MAGMAS

1 On pose pour tous $x, y \in [0,1] \times [0,1]$:

$$x \star y = x + y - xy.$$

Montrer que $\big([0,1], \star\big)$ est un magma commutatif et associatif avec élément neutre et déterminer ses inversibles.

---

2 Montrer que tout magma associatif fini non vide contient un *idempotent*, i.e. un élément x pour lequel $x^2 = x$.

GROUPES, SOUS-GROUPES

3 **1)** Soient G un groupe, M un ensemble et φ une bijection de G sur M. On définit une loi interne $\star$ sur M en posant pour tous $x, y \in M$:

$$x \star y = \varphi\big(\varphi^{-1}(x)\varphi^{-1}(y)\big).$$

Montrer que $(M, \star)$ est un groupe.

2) **a)** Montrer que $\text{th}\,(x+y) = \dfrac{\text{th}\,x + \text{th}\,y}{1 + \text{th}\,x\,\text{th}\,y}$ pour tous $x, y \in \mathbb{R}$.

b) On pose pour tous $x, y \in]-1,1[$:

$$x \oplus y = \frac{x+y}{1+xy}.$$

Montrer que $\oplus$ est une loi interne sur $]-1,1[$ et que $\big(]-1,1[, \oplus\big)$ est un groupe commutatif.

---

4 Soient G un groupe fini et H et K deux sous-groupes de G d'ordres premiers entre eux. Montrer que $H \cap K = \{1_G\}$.

---

5 Soit G un groupe.

1) Soit $x \in G$. On appelle *centralisateur de x dans G* l'ensemble $C_G(x)$ des éléments de G qui commutent à x. Montrer que $C_G(x)$ est un sous-groupe de G.

2) On appelle *centre de G* l'ensemble $Z(G)$ des éléments de G qui commutent à tout élément de G. Montrer que $Z(G)$ est un sous-groupe de G.

3) Pour tous $x, y \in G$, on dit que y est *conjugué à x* si $y = gxg^{-1}$ pour un certain $g \in G$.

a) Montrer que la relation de conjugaison ainsi définie est une relation d'équivalence sur G.

b) On suppose G fini. Montrer, en étudiant l'application $g \longmapsto gxg^{-1}$, que la classe de conjugaison de x est de cardinal $\dfrac{|G|}{|C_G(x)|}$ pour tout $x \in G$.

c) On suppose que $|G| = p^n$ pour certains $p \in \mathbb{P}$ et $n \in \mathbb{N}^*$. Montrer que p divise l'ordre de $Z(G)$, puis que $|Z(G)| \geqslant p$.

d) On suppose que $|G| = p^2$ pour un certain $p \in \mathbb{P}$. Montrer que G est commutatif.

---

6 **1)** Trouver deux sous-groupes de $\mathbb{R}^*$ dont la réunion n'est pas un sous-groupe de $\mathbb{R}^*$.

2) **a)** Montrer que $\bigcup_{n \in \mathbb{N}^*} \mathbb{U}_n$ est un sous-groupe de $\mathbb{C}^*$.

b) Soient $m, n \in \mathbb{N}^*$. À quelle condition nécessaire et suffisante sur m et n est-il vrai que $\mathbb{U}_m$ est un sous-groupe de $\mathbb{U}_n$?

3) Soient G un groupe et $(H_n)_{n \in \mathbb{N}}$ une suite croissante de sous-groupes de G. Montrer que $\bigcup_{n \in \mathbb{N}} H_n$ est un sous-groupe de G.

4) Soient G un groupe et H et K deux sous-groupes de G. Montrer que $H \cup K$ est un sous-groupe de G si et seulement si $H \subset K$ ou $K \subset H$.

---

7 **1)** Soient G un groupe commutatif fini et $g \in G$.

a) Montrer que l'application $x \longmapsto gx$ est une permutation de G.

b) Justifier l'existence du produit $\prod_{x \in G} (gx)$, puis le calculer de deux manières et en déduire que $g^{|G|} = 1_G$ (*théorème de Lagrange*).

2) Déterminer les sous-groupes finis de $\mathbb{C}^*$.

3) Soit $p \in \mathbb{P}$. On pose $G = \bigcup_{k \in \mathbb{N}^*} \mathbb{U}_{p^k}$.

a) Montrer que G est un sous-groupe de $\mathbb{C}^*$.

b) Soient $a \in \mathbb{Z}$ premier à p et $k \in \mathbb{N}^*$. Montrer que tout sous-groupe de $\mathbb{C}^*$ qui contient $e^{\frac{2ia\pi}{p^k}}$ contient $e^{\frac{2i\pi}{p^k}}$.

c) En déduire que tout sous-groupe de G distinct de G est fini.

---

8 Soit G un groupe.

1) On suppose que $x^2 = 1_G$ pour tout $x \in G$. Montrer que G est commutatif.

2) On suppose que $(xy)^3 = x^3y^3$ pour tous $x, y \in G$ et que tout élément de G peut être écrit comme un cube.

a) Montrer que $x^3y^2 = y^2x^3$ pour tous $x, y \in G$.

b) En déduire que pour tout $x \in G$, x^2 commute à tout élément de G.

c) En déduire que G est commutatif.

---

9 Soient G un groupe fini et A et B deux parties de G pour lesquelles $|A| + |B| > |G|$. On pose :

$$B^{-1} = \big\{b^{-1} \mid \quad b \in B\big\} \quad \text{et} \quad AB = \big\{ab \mid \quad a \in A, \quad b \in B\big\}.$$

Montrer que $A \cap gB^{-1}$ est non vide pour tout $g \in G$ et en déduire que $G = AB$.

MORPHISMES DE GROUPES

10 Montrer que les applications suivantes sont des morphismes de groupes et déterminer leur image et leur noyau : **1)** $n \longmapsto (-1)^n$ sur $\mathbb{Z}$.

2) $z \longmapsto \dfrac{z}{|z|}$ sur $\mathbb{C}^*$. **3)** $(r,u) \longmapsto ru$ sur $\mathbb{R}_+^* \times \mathbb{U}$.
4) $M \longmapsto \det(M)$ sur $\mathrm{GL}_2(\mathbb{C})$.

---

11 Soient G et G' deux groupes et f un morphisme de groupes de G dans G'.
1) Montrer que si G est commutatif, $\mathrm{Im}\, f$ l'est aussi.
2) Soit B' un sous-groupe commutatif de G'. Montrer que si f est injectif, alors $f^{-1}(B')$ est commutatif.

---

12 Soient G et G' deux groupes et f un morphisme de groupes de G dans G'. Montrer que si G est fini :

$$|G| = \big|\mathrm{Ker}\, f\big| \times \big|\mathrm{Im}\, f\big|.$$

---

13 Soit G un groupe.
1) Pour tout $g \in G$, on note σ_g l'application :

$$x \longmapsto gxg^{-1} \qquad \text{de } G \text{ dans } G.$$

a) Montrer que σ_g est un automorphisme de G pour tout $g \in G$.
b) Montrer que l'application $g \overset{\sigma}{\longmapsto} \sigma_g$ est un morphisme de groupes de G dans $\mathrm{Aut}(G)$ et décrire son noyau.
2) Pour tout $g \in G$, on note μ_g l'application $x \longmapsto gx$ de G dans G.
a) Montrer μ_g est une permutation de G pour tout $g \in G$.
b) Montrer que l'application $g \overset{\mu}{\longmapsto} \mu_g$ est un morphisme de groupes injectif de G dans S_G.

14
1) Montrer que les groupes $\mathbb{R}$ et $\mathbb{R}_+^*$ sont isomorphes.
2) Montrer que les groupes $\mathbb{Q}$ et $\mathbb{Q}_+^*$ ne sont pas isomorphes. On pourra noter que pour tout morphisme de groupes f de $\mathbb{Q}$ dans $\mathbb{Q}_+^*$, $f\left(\dfrac{x}{2}\right)^2 = f(x)$ pour tout $x \in \mathbb{Q}$.
3) Déterminer l'ensemble des morphismes de groupes de $\mathbb{Q}$ dans $\mathbb{Q}_+^*$.

---

15 Soient $m,n \in \mathbb{N}^*$. On note f l'application :

$$z \longmapsto \big(z^n, z^m\big) \qquad \text{de } \mathbb{U}_{mn} \text{ dans } \mathbb{U}_m \times \mathbb{U}_n.$$

1) Montrer que f est un morphisme de groupes et trouver un entier $k \in \mathbb{N}^*$ pour lequel $\mathrm{Ker}\, f = \mathbb{U}_k$.
2) À quelle condition nécessaire et suffisante sur m et n l'application f est-elle un isomorphisme de groupes de $\mathbb{U}_{mn}$ sur $\mathbb{U}_m \times \mathbb{U}_n$?

---

16 Soient G et G' deux groupes isomorphes. Montrer que $\mathrm{Aut}(G)$ et $\mathrm{Aut}(G')$ sont isomorphes.

---

17 Soient G un groupe fini et φ et ψ deux morphismes de groupes de G dans $\mathbb{C}^*$. Montrer que :

$$\sum_{x \in G} \varphi(x)\,\psi\big(x^{-1}\big) \in \big\{0, |G|\big\}.$$

GROUPES SYMÉTRIQUES

18 Pour tout $\sigma \in S_n$, on note parfois matriciellement $\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$ la permutation σ.
1) Écrire $(2\,4\,6\,5)(1\,3\,7)(2\,5\,4)(2\,5)\,(1\,4\,6)$ comme un produit de cycles disjoints.
2) Écrire $\sigma\sigma'$ et σ^{-1} comme des produits de cycles disjoints pour $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 7 & 1 & 3 & 5 & 6 \end{pmatrix}$ et :

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

---

19 Pour tout $\sigma \in S_n$, on note $\overline{\sigma}$ l'unique prolongement de σ à $[\![1,n+1]\!]$ qui fixe $n+1$. Montrer que l'application $\sigma \longmapsto \overline{\sigma}$ est un morphisme injectif de groupes de S_n dans S_{n+1}.

20
1) Soit $p \geqslant 2$.
a) Simplifier $(x_1\ x_2)(x_2\ x_3)\ldots(x_{p-1}\ x_p)$ et vérifier que :

$$\sigma(x_1\ x_2\ \ldots\ x_p)\sigma^{-1} = \big(\sigma(x_1)\,\sigma(x_2)\ \ldots\ \sigma(x_p)\big)$$

pour tous $x_1,\ldots,x_p \in [\![1,n]\!]$ distincts et $\sigma \in S_n$.
b) En déduire que tout p-cycle de $[\![1,n]\!]$ est un conjugué de $(1\ 2\ \ldots\ p)$.
2) Montrer que $\mathrm{Z}(S_n) = \{\mathrm{Id}\}$ si $n \geqslant 3$, où $\mathrm{Z}(S_n)$ est le *centre de* S_n, i.e. l'ensemble des éléments de S_n qui commutent à tout élément de S_n.
3)
a) Montrer que S_n est engendré par ses transpositions.
b) En déduire que S_n est engendré par les transpositions $(1\ i)$, i décrivant $[\![2,n]\!]$.
4) On pose $H = \big\{\sigma \in S_n \mid \sigma(1) = 1\big\}$, sous-groupe de S_n. On souhaite montrer que H est *maximal dans* S_n, i.e. que H et S_n sont les seuls sous-groupes de S_n contenant H. Soit M un sous-groupe de S_n contenant strictement H. On fixe $\sigma \in M \setminus H$.
a) Montrer que la transposition $\big(1\ \sigma(1)\big)$ apparaît dans la décomposition en produit de cycles disjoints du produit $\sigma\big(\sigma(1)\ \sigma^{-1}(1)\big)$.
b) En déduire que M contient $\big(1\ \sigma(1)\big)$, puis que $M = S_n$ grâce au résultat de la question **3)b)**.
5)
a) Montrer que toute permutation de $[\![1,n]\!]$ est un produit de transpositions $(i\ \ i+1)$, i décrivant $[\![1,n-1]\!]$.
b) En déduire que toute permutation de $[\![1,n]\!]$ est un produit des permutations $(1\,2)$ et $(1\ 2\ \ldots\ n)$.

ANNEAUX, SOUS-ANNEAUX

21 Soit A un anneau. On appelle *centre de A* l'ensemble $Z(A)$ des éléments de A qui commutent à tout élément de A. Montrer que $Z(A)$ est un sous-anneau de A.

---

22 Montrer que $\mathbb{Z}$ est le seul sous-anneau de $\mathbb{Z}$.

---

23 L'anneau $\mathbb{R}^{\mathbb{R}}$ est-il intègre ? Déterminer $U\left(\mathbb{R}^{\mathbb{R}}\right)$.

---

24 Montrer que $\mathbb{Q}\left(\sqrt{n}\right) = \left\{a + b\sqrt{n} \mid \quad a, b \in \mathbb{Q}\right\}$ est un corps pour tout $n \in \mathbb{N}^*$ qui n'est pas un carré parfait.

---

25 On pose $A = \left\{\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid \quad a, b \in \mathbb{Z}\right\}$.

1) Montrer que A est un anneau pour les lois d'addition et de multiplication matricielles.

2) Déterminer $U(A)$.

---

26 Soit $n \in \mathbb{N}^*$. On pose $A_n = \left\{\frac{p}{n^k} \mid \quad p \in \mathbb{Z}, \quad k \in \mathbb{N}\right\}$.

1) Montrer que A_n est un sous-anneau de $\mathbb{Q}$.

2) a) Montrer que $U(A_2) = \left\{\pm 2^k \mid \quad k \in \mathbb{Z}\right\}$.

b) Déterminer $U(A_{10})$.

---

27 Montrer que l'ensemble :

$$\mathbb{Z}\left[i\sqrt{2}\right] = \left\{a + ib\sqrt{2} \mid \quad a, b \in \mathbb{Z}\right\}$$

est un sous-anneau de $\mathbb{C}$, puis déterminer $U\left(\mathbb{Z}\left[i\sqrt{2}\right]\right)$.

---

28 Soit A un anneau commutatif intègre. Pour tous $a, b \in A$, on dit que a *divise* b (*dans A*), ce qu'on note $a \mid b$, si $b = ak$ pour un certain $k \in A$. Montrer que pour tous $a, b \in A$:

$$a \mid b \text{ et } b \mid a \iff \exists u \in U(A), \quad b = au.$$

---

29 Soit A un anneau commutatif fini. Montrer, en étudiant l'application $x \longmapsto ax$ pour tout $a \in A$, que A est intègre si et seulement si c'est un corps.

---

30 Soit A un anneau. On dit qu'un élément $x \in A$ est *nilpotent* si $x^p = 0_A$ pour un certain $p \in \mathbb{N}^*$. On note $\mathrm{Nil}(A)$ l'ensemble des éléments nilpotents de A.

1) Déterminer $\mathrm{Nil}(A)$ dans le cas où A est intègre.

2) Montrer que la somme et le produit de deux éléments nilpotents de A qui commutent sont encore nilpotents.

3) Montrer que $1_A + \mathrm{Nil}(A) \subset U(A)$.

4) Déterminer $\mathrm{Nil}\left(\mathbb{Z}/n\mathbb{Z}\right)$ pour tout $n \in \mathbb{N}^*$ ainsi que son cardinal.

MORPHISMES D'ANNEAUX

31 Soient K et K' deux corps et f un morphisme de corps de K dans K'. Montrer que f est injectif.

32

1) Les corps $\mathbb{R}$ et $\mathbb{C}$ sont-ils isomorphes ?

2) Déterminer tous les endomorphismes de corps de $\mathbb{C}$ dont la restriction à $\mathbb{R}$ est la fonction identité.

---

33 On admet que $\mathbb{Z}[i] = \left\{a + ib \mid \quad a, b \in \mathbb{Z}\right\}$ et $\mathbb{Z}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} \mid \quad a, b \in \mathbb{Z}\right\}$ sont des sous-anneaux de $\mathbb{C}$. Sont-ils isomorphes en tant que groupes ? Et en tant qu'anneaux ?

34

1) Soit φ un morphisme d'anneaux de $\mathscr{C}(\mathbb{R}, \mathbb{R})$ dans $\mathscr{C}^1(\mathbb{R}, \mathbb{R})$.

a) Montrer que pour toute fonction $f \in \mathscr{C}(\mathbb{R}, \mathbb{R})$ positive, la fonction $\varphi(f)$ est positive.

b) En déduire que $\varphi\left(|f|\right) = \left|\varphi(f)\right|$ pour toute fonction $f \in \mathscr{C}(\mathbb{R}, \mathbb{R})$.

2) En déduire que les anneaux $\mathscr{C}(\mathbb{R}, \mathbb{R})$ et $\mathscr{C}^1(\mathbb{R}, \mathbb{R})$ ne sont pas isomorphes.

---

35 Soit K un corps.

1) a) Montrer que l'application $n \overset{f}{\longmapsto} n1_K$ est un morphisme d'anneaux de $\mathbb{Z}$ dans K.

b) Montrer que soit f est injectif, soit $\mathrm{Ker}\, f = p\mathbb{Z}$ pour un certain $p \in \mathbb{P}$. On dit que K est *de caractéristique* 0 dans le premier cas et *de caractéristique p* dans le deuxième.

2) On suppose K de caractéristique $p \in \mathbb{P}$.

a) Montrer que K contient un sous-corps isomorphe à $\mathbb{F}_p$ et que celui-ci est le plus petit sous-corps de K.

b) Montrer que l'application $x \longmapsto x^p$ est un endomorphisme de corps de K.

3) Montrer que si K est de caractéristique 0, il contient un sous-corps isomorphe à $\mathbb{Q}$ et que celui-ci est le plus petit sous-corps de K.

ANNEAUX $\mathbb{Z}/n\mathbb{Z}$ ET ARITHMÉTIQUE

36

1) Résoudre les équations suivantes :

a) $\overline{3}x = \overline{7}$ d'inconnue $x \in \mathbb{Z}/13\mathbb{Z}$.

b) $\overline{2}x = \overline{5}$ d'inconnue $x \in \mathbb{Z}/12\mathbb{Z}$.

c) $\overline{6}x = \overline{21}$ d'inconnue $x \in \mathbb{Z}/45\mathbb{Z}$.

2) Résoudre les systèmes suivants d'inconnue $(x,y)\in\mathbb{Z}^2$:

a) $\begin{cases} x\equiv 6\ [9] \\ x\equiv 7\ [10]. \end{cases}$ **b)** $\begin{cases} x\equiv 3\ [11] \\ x\equiv 2\ [14]. \end{cases}$

3) Soient $p\in\mathbb{P}$ impair, $a\in\mathbb{F}_p^*$ et $b,c\in\mathbb{F}_p$. Montrer que l'équation $ax^2+bx+c=\overline{0}$ d'inconnue $x\in\mathbb{F}_p$ possède au plus 2 solutions. À quelle condition nécessaire et suffisante sur a, b et c en possède-t-elle au moins une ?

37

1) a) Soit $G=\{g_1,\dots,g_n\}$ un groupe commutatif fini d'ordre n. Montrer que $g_1\dots g_n$ est le produit des éléments d'ordre 2 de G.

b) Montrer que $(p-1)!\equiv -1\ [p]$ pour tout $p\in\mathbb{P}$ (*théorème de Wilson*).

2) Soit $p\in\mathbb{P}$ impair.

a) Montrer que $\left(\frac{p-1}{2}\right)!^2\equiv(-1)^{\frac{p+1}{2}}\ [p]$.

b) En déduire que p est congru à 1 modulo 4 si et seulement si -1 est un *carré modulo* p, i.e. $-\overline{1}$ est un carré dans $\mathbb{F}_p$.

38

1) Soient $n\in\mathbb{N}^*$, $x\in\mathbb{Z}$ premier à n et $k\in\mathbb{N}^*$. Montrer que si $x^k\equiv 1\ [n]$, alors $x^{k\wedge\varphi(n)}\equiv 1\ [n]$.

2) Soit $p\in\mathbb{P}$ impair. Montrer que tout diviseur premier impair de 2^p-1 est congru à 1 modulo $2p$.

---

39 On étudie quelques conséquences arithmétiques du petit théorème de Fermat.

1) Montrer que pour tout $n\in\mathbb{Z}$, tout diviseur premier impair de n^2+1 est congru à 1 modulo 4.

2) En déduire qu'il existe une infinité de nombres premiers congrus à 1 modulo 4.

3) On suppose par l'absurde que $y^2=x^3-3$ pour un certain $(x,y)\in\mathbb{Z}^2$.

a) Étudier la parité de x et y en raisonnant modulo 8.

b) Montrer que tout diviseur premier impair de x^3+1 est congru à 1 modulo 4, puis dénicher une contradiction.

PARTIES GÉNÉRATRICES D'UN GROUPE

40

1) À quel groupe usuel $\left\langle\begin{pmatrix}1&1\\0&1\end{pmatrix}\right\rangle$ est-il isomorphe ?

2) Et $\left\langle\begin{pmatrix}1&1\\0&1\end{pmatrix},\begin{pmatrix}2&0\\0&2\end{pmatrix}\right\rangle$?

41

1) Montrer que pour tous $a_1,\dots,a_r\in\mathbb{Z}$:
$$a_1\mathbb{Z}+\dots+a_r\mathbb{Z}=(a_1\wedge\dots\wedge a_r)\mathbb{Z}.$$

2) En déduire que $\frac{2}{3}\mathbb{Z}+\frac{1}{5}\mathbb{Z}$ est un sous-groupe monogène de $\mathbb{Q}$.

3) Montrer que $\left\{\frac{n}{2^k}\ \middle|\ n\in\mathbb{Z},\quad k\in\mathbb{N}\right\}$ est un sous-groupe de $\mathbb{Q}$ et ne possède pas de partie génératrice finie.

---

42 On note $\mathscr{G}$ l'ensemble des matrices $I_n+\lambda E_{ij}$ et $I_n+(\alpha-1)E_{ii}$, λ décrivant $\mathbb{K}$, α décrivant $\mathbb{K}^*$ et i et j décrivant $[\![1,n]\!]$ avec $i\neq j$.

1) Montrer que toute opération du genre $L_i\leftrightarrow L_j$ peut être simulée à coups d'opérations du genre $L_i\leftarrow L_i+\lambda L_j$ et $L_i\leftarrow\alpha L_i$.

2) En déduire que $\mathrm{GL}_n(\mathbb{K})=\langle\mathscr{G}\rangle$.

43

1) Soient G un groupe et $x\in G$. Montrer que les endomorphismes de groupe de $\langle x\rangle$ sont exactement les applications $g\longmapsto g^n$, n décrivant $\mathbb{Z}$.

2) Décrire les groupes d'automorphismes suivants et préciser un groupe usuel auquel ils sont isomorphes : **a)** $\mathrm{Aut}(\mathbb{Z})$. **b)** $\mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)$ $(n\in\mathbb{N}^*)$. **c)** $\mathrm{Aut}(\mathbb{Q})$.

---

44 Dans cet exercice, le symbole de composition $\circ$ est omis. On note s l'application $z\longmapsto\overline{z}$ et H l'ensemble des similitudes directes $z\longmapsto az+b$, (a,b) décrivant $\mathbb{C}^*\times\mathbb{C}$, puis on pose $G=H\cup Hs$.

1) a) Montrer que H est un groupe pour la composition.

b) Montrer que $shs\in H$ pour tout $h\in H$, puis que G est un sous-groupe de $S_{\mathbb{C}}$.

2) Soit $n\geqslant 2$. On note D_n l'ensemble des fonctions $f\in G$ qui stabilisent $\mathbb{U}_n$.

a) Sans preuve, quelles similitudes directes et symétries connaît-on qui stabilisent $\mathbb{U}_n$?

b) Pourquoi $f_{|\mathbb{U}_n}$ est-elle une permutation de $\mathbb{U}_n$ pour tout $f\in D_n$?

c) Montrer que D_n est un sous-groupe de G. On l'appelle le *groupe diédral de degré* n.

d) Montrer que D_n contient s et $z\overset{r}{\longmapsto}\mathrm{e}^{\frac{2\mathrm{i}\pi}{n}}z$ et qu'il n'est pas commutatif.

e) Montrer que $\sum_{\omega\in\mathbb{U}_n}f(\omega)=\sum_{\omega\in\mathbb{U}_n}\omega$ pour tout $f\in D_n$, puis que $f(0)=0$.

f) En déduire que $D_n=\langle r,s\rangle$ et préciser $|D_n|$.

ORDRE D'UN ÉLÉMENT

45 Soit G un groupe. Montrer que xy et yx sont conjugués pour tous $x,y\in G$, puis que $|yx|=|xy|$.

---

46 Soit $p \in \mathbb{P}$. Montrer que tout groupe fini d'ordre p est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

47

1) Montrer que les groupes $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^3$ et le groupe diédral D_4 sont deux à deux non isomorphes.

2) Soient $p \in \mathbb{P}$ et $\alpha, \alpha_1, \dots, \alpha_r \in \mathbb{N}^*$. Combien d'éléments d'ordre p dans les groupes suivants ?

a) $\mathbb{Z}/p^\alpha\mathbb{Z}$. **b)** $\mathbb{Z}/p^{\alpha_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{\alpha_r}\mathbb{Z}$.

---

48 On pose $E = \mathbb{R} \setminus \{0,1\}$ et on note a la fonction $x \longmapsto 1-x$ et b la fonction $x \longmapsto \dfrac{1}{x}$ sur E.

1) Montrer que a et b appartiennent à S_E et calculer l'ordre de a, b et $c = ab$.

2) Montrer que $\langle a, b\rangle = \langle a, c\rangle$ et $aca^{-1} = c^{-1}$. À quel groupe usuel $\langle a, b\rangle$ est-il isomorphe ?

49

1) Soient G un groupe fini et H et K deux sous-groupes de G. On suppose que tout élément de H commute à tout élément de G.

a) Montrer que HK est un sous-groupe de G.

b) On suppose que $G = HK$ et $H \cap K = \{1_G\}$. Montrer que G est isomorphe à $H \times K$.

2) Soient $p \in \mathbb{P}$ et G un groupe fini d'ordre p^2. On a vu que G est commutatif dans un exercice précédent. Montrer que G est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou $(\mathbb{Z}/p\mathbb{Z})^2$.

3) À quels groupes parmi $\mathbb{Z}/4\mathbb{Z}$ et $(\mathbb{Z}/2\mathbb{Z})^2$ les groupes $\mathrm{U}(\mathbb{Z}/5\mathbb{Z})$ et $\mathrm{U}(\mathbb{Z}/8\mathbb{Z})$ sont-ils isomorphes ?

---

50 Soient G un groupe et $m, n \in \mathbb{N}^*$ premiers entre eux.

1) Soient $x \in G$ d'ordre m et $y \in G$ d'ordre n qui commutent.

a) Montrer que $|xy|$ divise mn, puis que :
$$x^{|xy|} = y^{-|xy|}.$$

b) En déduire que $|xy| = mn$.

2) Montrer que pour tout $z \in G$ d'ordre mn, il existe un unique $x \in G$ d'ordre m et un unique $y \in G$ d'ordre n pour lesquels $z = xy = yx$.

51

1) Montrer que tout groupe fini d'ordre pair contient un élément d'ordre 2.

À présent, soit G un groupe fini d'ordre 6.

2) On suppose par l'absurde que G ne contient pas d'élément d'ordre 3.

a) Montrer que $x^2 = 1_G$ pour tout $x \in G$, puis que G est commutatif.

b) Que vaut $\big|\langle u, v\rangle\big|$ pour tous $u, v \in G \setminus \{1_G\}$ distincts ? En déduire une contradiction.

3) D'après **1)** et **2)**, G contient un élément a d'ordre 3 et un élément b d'ordre 2.

a) Montrer que
$$G = \{1_G, a, a^{-1}, b, ab, a^{-1}b\} = \{1_G, a, a^{-1}, b, ba, ba^{-1}\}.$$

b) En déduire que G est isomorphe à $\mathbb{Z}/6\mathbb{Z}$ ou S_3. On pourra utiliser le résultat de la question **1)** de l'exercice précédent.
