $x < f(x)$, alors $x < f(x) < \dots < f^p(x) = x$, absurde aussi !

Ainsi, $f = \text{Id}_{\mathbb{R}}$.

B-II. Cas où f est strictement décroissante

Dans cette partie seulement, on suppose f strictement décroissante.

6. Démontrer que $f \circ f = \text{Id}_{\mathbb{R}}$.

Correction

On sait alors que $f \circ f$ est strictement croissante, donc, par la question précédente, $f \circ f = \text{Id}_{\mathbb{R}}$.

On définit la fonction $g \in \mathbb{R}^{\mathbb{R}}$ par : $\forall x \in \mathbb{R}, g(x) = x - f(x)$.

7. Montrer que g est une bijection de \mathbb{R} dans \mathbb{R} , et que

$$\forall x \in \mathbb{R}, f(x) = g^{-1}(-g(x)) = g^{-1} \circ (-\text{Id}_{\mathbb{R}}) \circ g(x).$$

Correction

Déjà, g est **strictement croissante** comme somme de fonctions strictement croissantes, donc est injective.

Ensuite, si $x \geq 0$, $g(x) \geq x - f(0)$, donc $g(x) \xrightarrow{x \rightarrow +\infty} +\infty$.

De même, si $x \leq 0$, $g(x) \leq x - f(0)$, donc $g(x) \xrightarrow{x \rightarrow +\infty} -\infty$.

g étant continue, on en déduit, par le théorème des valeurs intermédiaires, que g est surjective de \mathbb{R} dans \mathbb{R} .

Donc g est une bijection de \mathbb{R} dans \mathbb{R} .

Soit x dans \mathbb{R} . Alors

$$g \circ f(x) = f(x) - f(f(x)) = f(x) - x = -g(x),$$

donc, en composant à gauche par g^{-1} , $f(x) = g^{-1}(g(x))$.

C. Conclusion

8. Décrire le plus précidément possible les sous-groupes finis de G : quel peut être leur cardinal, quelle est la forme de leurs éléments, etc.

Correction

Les sous-groupes finis de G possèdent donc 1 ou 2 éléments : au plus une application strictement croissante, $\text{Id}_{\mathbb{R}}$, et au plus une application strictement décroissante : si g et h sont deux applications décroissantes de \mathbb{R} , $g \circ h$ et $g \circ g$ sont strictement croissantes, donc égales à $\text{Id}_{\mathbb{R}}$, donc $g = h$.

On a donc :

- le singleton $\{\text{Id}_{\mathbb{R}}\}$,
- les paires de la forme $\{\text{Id}_{\mathbb{R}}, g^{-1} \circ (-\text{Id}_{\mathbb{R}}) \circ g\}$ où g est une bijection continue quelconque de \mathbb{R} .