Exercices d'Algèbre et d'Arithmétique

Yann Rotella

11 août 2023

1 TD 1 - Algèbre générale

Exercice 1. *Fonctions et lois (*).*
Une loi sur un ensemble E est vue comme une fonction de $E \times E$ dans E.

(1) Comme une loi est une fonction, rappelez les notions d'injectivité, surjectivité et bijectivité des fonctions.
(2) Dans quel cas (sur E) pouvons-nous avoir une loi bijective et dans quel cas c'est impossible ?
(3) Cominatoire facile : il y a combien de lois *différentes* sur E quand $|E| = n \in \mathbb{N}$? On pourra réfléchir à cette question en y ajoutant l'existence d'un neutre et/ou la commutativité.

Exercice 2. *Inversibilité et composition (*).*
Si x et y sont inversibles, montrez que $x \circ y$ l'est aussi et donner l'expression.

Exercice 3. *Équations dans un groupe (*).*
Montrer que si a et b sont deux éléments d'un groupe quelconque $(G, \circ)$, les équations $a \circ x = b$ et $x \circ a = b$ admettent une solution unique.

Exercice 4. *L'inversibilité est à droite et à gauche (*).*
Soit E un ensemble muni d'une loi de composition, associative, avec élément neutre et telle que tout élément possède un inverse à gauche. Montrer que tout élément possède un inverse à droite qui coïncide avec son inverse à gauche. Qu'en déduisez vous.

Exercice 5. *Le binaire est abélien ? (*).*
Soit G un groupe tel que $g^2 = e$ pour tout $g \in G$. Montrer que G est abélien.

Exercice 6. *Caractérisation des sous-groupes (**).*
Soit $(G, *)$ un groupe et H une partie de G. Montrer que H est un sous-groupe de $(G, *)$ si et seulement si H est non vide et $\forall (x, y) \in H^2, x * y^{-1} \in H$ où y^{-1} est l'inverse de y.

Exercice 7. *Intersection de sous-groupes (**).*
Soit $(G, *)$ un groupe quelconque. Montrer qu'une intersection quelconque de sous-groupes de G est encore un sous-groupe de G.

Exercice 8. *Union de sous-groupes (**).*
Soit $(G, *)$ un groupe quelconque. Montrer qu'une union de sous-groupes de G, $H \cup K$ est un sous-groupe de G si et seulement si $H \subset K$ ou $K \subset H$.

Exercice 9. *Définition des puissances (*).*
Définir proprement les puissances entières (notation multiplicative) d'éléments d'un groupe.

Exercice 10. *Exemples de groupes (*).*
On définit pour (x, y) et (x', y') dans $\mathbb{R}^* \times \mathbb{R}$ l'opération $*$ définie par

$$(x, y) * (x', y') = (xx', xy' + y)$$

— Montrer que l'ensemble $\mathbb{R}^* \times \mathbb{R}$ muni de la loi $*$ est un groupe.

— Donner une formule simple pour $(x, y)^n$ pour tout $(x, y) \in \mathbb{R}^* \times \mathbb{R}$ et tout entier naturel n.

Exercice 11. *Exemples de groupes (*).*
Les ensembles suivants munis des lois considérées sont-ils des groupes ?

1. G est l'ensemble des fonctions de $\mathbb{R}$ dans $\mathbb{R}$ définies par $x \mapsto ax + b$ avec $a \in \mathbb{R}^*$ et $b \in \mathbb{R}$, muni de la loi de composition.
2. G est l'ensemble des fonctions croissantes de $\mathbb{R}$ dans $\mathbb{R}$ muni de l'addition.
3. $G = \{f_1, f_2, f_3, f_4\}$ où

$$f_1(x) = x, f_2(x) = -x, f_3(x) = \frac{1}{x}, f_4(x) = -\frac{1}{x}$$

muni de la composition.

Exercice 12. *Exemples de sous-groupes (*).*
Dans chaque exemple suivant, on vous donne un groupe G. Dire à chaque fois si H est un sous-groupe ou non.

— $G = (\mathbb{Z}, +)$ et $H = \{\text{nombres pairs}\}$.
— $G = (\mathbb{Z}, +)$ et $H = \{\text{nombres impairs}\}$.
— $G = (\mathbb{R}, +)$ et $H = [-1, +\infty[$.
— $G = (\mathbb{R}^*, \times)$ et $H = \mathbb{Q}^*$.
— $G = (\{\text{bijections de } E \text{ dans } E\}, \circ)$ et $H = \{f \in G, f(x) = x\}$ où E est un ensemble et $x \in E$.
— $G = (\{\text{bijections de } E \text{ dans } E\}, \circ)$ et $H = \{f \in G, f(x) = y\}$ où E est un ensemble et $x, y \in E$ avec $x \neq y$.

Exercice 13. *Sous-groupe engendré par le complémentaire (**).*
Soit H un sous-groupe strict d'un groupe $(G, \cdot)$. Montrer que le sous-groupe engendré par le complémentaire ($K = \{x \in G, x \notin H\}$) de H est l'ensemble G tout entier.

Exercice 14. *Groupe des éléments inversibles (*).*
Montrer la proposition 2.

Exercice 15. *Théorème de Lagrange (***).*
Montrer le théorème de Lagrange.

Pour aller plus loin

Exercice 16. *Somme d'éléments nilpotents (**).*
Soit $(A, +\times)$ un anneau non-nul. Soient a, b deux éléments nilpotents de A. On suppose que a et b commutent. Montrez que $a + b$ est nilpotent.

Exercice 17. *Inverse de $1 - x$ (**).*
Soit x un élément nilpotent. Montrez que $1 - x$ est inversible.

Exercice 18. *Sous-groupe engendré, ordre d'un élément, groupe cyclique (***).*
Soit $(G, *)$ un groupe. On considère $(a) = \{a^m, m \in \mathbb{Z}\}$.

— Montrer que (a) est un sous-groupe de G.
— Si (a) est fini, sa cardinalité donne l'ordre de a qui est l'ordre du groupe engendré par a. De plus, quand un groupe fini est engendré par un seul élément on parle de groupe cyclique. Dans ce cas, montrez que $b = a^k$ est un générateur de G si et seulement si k et n sont premiers entre eux. Que pouvez-vous en déduire ?

Exercice 19. *Sous groupe cyclique (**).*
Soit G un groupe cyclique et soit H un sous-groupe de G. Montrer que H est cyclique.

Exercice 20. *L'anneau des matrices.*
Justifiez les propriétés de l'anneau des matrices carrées de taille 2 en utilisant les applications linéaires.

2 TD 2 - Arithmétique

Exercice 21. *Sous-anneau (*).*

1. Donner la définition d'un sous-anneau.
2. Les $n\mathbb{Z}$ sont-ils des sous-anneaux ?

Exercice 22. *Propriétés du pgcd (**).*
Montrer les propriétés du pgcd comme plus grand commun diviseur que vous connaissez.

Exercice 23. *Algorithme d'Euclide (**).*
Donner la description de l'algorithme d'Euclide, et prouver sa terminaison et son exactitude.

Exercice 24. *Équations de Bézout (*).*
Résoudre les équations suivantes

1. $4x + 6y = 2$
2. $4x + 12y = 2$
3. $221x + 247y = 15$
4. $162x + 207y = 27$

Exercice 25. *Théorème des restes chinois (***).*
Le but est de montrer le théorème des restes chinois vu en cours.

1. Montrer l'existence d'un tel x.
2. Montrer l'unicité
3. Généraliser à deux nombres non-premiers entre eux.
4. Montrer comment faire pour plus de deux équations.

Exercice 26. *Restes chinois.*
Résoudre les systèmes d'équations suivants.

1. $\begin{cases} x = 11 & \mod 17 \\ x = 5 & \mod 6 \end{cases}$
2. $\begin{cases} x = 7 & \mod 8 \\ x = 5 & \mod 9 \\ x = 6 & \mod 14 \end{cases}$
3. $\begin{cases} x = 2 & \mod 8 \\ x = 7 & \mod 9 \\ x = 8 & \mod 14 \end{cases}$

Exercice 27. *Théorème fondamental de l'arithmétique (***).*

1. Montrer que tout entier naturel $n \geq 2$ est divisible par au moins un nombre premier.
2. Montrer le théorème “décomposition en produit de facteurs premiers”.
3. Montrer que l'ensemble des nombres premiers est infini.

Exercice 28. *Calcul de l'indicatrice d'Euler (***).*

1. Quelle est la complexité de l'algorithme naif qui calcule l'indicatrice d'Euler à partir de la définition ?
2. Montrez le théorème 7.
3. Donner la valeur de l'indicatrice d'Euler pour n'importe quel entier n
4. Montrez dans quel cas $\mathbb{Z}/n\mathbb{Z}$ est un corps.

Exercice 29. *Utilisation du théorème fondamental (**).*

1. Cominatoire (quand vous aurez fait le cours) : comptez le nombre distincts de diviseurs d'un entier n quelconque en utilisant cette expression.
2. Donner une expression du pgcd de deux entiers en utilisant cette expression.

Exercice 30. *Théorème de Fermat général (***).* 1. Montrer le théorème 8.

2. Énoncez le petit théorème de Fermat.
3. Autre preuve du théorème de Fermat ?

Exercice 31. *Nombres de Fermat (*).*
Soit q un entier impair. Démontrer que pour tout $x \in \mathbb{R}$,

$$x^q + 1 = (x+1)(x^{q-1} - x^{q-2} + \cdots + 1)\,.$$

Soit $m \in \mathbb{N}^*$ tel que $2^m + 1$ soit premier. Montrer que $m = 2^n$ où n est un entier.

Exercice 32. *Nombre premier dans un intervalle (**).*
Soit $n \in \mathbb{N}$ vérifiant $10 \leq n \leq 210$. Démontrer que n est premier si et seulement si il existe un entier a relatif tel que $an = 1[210]$.

Exercice 33. *Divisibilité et carré (*).*
Soit $(a, b \in \mathbb{N}^*$ tels que a^2 divise b^2. Montrer que a divise b.

Exercice 34. *Puissances (*).* 1. Montrer qu'un entier qui est un carré et un cube est aussi un entier à la puissance 6 d'un autre entier.

2. Soient a, b, p, q, n des entiers naturels avec p et q premiers entre eux et $n = a^p = b^q$. Montrer qu'il existe un entier naturel c tel que $n = c^p q$.

Exercice 35. *Division euclidienne (*).* 1. Donner les entiers a et b avec $a < 4000$ telle que la division euclidienne de a par b donne un quotient de 82 et un reste de 47.

2. Déterminer le quotient et le reste de la division euclidienne de $2^{2013} + 562$ par 4.

Exercice 36. *Identité remarquable (*).*
Montrer que

$$x^n - y^n = (x-y)\sum_{k=0}^{n-1} x^k y^{n-1-k}\,.$$

En déduire que 23 divise $3^{3n} - 2^{3n}$.

Exercice 37. *Coefficients de Bézout (***).* 1. Expliquer comment transformer euclide en euclide étendu pour trouver les coefficients de Bézout.

2. Notez que les couples (u, v) ne sont pas uniques. Comment pouvez-vous engendrer plusieurs couples à partir d'une solution donnée ?
3. Donner une méthode itérative et récursive de la recherche des coefficients de Bézout.