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 $\mathbb{N}^*$,

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

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 $x_1, \ldots, x_{n+1}$ sont $n+1$ éléments de E, alors il existe $(i, j) \in [\![1, n+1]\!]^2$ 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 $\omega(x)$.
2. Démontrer que si $(G, \star)$ est **finie**, alors tout élément de G admet un ordre.
   On pourra considérer, si n est le cardinal de G et $x \in G$, $x^0, x^1, \ldots, x^n$, et utiliser le principe des tiroirs.
3. Soit x dans G. Démontrer que si x est d'ordre p dans G (où $p \in \mathbb{N}^*$), alors $x^0, \ldots, x^{p-1}$ sont deux à deux distincts. *On raisonnera par l'absurde et on contredira la minimalité de p.*

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.

B. Théorème de Lagrange faible

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

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

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

Dans cette partie, on va démontrer le résultat suivant :

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

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 $\varphi : \left| \begin{array}{l} G \to G \\ y \mapsto x \star y \end{array} \right.$

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

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.

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

Soit n un entier naturel supérieur ou égal à 2. Soit p dans $[\![2, n]\!]$.

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

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.

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

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

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 $(\mathbb{R}, +, \times)$.

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 $\mathbb{Q}$, $\varphi(x) = x$.

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

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

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 Card(H) divise 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.

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

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

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

3. Soit φ_i l'application définie par

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

Montrer que φ_i est une bijection de H sur Hy_i.

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

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 $< x >$, par

$$< x >= \{x^k, k \in \mathbb{Z}\}.$$

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

(a) Montrer que $< x >$ est un sous groupe de G.

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

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

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 $\mathbb{U}_p$.

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

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.

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.

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.*

(b) En déduire que 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 $\mathrm{Id}_{\mathbb{R}}$. Si $f \in G$ et $n \in \mathbb{N}^*$, on note

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

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

A. Généralités

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

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

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 ?

Soit désormais f dans H.

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

B-I. Cas où f est strictement croissante

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

B-II. Cas où f est strictement décroissante

Dans cette partie seulement, on suppose f strictement décroissante.

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

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

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

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.