TD 1 – Algèbre générale

Jules Baudrin jules.baudrin@uvsq.fr, d'après les TDs de Yann Rotella. Les exercices notés d'une étoile ★ sont particulièrement importants. Cela ne signifie pas que les autres sont optionnels.

1 Lois de composition

Exercice 1 (Fonctions et lois)**.** Une loi sur un ensemble E est 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) peut-on avoir une loi bijective et dans quel cas c'est impossible ?
3. Combinatoire facile : combien de lois peut-on construire sur E quand $|E| = n \in \mathbb{N}$?
4. (Chez vous) Combien de lois admettant un élément peut-on construire sur E ? Combien de lois commutative peut-on construire sur E ?

Exercice 2 (Inversibilité et composition)**.** Soit E un ensemble muni d'une loi $\star$ associative et pour laquelle il existe un neutre (on parle de *monoïde*). Soit x et y des éléments inversibles. Montrez que $x \star y$ est aussi inversible et donner une expression de son inverse.

Exercice 3 (L'inversibilité est à droite et à gauche)**.** Soit E un ensemble muni d'une loi $\star$ qui vérifie :

— $\star$ est associative,

— $\star$ admet un élément neutre, et

— tout élément possède un inverse à gauche.

1. Décrire mathématiquement la 3ème proposition.
2. Montrer que tout élément possède un inverse à droite et que cet inverse coïncide avec son inverse à gauche.
3. Qu'en déduisez vous ?

2 Groupes et sous-groupes

2.1 À maîtriser absolument

Exercice 4 (Équation dans un groupe)**.** Soit $(G, \star)$ un groupe. Soit $a, b \in G$. Montrer (par analyse-synthèse) que les équations $a \star x = b$ et $x \star a = b$ admettent une solution unique.

Exercice 5 (Le binaire est abélien ?)**.** Soit $(G, \star)$ un groupe qui vérifie la proposition suivante :

$$\forall g \in G, \quad g^2 = e\,.$$

1. Montrer que $(G, \star)$ est abélien.
2. Donner un exemple d'un tel groupe.

Exercice 6 (Caractérisation des sous-groupes ★)**.** Soit $(G, \star)$ un groupe et H un sous-ensemble de G. Montrer que les propositions suivantes sont équivalentes :

— $(H, \star)$ est un sous-groupe de $(G, \star)$.

— H est non vide et $\forall (x, y) \in H^2, x \star y^{-1} \in H$ où y^{-1} est l'inverse de y dans G.

Exercice 7 (Intersection de sous-groupes ★)**.** Soit $(G, \star)$ un groupe.

1. Montrer qu'une intersection quelconque de sous-groupes de G est encore un sous-groupe de G.

2. Soit S un sous-ensemble de G. Montrer que $\bigcap_{\substack{H<G \\ S\subset H}} H$ est le plus petit sous-groupe de G qui contient S.
NB : Ce sous-groupe est appelé le *sous-groupe engendré* par S.

Exercice 8 (Union de sous-groupes ★)**.** Soit $(G, \star)$ un groupe quelconque.

1. Montrer qu'une union de deux sous-groupes de G, $H \cup K$ est un sous-groupe de G si et seulement si $H \subset K$ ou $K \subset H$.

2. Soit $(H_n)_{n\in\mathbb{N}}$ une famille de sous-groupes de G tel que : $\forall n \in \mathbb{N}, \quad H_n \subset H_{n+1}$. Montrer que $\bigcup_{n\in\mathbb{N}} H_n$ est un sous-groupe.

Exercice 9 (Un autre groupe)**.** On définit pour (x, y) et (x', y') dans $\mathbb{R}^* \times \mathbb{R}$ la loi $\star$ définie par

$$(x, y) \star (x', y') = (xx', xy' + y)$$

1. Montrer que l'ensemble $(\mathbb{R}^* \times \mathbb{R}, \star)$.

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

Exercice 10. Les ensembles suivants sont-ils des groupes pour la loi de composition de fonctions $\circ$?

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 $b \in \mathbb{R}$.

2. G est l'ensemble des fonctions croissantes de $\mathbb{R}$ dans $\mathbb{R}$.

3. $G = \{f_1, f_2, f_3, f_4\}$ où

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

Exercice 11 (Exemples de sous-groupes)**.** Dans chaque exemple suivant, on considère un groupe $(G, \star)$ et un sous-ensemble $H \subset G$. $(H, \star)$ est-il un sous-groupe de $(G, \star)$?

1. $G = (\mathbb{Z}, +)$ et $H = \{\text{nombres pairs}\}$.

2. $G = (\mathbb{Z}, +)$ et $H = \{\text{nombres impairs}\}$.

3. $G = (\mathbb{R}, +)$ et $H = [-1, +\infty[$.

4. $G = (\mathbb{R}^*, \times)$ et $H = \mathbb{Q}^*$.

5. $G = (\{\text{bijections de } E \text{ dans } E\}, \circ)$ et $H = \{f \in G, f(x) = x\}$ où E est un ensemble et $x \in E$.

6. $G = (\{\text{bijections de } E \text{ dans } E\}, \circ)$ et $H = \{f \in G, f(x) = y\}$ où E est un ensemble et $x, y \in E$ avec $x \neq y$.

3 Des résultats fondamentaux

Exercice 12 (Groupe des éléments inversibles ★)**.** Soit $(A, +, \times)$ un anneau. Soit $A^\times$ l'ensemble défini par :

$$A^\times \stackrel{\text{def}}{=} \{a \in A \mid a \text{ est inversible pour } \times\} .$$

Montrer que $(A, \times)$ est un groupe.

Exercice 13 (Théorème de Lagrange ★)**.** Rappel : une *partition d'un ensemble* E est une famille de sous-ensembles $(H_i)_{i\in I}$ qui vérifie les propriétés suivantes :

— Chaque H_i est non-vide : $\forall i \in I, \quad H_i \neq \emptyset$.

— Les H_i recouvrent E : $\bigcup_{i\in I} H_i = E$.

— Les H_i distincts ne s'intersectent pas : $\forall i, j \in I, \quad H_i \neq H_j \implies H_i \cap H_j = \emptyset$.

Soit $(G, \star)$ un groupe fini et H un sous-groupe de G. On cherche à démontrer le théorème de Lagrange.

1. On considère la famille suivante $(gH)_{g\in G}$ où pour tout $g \in G$, gH est défini par $gH \stackrel{\text{def}}{=} \{gh \mid h \in H\}$. Montrer que cette famille forme une partition de E.
2. Montrer que pour tout $g \in G$, $|gH| = |H|$.
3. En déduire que $|H|$ est un diviseur de $|G|$.

4 Exercices supplémentaires

Exercice 14 (Centre d'un groupe)**.** Soit $(G, \star)$ un groupe. Soit $Z(G)$ le sous-ensemble de G défini par :

$$Z(G) \stackrel{\text{def}}{=} \{g \in G \mid \forall h \in G, gh = hg\} .$$

1. Montrer que $Z(G)$ est un sous-groupe de G.
   NB : Ce sous-groupe est le *centre de* G (La notation Z vient de l'allemand Zentrum).
2. (***) On suppose que G admet un unique élément d'ordre 2. Montrer que cet élément appartient à $Z(G)$.

Exercice 15 (Produit de sous-groupes)**.** Soit $(G, \star)$ un groupe. Soit H, K deux sous-groupes de G. On considère le produit de H et K défini par :

$$HK \stackrel{\text{def}}{=} \{hk, h \in H, k \in K\} \subset G .$$

Montrer que HK est un sous-groupe si et seulement si $HK = KH$.

Exercice 16 (Définition des puissances)**.** Définir proprement les puissances entières (notation multiplicative) d'éléments d'un groupe.

Exercice 17 (Sous-groupe engendré par le complémentaire)**.** Soit H un sous-groupe strict d'un groupe $(G, \star)$. Montrer que le sous-groupe engendré par le complémentaire de H, c'est-à-dire par l'ensemble $S = \{x \in G, x \notin H\}$, est le groupe G tout entier.

Exercice 18 (Encore des partitions...)**.** Soit E un ensemble et $\sim$ une relation d'équivalence sur E. Pour tout $x \in E$, on rappelle que la *classe d'équivalence* de x (pour la relation $\sim$) est l'ensemble défini par $\overline{x} \coloneqq \{y \in E \mid x \sim y\}$.

1. Soit $x \in E$, et $y \in \overline{x}$. Montrer que $\overline{x} = \overline{y}$.
2. Montrer que la famille $(\overline{x})_{x\in E}$ forme une partition de E.
3. (**) Reprendre l'Exercice 13 et trouver une relation d'équivalence telle que pour tout $g \in G$, $\overline{g} = gH$.
4. (**) Soit G un groupe d'ordre pair. En considérant la relation « est l'inverse de », montrer qu'il existe un élément $g \in G$ tel que $g \neq e$ et $g = g^{-1}$.

5 Pour aller encore plus loin

Exercice 19 (Sous-groupe cyclique)**.** Soit $(G, \star)$ un groupe cyclique, c'est-à-dire un groupe pour lequel qu'il existe $g \in G$ tel que $G = \left\{g^k \mid k \in \mathbb{Z}\right\}$. Soit H un sous-groupe de G. Montrer que H est cyclique.

Exercice 20 (Sous-groupe engendré, ordre d'un élément, groupe cyclique)**.** Soit $(G, \star)$ un groupe. On considère $\langle a \rangle \stackrel{\text{def}}{=} \{a^m, m \in \mathbb{Z}\}$.

1. Montrer que $\langle a \rangle$ est un sous-groupe de G.
2. On suppose que $\langle a \rangle$ est fini d'ordre n. Dans ce cas, $n = |\langle a \rangle| = o(a)$ où $o(a)$ est l'ordre de a, c'est-à-dire la plus petite puissance $k \geq 1$ tel que $a^k = e$. Montrer que $b = a^k$ est un générateur de G si et seulement si k et n sont premiers entre eux.
3. Que peut-on en déduire ?

Exercice 21 (Sous-groupe non trivial d'un groupe infini.)**.** Soit $(G, \star)$ un groupe.

1. Soit $g \in G$. Montrer que $\langle g^2 \rangle \subset \langle g \rangle$.
2. On suppose que G est un groupe infini. En considérant un élément $g \in G$ non nul, montrer que G possède un sous-groupe non trivial, c'est-à-dire un sous-groupe H tel que $H \neq \{e\}$ et $H \neq G$.

Exercice 22 (Somme d'éléments nilpotents)**.** Soit $(A, +, \times)$ un anneau non-nul. Soit a, b deux éléments nilpotents de A. On suppose que a et b commutent. Montrer que $a + b$ est nilpotent.

Exercice 23 (Inverse de $1 - x$)**.** Soit$(A, +, \times)$ un anneau. Soit $x \in A$ un élément nilpotent. Montrer que $1 - x$ est inversible.

Exercice 24 (L'anneau des matrices)**.** Montrer que l'ensemble des matrices carrées de taille 2 est un anneau (muni de l'addition et la multiplication adéquate) en s'appuyant sur les applications linéaires.

TD 2 – Arithmétique

1 Un exercice sur les anneaux

Exercice 1 (Sous-anneau)**.** **1.** Donner la définition d'un sous-anneau.

2. Les $n\mathbb{Z}$ sont-ils des sous-anneaux ?

2 PGCD et algorithme d'Euclide

Exercice 2 (Propriétés du pgcd)**.** Lister les propriétés du pgcd que vous connaissez et montrer-les en utilisant la définition du PGCD vue en cours.

Exercice 3 (Algorithme d'Euclide ★)**.** Prouver la terminaison et l'exactitude de l'algorithme d'Euclide.

Exercice 4 (Identité de Bézout ★)**.**

1. Expliquer comment transformer l'algorithme d'Euclide en algorithme *étendu* afin de trouver une identité de Bézout.

2. Il faut noter que les solutions (u, v) à une équation $au + bv = c$ ne sont pas uniques. Comment faire pour engendrer d'autres solutions à partir d'une solution particulière (u_0, v_0) ?

3. Donner une méthode itérative et récursive de la recherche des coefficients de Bézout.

Exercice 5 (Équations de Bézout ★)**.** Pour chaque équation trouver, lorsque c'est possible, une solution particulière puis l'ensemble des solutions dans $\mathbb{Z} \times \mathbb{Z}$.

1. $4x + 6y = 2$.

2. $4x + 12y = 2$.

3. $221x + 247y = 15$.

4. $162x + 207y = 27$.

3 Théorème de Sun Zi (dit « des restes chinois »)

Exercice 6 (Preuve du théorème)**.** Le but est de montrer le théorème de Sun Zi vu en cours. On considère donc le système d'équation $x = a \bmod n, x = b \bmod m$ où n et m sont premiers entre eux.

1. Montrer que si elle existe, une solution est nécessairement unique modulo nm.

2. Déterminer une solution x à ce système.

3. Montrer comment faire pour plus de deux équations.

Exercice 7 (Système linéaire d'équations modulaires ★)**.** Pour chaque système trouver, lorsque c'est possible, une solution particulière puis l'ensemble des solutions dans $\mathbb{Z}$.

1. $\begin{cases} x = 11 & \bmod 17 \\ x = 5 & \bmod 6 \end{cases}$

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

3. $\begin{cases} x = 2 & \mod 8 \\ x = 7 & \mod 9 \\ x = 8 & \mod 14 \end{cases}$

4 D'autres théorèmes d'arithmétique

Exercice 8 (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 de « décomposition en produit de facteurs premiers ».
3. Montrer que l'ensemble des nombres premiers est infini.

Exercice 9 (Calcul de l'indicatrice d'Euler ★)**.**

1. Quelle est la complexité de l'algorithme naif qui calcule l'indicatrice d'Euler à partir de sa définition ?
2. Montrer les formules de calculs de φ vue en cours.
3. Donner une formule générale pour $\varphi(n)$ lorsque la décomposition de n en facteurs premiers est connue.
4. Montrer dans quel cas $\mathbb{Z}/n\mathbb{Z}$ est un corps.

Exercice 10 (Utilisation du théorème fondamental)**.**

1. (Combinatoire) Exprimer le nombre de diviseurs distincts d'un entier n quelconque en utilisant sa décomposition en produit de nombre premiers.
2. Donner une expression du pgcd de deux entiers en utilisant cette expression.

Exercice 11 (Théorème d'Euler-Fermat)**.**

1. Montrer le théorème d'Euler-Fermat.
2. Énoncer le petit théorème de Fermat et déduire une autre preuve de ce théorème.

5 Pour aller plus loin

Exercice 12 (Une fonction et une équation sur un groupe...)**.** Soit G un groupe fini et m un entier premier à $|G|$. On considère la fonction $f : G \to G, g \mapsto g^m$.

1. En utilisant les théorèmes de Bézout et de Lagrange, montrer que f est bijective.
2. Soit $a \in G$. En déduire que l'équation $x^m = a$ admet une unique solution.

Exercice 13 (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 14 (Divisibilité et carré)**.** Soit $a, b \in \mathbb{N}^*$ tels que a^2 divise b^2. Montrer que a divise b.

Exercice 15 (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 16 (Identité remarquable)**.** Soit $x, y \in \mathbb{R}$. Montrer que

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

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