EXERCICES : GROUPES, ANNEAUX, CORPS

Dans les exercices suivants $(G,.)$ *est un groupe dont l'élément neutre est noté* e.

---

1. † Soient x, y, z trois éléments de G tels que $x^3 = y^2$, $y^3 = z^2$, $z^3 = x^2$.
(a) Montrer que $x^{19} = e$, $y = x^{-8}$, $z = x^7$.
(b) On suppose que G est le groupe engendré par $\{x, y, z\}$. Montrer que G est un groupe cyclique et que, pour tout $u \in G$, $u^{19} = 1$.

---

2. Soit h une bijection du groupe G sur un ensemble G'. Indiquer comment cela permet de définir une structure de groupe sur l'ensemble G'.
Construire ainsi diverses structures de groupe sur l'ensemble $\mathbb{R}$, comme $x \star y = \sqrt[3]{x^3 + y^3}$.

---

3. On considère $\overline{\mathbb{R}} = \mathbb{R} \cup \{\infty\}$ et on pose dans cet ensemble

$$x * y = \frac{3 + xy}{x + y}.$$

Montrer que cela définit une structure de groupe commutatif, d'élément neutre ∞ (on posera $x * \infty = \lim\limits_{y \to \infty} x * y$).

---

4. † Soient H et K deux sous-groupes de G tels que $H \cup K$ soit un sous-groupe de G. Montrer que $H \subset K$ ou $K \subset H$ (raisonner par l'absurde).

---

5. † Si a est un élément de G, on note h_a l'application de G dans lui-même définie par $\forall x \in G$, $h_a(x) = axa^{-1}$. Vérifier que h_a est un automorphisme (isomorphisme dans G lui-même), et montrer que l'application $a \to h_a$ est un morphisme du groupe G dans le groupe $(\mathrm{Aut}(G), \circ)$ des automorphismes de G (Un automorphisme de la forme h_a est dit *intérieur*).

---

6. On suppose que G est un groupe fini d'ordre 4. Montrer que G est isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
Exemple : le groupe multiplicatif du corps $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$ *est un groupe d'ordre* 4*. De quel genre est-il ? Même question avec le groupe des éléments inversibles de l'anneau* $\mathbb{Z}/12\mathbb{Z}$*.*

---

7. Un exercice qui a du caractère !
On appelle *caractère* d'un groupe $(G, \star)$ tout morphisme de G dans le groupe multiplicatif $\mathbb{C}^*$, i.e. toute application $\chi : \; G \to \mathbb{C}^*$ telle que $\chi(g \star h) = \chi(g).\chi(h)$ [en particulier $\chi(e) = 1$].
a) montrer que si χ, χ' sont des caractères alors $\chi \times \chi'$ et χ^{-1} aussi. Leur ensemble $\widetilde{G}$ est donc un groupe multiplicatif [dit *groupe dual*].
b) on considère un caractère χ du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$. Montrer que χ est entièrement déterminé par la valeur $\xi = \chi(\overline{1})$, puis que ξ vérifie $\xi^n = 1$. Quels sont tous les caractères de $\mathbb{Z}/n\mathbb{Z}$? En déduire que le groupe dual $\widetilde{\mathbb{Z}/n\mathbb{Z}}$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.
c) [recherche] trouver les caractères de $(\mathbb{Z}, +)$ et reconnaître leur groupe.
d) [recherche biblio] Le groupe dual est-il toujours isomorphe au groupe de départ ?

---

8. On considère le groupe $G = (\mathbb{Z}/12\mathbb{Z}, +)$, aimé des musiciens. Montrer qu'il possède un seul sous-groupe à 4 (resp. 3) éléments, à savoir $3G = \{\dot{0}, \dot{3}, \dot{6}, \dot{9}\}$ (resp. ... à vous de trouver) et que tout élément de G s'écrit de manière unique comme somme d'un élément de chacun de ces sous-groupes, i.e. $G = 3G \oplus 4G$ (tout intervalle est somme de tierces mineures et de tierces majeures).

---

9. On considère le groupe P du pentagone régulier, composé des 5 rotations d'angles $2k\pi/5, k = 0 \ldots 4$ et des cinq symétries par rapport aux droites joignant le centre à un sommet du

pentagone (faire dessin).
Trouver tous les sous-groupes stricts de P, vérifier qu'ils sont cycliques. Et P ?

---

10. Est-ce qu'un sous-groupe d'un produit de groupes est forcément un produit de sous-groupes ?
Quel est le sous-groupe de $(\mathbb{Z}^2, +)$ engendré par $(1, 2)$ et $(2, 1)$?

---

11. Avec le théorème de LAGRANGE, ou bien en considérant l'application $x \mapsto ax$ dans $(\mathbb{Z}/p\mathbb{Z})^*$, démontrer le petit théorème de FERMAT : si p (premier) ne divise pas a, alors $a^{p-1} \equiv 1 \pmod p$.
Démontrer de façon similaire le théorème de WILSON : p est premier $\iff$ $(p-1)! \equiv -1 \pmod p$.

---

12. Il y a cinq chambres à la colonie de vacances «Taupe niveau». Des animateurs facétieux disposent, la première nuit, un certain nombre de panneaux qui indiquent : «les occupants de la chambre X... déménagent à la chambre Y. . . ». Tout le monde obtempère, les panneaux restent en place, et trois jours plus tard chacun a réintégré sa chambre initiale. Combien y avait-il de panneaux ? LE MONDE, août 98. Indication : considérer les circuits suivis par les occupants.
Généralisation : on considère une permutation de 12 éléments. Montrer que son ordre dans le groupe S_{12} est au maximum égal à 60.

---

13. On mélange un jeu de 52 cartes de la façon suivante : on sépare le jeu en deux moitiés, puis on intercale une carte de chaque paquet alternativement. Ainsi l'ordre 1 2 3 4 5 6. . . devient 27 1 28 2 29 3 . . .
a) Montrer que la $k^{\text{ème}}$ carte passe en position $2k \pmod{53}$.
b) En déduire en combien d'opérations le jeu retrouve son état initial.
c) Même étude pour le battage 1 27 2 28 3 29. . .

---

14. Ordinateur télépathe ? Expliquer ce qui se passe quand on va sur
`http : //www.k-netweb.net/projects/mindreader/`

---

15. Pourquoi la suite des chiffres décimaux de $4/9$ est-elle de période 1, alors que celle de $22/7$ est de période 6 ? Nous l'allons savoir tout à l'heure.
a) Montrer qu'un nombre $r = p/q$ dont l'écriture décimale illimitée est de période k (à partir d'un certain rang) est tel que $q \mid 10^k - 1$. On supposera (quitte à décaler la virgule) $q \wedge 10 = 1$.
b) En déduire qu'un rationnel $r = p/q$ a un développement décimal de période k, **ordre** de 10 dans le groupe multiplicatif $\mathbb{Z}/q\mathbb{Z}^*$.
c) Pour conclure, quelle est la plus grande période possible (par rapport à q) et quand-est-ce que cela se produit ? Donner les premières valeurs de q correspondantes.

---

16. Parsimonious cycles (R. Cohn, 1986)
On considère la séquence $0, 7, 14 = 2, \dots 7k, \dots, 42 = 36 + 6 = 6 \pmod{12}$ dans $\mathbb{Z}/12\mathbb{Z}$ pour k allant de 0 à 6.
Ranger ses éléments. Montrer qu'entre l'ensemble D de ces 7 valeurs et son translaté $D+7$, il y a un seul élément différent – et encore, la différence entre eux est minimale.
Plus généralement, on appelle P-cycle de raison d modulo n une séquence arithmétique de k termes telle que l'ensemble des valeurs A soit doué de la même propriété : A et $A + d$ ont $k - 1$ éléments communs, et les deux éléments non communs $a \in A \setminus (A + d)$ et $b \in (A + d) \setminus A$ vérifient $|a - b| = 1$. Montrer que si A est l'ensemble de k valeurs successives d'une progression arithmétique de raison d, c'est un P-cycle ssi $k \times d = \pm 1 \pmod n$.

Donner toutes les solutions pour $n = 12$ et $k \geqslant 2$.

Anneaux & corps

---

17. Un élément x d'un anneau commutatif A est dit *nilpotent* s'il existe un entier $n \in \mathbb{N}$ tel que $x^n = 0$. Montrer que l'ensemble des éléments nilpotents de A est un idéal.
Et si $A = \mathcal{M}_2(\mathbb{R})$?

---

18. Montrer qu'un anneau commutatif A est un corps si, et seulement si, les seuls idéaux de A sont $\{0\}$ et A. Rechercher les idéaux de $\mathcal{M}_n(\mathbb{R})$ (les sous-groupes I tq $\forall A, B\ A \times \mathcal{I} \times B \subset \mathcal{I}$) (indication : penser à la base canonique de $\mathcal{M}_n(\mathbb{R})$).

---

19. Choisissez un nombre entre 1 et 1000 ; multipliez par 9, ajoutez 4. Faites la somme des chiffres du résultat, itérez jusqu'à ce qu'il ne reste qu'un chiffre n. Choisissez un pays d'Europe dont le nom (en Français) commence par la $n^{\text{ème}}$ lettre de l'alphabet. Choisissez maintenant un fruit qui commence par la **dernière** lettre du nom de ce pays.
Prouvez qu'on trouve toujours un Kiwi (OK, il y a les Kumquats aussi mais c'est abusay).

---

20. Montrer qu'il existe un nombre de la forme $111111\ldots111$ (un **rep-unit**) divisible par 143 (ou 2021 si vous préférez).

---

21. Soit $A = \mathbb{Z}/12\mathbb{Z}$, on étudie l'ensemble $\mathcal{F}$ des applications affines de A, c'est à dire les applications $f: \ x \mapsto ax + b$ où $a, b \in A$. Quelle structure possède $\mathcal{F}$, muni des lois : $+, (+, \circ), \circ$? Quels éléments de $\mathcal{F}$ sont inversibles pour la loi $\circ$? Calculer $f^n = f \circ f \circ \ldots f$. Donner des cas (* tous) où la suite (f^n) est stationnaire.

---

22. On considère l'anneau des polynômes à deux variables $A = k[X, Y]$.
Quel est le complémentaire de l'idéal $I = (X, Y) = X.A + Y.A = \{XP(X, y) + YQ(X, Y)\}$?
Montrer que I est un idéal maximal [le seul idéal strictement plus grand est A], mais qu'il n'est pas **principal** (engendré par un seul élément).
Quels sont les idéaux de l'anneau $\mathbb{Z}/n\mathbb{Z}$? (pour cette question il est nécessaire d'avoir étudié $\mathbb{Z}/n\mathbb{Z}$).

---

23. * Dans l'anneau $A = \{a + b\, i\sqrt{5} \mid a, b \in \mathbb{Z}\}$, montrer que 3 et $2 + i\sqrt{5}$ n'ont pas de ppcm. On cherchera l'idéal des communs multiples et établira que c'est $\{3x + 3iy\sqrt{5} \mid x + y \text{ est multiple de } 3\}$.

---

24. Soit k le sous-ensemble de $\mathbb{R}$ constitué des nombres réels de la forme $a + b\sqrt{2}$, avec $a, b \in \mathbb{Q}$. Montrer que k est un sous-corps de $\mathbb{R}$.
(* un soupçon de Topologie ici. . .) montrer que tout réel est limite d'éléments de k.
Variante : quel est le plus petit anneau contenant $1, \sqrt{2}, \sqrt{3}$?

---

25. Vérifier que $A = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{R}$, puis * que ses éléments inversibles sont les $a + b\sqrt{2}$ tels que $a^2 - 2b^2 = \pm 1$ (utilisez $d = a \wedge b$). On note A^* leur groupe. Donnez plusieurs solutions de cette équation (de Pell-Fermat).
On suppose donnée une solution de $a_0^2 - 2b_0^2 = +1$, avec $a_0, b_0 \in \mathbb{N}^*$. Montrer que a_1, b_1 définis par $a_1 + b_1\sqrt{2} = (a_0 + b_0\sqrt{2})(3 - 2\sqrt{2})$ vérifient $0 < a_1, 0 \leqslant b_1 < b$ et en déduire que $a_0 + b_0\sqrt{2} = (3 + 2\sqrt{2})^n$ pour un n approprié. Conclure que A^* est engendré par $1 + \sqrt{2}$ et -1.
Application On cherche les nombres triangulaires $\frac{n(n+1)}{2}$ qui sont des carrés m^2. Montrer qu'on a alors

$$(2n + 1)^2 - 2(2m)^2 = 1 \qquad \text{et en déduire l'ensemble des solutions dans } \mathbb{N}.$$

(les plus petites solutions sont $\frac{1.2}{2} = 1^2, 36 = \frac{8.9}{2} = 6^2, 1225 = \frac{50.49}{2} = 35^2, \frac{288.289}{2} = 204^2, \dots$)

---

26. Que peut-on dire de la structure de l'ensemble $\mathbb{Q}[\pi]$ des polynômes en π, à coefficients rationnels ? Idem avec $\mathbb{Q}(\pi)$ (fractions dont les éléments sont dans $\mathbb{Q}[\pi]$).

---

27. • Polynôme minimal de $\alpha = \sqrt{2} + \sqrt{3}$ dans $\mathbb{Q}$? trouver au moins un polynôme annulateur rationnel de $\alpha = \cos 5\pi/7$, * montrer qu'il est minimal.
• Même question avec la matrice $\alpha = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ dans $\mathcal{M}_2(\mathbb{R})$. Que dire de $\mathbb{R}[\alpha]$?
• Idem en replaçant $\mathbb{R}$ par $k = \mathbb{Z}/5\mathbb{Z}$, puis $k = \mathbb{Z}/7\mathbb{Z}$. Que se passe-t-il de différent dans les deux cas ?

---

28. On considère l'ensemble $\aleph = \mathbb{N} \setminus \{0, 2\} = \{1, 3, 4, 5, \dots\}$ muni de la multiplication [Ce n'est pas un groupe, c'est un monoïde].
Vérifier que 8 est, dans $\aleph$, un nombre premier, et trouver toutes les factorisations de 64. Tout élément de $\aleph$ est-il de façon unique à l'ordre près produit de facteurs premiers ?

---

29. Prouver que l'algorithme ci-dessous calcule les coefficients de Bezout, c'est à dire qu'à la sortie on a $au + bv = r = \text{pgcd}(a, b)$. Pour cela, on vérifiera que $r = a\,u + b\,v$ est un invariant de boucle ainsi que $rp = a\,up + b\,vp$.
Tester l'algorithme avec $a = 34, b = 21$.

```
def pgcde(a, b) :
     r, u, v = a, 1, 0
    rp, up, vp = b, 0, 1
    while rp != 0 :
        q = r//rp
        rs, us, vs = r, u, v
        r, u, v = rp, up, vp
        rp, up, vp = (rs - q*rp), (us - q*up), (vs - q*vp)
    return (r, u, v)
```

Calculer le pgcd des polynômes $X^3 + X^2 + X + 1$ et $X^4 + X^2 + 1$ et donner la relation de Bezout correspondante.

---

30. Montrer que le polynôme $1 + X + X^4$ est irréductible dans $k[X]$ quand $k = \mathbb{Z}/2\mathbb{Z}$ est le corps à deux éléments.

---

31. Polynômes cyclotomiques.
On définit dans $\mathbb{C}[X]$ le polynôme $\Phi_d(X)$ par $\prod(X - \xi)$, où ξ parcourt l'ensemble des nombres complexes d'ordre exactement d : càd que $\xi^d = 1$ mais $\xi^k \neq 1$ pour tout $0 < k < d$.
a) Calculer Φ_d pour $d = 1, 2, 3, 4$.
(https : //fr.wikipedia.org/wiki/Polyn\^ome_cyclotomique).
b) Montrer la formule magique

$$\boxed{\prod_{d|n} \Phi_d(X) = X^n - 1}$$

Que dire de Φ_p pour p premier ?
c) En déduire (récurrence forte) que tous les Φ_d sont unitaires à coefficients entiers.

NB : on montre (plus difficilement) que ces polynômes sont irréductibles dans $\mathbb{Q}[X]$. On obtient ainsi des polynômes irréductibles de degré arbitrairement grand, contrairement au cas de $\mathbb{R}[X]$. En effet le degré de Φ_d n'est autre que $\varphi(d)$, où φ est la fonction d'Euler. On redémontre ainsi que $\sum_{d|n} \varphi(d) = n$.

---

32. * **Une autre formule pour la fonction d'Euler φ.**
On pose $\psi(n) = \sum_{k=1}^{n} e^{\frac{2i\pi k}{n}} \mathrm{pgcd}(n,k)$. Calculer $\psi(n)$ pour $n = 2, 3, 4, 5$.
Vérifier que ψ est *multiplicative* (si p, q sont premiers entre eux alors $\psi(p \times q) = \psi(p)\psi(q)$),
* puis que

$$\psi(p^m) = \sum_{k=1}^{p^m} 1 \times e^{2i\pi k/p^m} + \sum_{k'=1}^{p^{m-1}} (p-1) \times e^{2i\pi k' p/p^m} + \sum_{k''=1}^{p^{m-2}} (p^2-p) \times e^{2i\pi k'' p^2/p^m} + \dots (p^m - p^{m-1}) e^{2i\pi p^m/p^m} = \varphi(p^m)$$

pour p premier, et conclure que

$$\varphi(n) = \sum_{k}^{n} e^{\frac{2i\pi k}{n}} \mathrm{pgcd}(n,k) = \sum_{k}^{n} \cos\left(\frac{2\pi k}{n}\right) \mathrm{pgcd}(n,k).$$

(cette formule a été découverte seulement en 2008)

---

33. Sous-corps premier.
Soit k un corps. Montrer que l'intersection de **tous** les sous-corps de k est un sous-corps k' de k.

---

34. Montrer que si p est premier alors $p \mid \binom{p}{k}$ pour $k = 1 \dots p-1$. Réciproque ?

---

35. Entiers de GAUSS : on considère les nombres de la forme $\{a + ib \mid (a,b) \in \mathbb{Z}^2\}$. Montrer que leur ensemble A est un anneau euclidien, i.e. pour tous $z, z' \neq 0 \in A$ $\exists q, r \mid z = q z' + r$ avec $|r| < |z'|$. On montrera qu'il existe un entier de GAUSS u tel que dans $\mathbb{C}$, $|z/z' - u| \leqslant 1/\sqrt{2}$.
Par exemple, effectuer le quotient de $29 - 5i$ par $3 - 2i$.
En conséquence, dans A il existe une notion de pgcd, des éléments irréductibles, des décompositions uniques en produits de tels éléments, etc. . .
