MAT35B - L3A ALGÈBRE
Premier semestre — 2022-2023
Fiche 1: Relations d'équivalence

1. Soit f une application d'un ensemble E dans lui-même. Pour tout entier naturel n, on note f^n la composée $f \circ \cdots \circ f$ (n facteurs), avec la convention $f^0 = \mathrm{id}_E$.

(a) Montrer qu'on définit une relation d'équivalence $\sim$ sur E en posant $x \sim y$ si et seulement s'il existe $(p, q) \in \mathbb{N}^2$ tel que $f^p(x) = f^q(y)$.

(b) Dans le cas où f est bijective, décrire la classe d'équivalence $[x]$ de $x \in E$, appelée **orbite** de x suivant f. À quelle condition cette orbite est-elle finie ?

2. Soit G un groupe et H un sous-groupe de G.

(a) Montrer que l'on définit une relation d'équivalence sur G par $g_1 \sim_H g_2$ si et seulement si $g_1^{-1}g_2 \in H$, pour tous $g_1, g_2 \in G$.

(b) Les classes d'équivalences sont appelées les **classes à gauche modulo** H. Les décrire et montrer qu'elles sont toutes en bijection avec H.

(c) L'ensemble quotient pour cette relation d'équivalence est noté G/H. Lorsque G est un groupe fini, montrer que $|G/H| = |G|/|H|$.

3. Soit n un entier strictement positif. Comme $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$, on obtient une relation d'équivalence sur $\mathbb{Z}$ en posant $a \sim b$ si et seulement si $b - a \in n\mathbb{Z}$, pour tous $a, b \in \mathbb{Z}$.

(a) Montrer que sur l'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$, on peut définir une addition et une multiplication par

$$\bar{a} + \bar{b} = \overline{a+b} \text{ et } \bar{a} \cdot \bar{b} = \overline{a \cdot b}$$

pour tous $a, b \in \mathbb{Z}$.

(b) Montrer que $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau commutatif.

(c) Quel est l'ordre du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$?

(d) Montrer que les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ pour la loi $\cdot$ sont les classes des entiers premiers avec n. On note $(\mathbb{Z}/n\mathbb{Z})^\times$ l'ensemble de ces inversibles.

(e) Montrer que $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$ est un groupe. L'ordre de ce groupe est donc la fonction φ de $\mathbb{N}^*$ dans lui-même donnée par

$$\varphi(n) = \left|\left(\mathbb{Z}/n\mathbb{Z}\right)^\times\right| = \left|\left\{k \in [\![0, n-1]\!] : \mathsf{PGCD}(k, n) = 1\right\}\right|,$$

appelée l'**indicateur d'Euler**.

(f) Montrer que l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est nul (*i.e.*, réduit à $\{\bar{0}\}$) si $n = 1$, un corps si n est premier, et non-intègre (*i.e.*, le produit de deux éléments non nuls peut être nul) si n est composé.

4. Soit $f : E \to F$ une application.

(a) Montrer que l'on définit une relation d'équivalence sur E par $x_1 \sim_f x_2$ si et seulement si $f(x_1) = f(x_2)$ pour tous $x_1, x_2 \in E$ et décrire les classes d'équivalences.

(*b*) On note $E/\sim_f$ l'ensemble quotient et p la projection canonique de E sur $E/\sim_f$. Montrer qu'il existe une unique application $\bar{f} : E/\sim_f \to F$ telle que $f = \bar{f} \circ p$ et que cette application $\bar{f}$ est injective.

(*c*) On suppose maintenant que $f : G \to G'$ est un morphisme de groupes et on note p la projection de G sur l'ensemble quotient $G/\mathsf{Ker}(f)$. Montrer alors que $g_1 \sim_f g_2$ si et seulement si $g_1^{-1}g_2 \in \mathsf{Ker}(f)$ pour tous $g_1, g_2 \in G$. En déduire que les classes d'équivalence pour la relation $\sim_f$ sont les classes à gauche modulo $\mathsf{Ker}(f)$ et qu'il existe une application injective $\bar{f} : G/\mathsf{Ker}(f) \to G'$ telle que $f = \bar{f} \circ p$.

(*d*) Appliquer ce résultat à l'application $f : \mathbb{R} \to \mathbb{C}^*$ définie par $f(t) = e^{it}$.

5. Soient G un groupe, H et K deux sous-groupes de G et $f : H \times K \to G$ l'application donnée par $f(h,k) = hk$. Soit $HK = f(H \times K)$ l'ensemble image de l'application f.

(*a*) Montrer que chaque classe d'équivalence pour $\sim_f$ est en bijection avec $H \cap K$.

(*b*) En déduire que $|H \times K| = |HK||H \cap K|$.

6. Soit $f : E \to F$ une application, $\sim$ une relation d'équivalence sur E et p la projection de E sur l'ensemble quotient $E/\sim$.

(a) À quelle condition portant sur f et $\sim$ existe-t-il une application $\bar{f} : E/\sim \to F$ telle que $f = \bar{f} \circ p$? Montrer qu'une telle application est unique si elle existe, ce qui légitime la notation $\bar{f}$.

(b) Expliciter la condition précédente sur f lorsque $E = F = \mathbb{R}$ et $\sim$ est la relation d'équivalence :

(i) $\sim_g$ associée à la fonction g donnée par $g(x) = |x|$ pour $x \in \mathbb{R}$;

(ii) $\sim_H$ associée au sous-groupe $H = a\mathbb{Z}$ de E, avec $a > 0$.

(c) On revient au cas général et on suppose que $\bar{f}$ existe. Montrer que $\bar{f}$ a même image que f. Montrer que $\bar{f}$ est injective si et seulement si les relations $\sim$ et $\sim_f$ coïncident.

7. Soit $f : G \to G'$ un morphisme de groupes et H un sous-groupe de G. Soit $p : G \to G/H$ la projection de G sur l'ensemble des classes à gauche modulo H.

(a) Montrer qu'il existe une application $\bar{f} : G/H \to G'$ telle que $f = \bar{f} \circ p$ si et seulement si $H \subseteq \mathsf{Ker}(f)$.

(b) À quelle condition $\bar{f}$ est-elle injective ?

8. Soit K un corps. On pose $E = K^2 \setminus \{(0,0)\}$. On munit E de la relation $\sim$ définie par $v_1 \sim v_2$ si et seulement s'il existe $\alpha \in K^*$ tel que $v_1 = \alpha v_2$.

(a) Montrer que $\sim$ est une relation d'équivalence sur E. Pour $v \in E$, quelle est la classe d'équivalence de v ? On note p la projection canonique de E sur $E/\sim$. On appelle **droite projective sur** K, notée $\mathbb{P}^1(K)$, l'ensemble quotient $E/\sim$.

(b) Montrer que l'application $f : E \to K \sqcup \{\infty\}$ définie par $f(x,y) = x/y$ si $y \neq 0$ et $f(x,y) = \infty$ si $x \neq 0$ et $y = 0$ passe au quotient et induit une bijection $\bar{f}$ de $E/\sim$ vers $K \sqcup \{\infty\}$.

(c) On considère l'application

$$g : \mathsf{GL}_2(K) \to \mathsf{GL}(K^2)$$

qui associe à toute matrice inversible $M \in \mathsf{GL}_2(K)$ l'application linéaire inversible $g_M \in \mathsf{GL}(K^2)$ de matrice M dans la base canonique. Montrer que g est un isomorphisme de groupes. Noter que l'automorphisme g_M induit une permutation $g_M|_E$ sur l'ensemble $E = K^2 \setminus \{(0,0)\}$.

(d) Montrer que, étant donné $\phi \in \mathsf{GL}(K^2)$, il existe une unique application

$$\hat{\phi} : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$$

telle que $\hat{\phi} \circ p = p \circ \phi|_E$. Montrer en plus que $\hat{\phi}$ est bijective et que l'application

$$\wp : \mathsf{GL}(K^2) \to \mathsf{Aut}_{\mathsf{Ens}}(\mathbb{P}^1(K))$$

qui associe $\hat{\phi}$ à ϕ est un morphisme de groupes.

(e) Soient X et Y deux ensembles et $f : X \to Y$ une application bijective. Montrer que l'application

$$\mathsf{Ad}_f : \mathsf{Aut}_{\mathsf{Ens}}(X) \to \mathsf{Aut}_{\mathsf{Ens}}(Y)$$

donnée par $\mathsf{Ad}_f(\phi) = f \circ \phi \circ f^{-1}$ est un isomorphisme de groupes. En déduire que l'application $h_M = \bar{f} \circ \hat{g}_M \circ \bar{f}^{-1}$ est une permutation de $K \sqcup \{\infty\}$ et que l'application $h = \mathsf{Ad}_{\bar{f}} \circ \wp \circ g$, qui associe h_M à M, est un morphisme de $\mathsf{GL}_2(K)$ dans le groupe $\mathsf{Aut}_{\mathsf{Ens}}(K \sqcup \{\infty\})$ des permutations de $K \sqcup \{\infty\}$.

(f) Expliciter le noyau de h. En déduire que l'image de h, le **groupe des homographies**, est isomorphe au groupe projectif linéaire $\mathsf{PGL}_2(K) = \mathsf{GL}_2(K)/(K^* I_2)$, où I_2 dénote la matrice unitaire de $M_2(K)$.

(g) Désormais, on fixe $M \in \mathsf{GL}_2(K)$ et on pose

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Pour $z \in K \sqcup \{\infty\}$, exprimer $h_M(z)$ en fonction de z et des coefficients de M. Calculer en particulier $h_M(\infty)$, $h_M(0)$ et $h_M(-d/c)$. Donner la formule générale pour $h_M^{-1}(z)$.

(h) Soit $(x, y) \in E$. Montrer que (x, y) est un vecteur propre de g_M si et seulement si $f(x, y)$ est un point fixe de h_M. À quelle condition sur les coefficients de M

(i) ∞ est-il point fixe de h_M ?

(ii) ∞ est-il le seul point fixe de h_M ?

(iii) 0 est-il point fixe de h_M ?

(i) On suppose dans cette question que $K = \mathbb{C}$ et que ∞ n'est pas point fixe de h_M. Soit $(z_n)_{n\in\mathbb{N}} \in \mathbb{C}^{\mathbb{N}}$ une suite vérifiant la relation de récurrence $z_{n+1} = h_M(z_n)$. Montrer que l'on est dans une des deux situations suivantes :

(H.1) h_M a exactement deux points fixes distincts r_- et r_+ dans K, la matrice

$$P = \begin{pmatrix} r_- & r_+ \\ 1 & 1 \end{pmatrix}$$

est inversible, la matrice $P^{-1}MP$ est diagonale et la suite

$$(w_n)_{n\in\mathbb{N}} = \left(h_{P^{-1}}(z_n)\right)_{n\in\mathbb{N}}$$

est géométrique ;

(H.2) h_M a un seul point fixe r_0 dans K, la matrice

$$P = \begin{pmatrix} r_0 & 1 \\ 1 & 0 \end{pmatrix}$$

est inversible, $P^{-1}MP$ est triangulaire avec ses deux coefficients diagonaux égaux et la suite $(w_n)_{n\in\mathbb{N}} = (h_{P^{-1}}(z_n))_{n\in\mathbb{N}}$ est arithmétique.

(j) Donner l'expression du terme général de la suite $(z_n)_{n\in\mathbb{N}}$ donnée par $z_0 = 0$ et $z_{n+1} = (2z_n + 3)/(z_n + 4)$ pour tout $n \in \mathbb{N}$.