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 ?

Solution.

(*a*) C'est clair que $\sim$ est réflexive, car $x = f^0(x) = f^0(x) = x$ pour tout $x \in E$. En plus, $\sim$ est symétrique, car étant donné $x, y \in E$ tels que $x \sim y$, il existe $(p,q) \in \mathbb{N}^2$ tel que $f^p(x) = f^q(y)$, ce qui nous dit que $y \sim x$, vu que $f^q(y) = f^p(x)$. Enfin, $\sim$ est transitive, car, étant donné $x, y, z \in E$ tels que $x \sim y$ et $y \sim z$, il existe $(p,q) \in \mathbb{N}^2$ et $(r,s) \in \mathbb{N}^2$ tels que $f^p(x) = f^q(y)$ et $f^r(y) = f^s(z)$, ce qui nous dit que $x \sim z$, vu que $f^{(p+r)}(x) = f^{(q+r)}(y) = f^{(s+p)}(z)$.

(*b*) On affirme que

$$[x] = \{f^k(x) : k \in \mathbb{Z}\}, \tag{1}$$

où $f^k(x) = (f^{-1})^{-k}(x)$, pour $-k \in \mathbb{N}$. En effet, pour démontrer $[x] \subseteq \{f^k(x) : k \in \mathbb{Z}\}$, on remarque que $x \sim y$ avec $y = f^k(x)$ pour $k \in \mathbb{Z}$, car $f^k(x) = f^0(y)$ si $k \geq 0$ et $f^0(x) = f^k(y)$ si $k \leq 0$. En outre, $[x] \supseteq \{f^k(x) : k \in \mathbb{Z}\}$ suit du fait que, si $x \sim z$ avec $z \in E$, alors il existe $(p,q) \in \mathbb{N}^2$ tel que $f^p(x) = f^q(z)$, ce qui implique que $z = f^{(p-q)}(x)$.

Enfin, on affirme que $[x]$ est fini si et seulement s'il existe $N \in \mathbb{N}^*$ tel que $f^N(x) = x$. En effet, (1) nous dit que si $[x]$ est fini, alors il existe $p, q \in \mathbb{Z}$ différents tels que $f^p(x) = f^q(x)$. On suppose dans perte de généralité que $p > q$. En conséquence, $f^{(p-q)}(x) = x$, *i.e.* on prend $N = p - q$. Réciproquement, s'il existe $N \in \mathbb{N}^*$ tel que $f^N(x) = x$, alors $f^{r+mN}(x) = f^r(x)$ pour tout $m \in \mathbb{Z}$ et $r \in [\![0, N-1]\!]$, ce qui implique que $[x] = \{f^k(x) : k \in \mathbb{Z}\} = \{f^k(x) : k \in [\![0, N-1]\!]\}$ est fini.

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 $|G/H| = |G|/|H|$.

Solution.

(*a*) On voit bien que $\sim_H$ est réflexive, *i.e.* $g \sim_H g$ pour tout $g \in G$, car $1_G = g^{-1}g \in H$, vu que H est un sous-groupe. En plus, $\sim_H$ est symétrique, *i.e.* $g \sim_H g'$ implique $g' \sim_H g$ pour tous $g, g' \in G$, car $g^{-1}g' \in H$ implique que $g'^{-1}g = (g^{-1}g')^{-1} \in H$, vu que H est un sous-groupe. Enfin, $\sim_H$ est transitive, *i.e.* $g \sim_H g'$ et $g' \sim_H g''$ implique $g \sim_H g''$ pour tous $g, g', g'' \in G$, car $g^{-1}g' \in H$ et $g'^{-1}g'' \in H$ impliquent que $g^{-1}g'' = g^{-1}g'g'^{-1}g'' \in H$, vu que H est un sous-groupe.

(*b*) Étant donné $g \in G$, on définit

$$\phi_g : H \to [g]$$

via $\phi_g(h) = gh$ pour $h \in H$. L'application précédente est bien définie car $g \sim_H \phi_g(h)$ pour tout $h \in H$, vu que $g^{-1}\phi_g(h) = g^{-1}gh = h \in H$. On affirme que ϕ_g est bijectif. En effet, ϕ_g est injectif, car $\phi_g(h) = \phi_g(h')$ pour $h, h' \in H$, *i.e.* $gh = gh'$, implique $h = g^{-1}gh = g^{-1}gh' = h'$. En outre, ϕ_g est surjectif, car étant donné $g' \in G$ tel que $g \sim_H g'$, *i.e.* $g^{-1}g' \in H$, $\phi_g(g^{-1}g') = gg^{-1}g' = g'$.

(*c*) Soit $s : G/H \to G$ une **section** de la projection canonique $p : G \to G/H$, *i.e.* $p \circ s = \mathrm{id}_{G/H}$, qui existe grâce à l'axiome du choix. Noter que s est injectif. On définit l'application

$$\phi_s : H \times G/H \to G$$

via $\phi_s(h, x) = s(x)(h)$, pour $h \in H$ et $x \in G/H$. On affirme que ϕ_s est bijectif. En effet, ϕ_s est injectif, car $\phi_s(h, x) = \phi_s(h', x')$ pour $h, h' \in H$ et $x, x' \in G/H$, *i.e.* $s(x)h = s(x')h'$, implique $x = p(s(x)h) = p(s(x')h') = x'$, ce qui nous dit en plus $s(x)h = s(x)h'$, qui implique $h = h'$. En outre, ϕ_s est surjectif, car étant donné $g \in G$, on a $p(g) = p(s(p(g)))$, ce qui implique que $p(g) \sim_H s(p(g))$, et $g = \phi_s(p(g)^{-1}s(p(g)), p(g))$. En conséquence, $|G/H|.|H| = |G|$, ce qui implique que $|G/H| = |G|/|H|$ lorsque G est un groupe fini.

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

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

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.

Solution.

(*a*) Il suffit de montrer que si $a, a', b, b' \in \mathbb{Z}$ satisfont que $n|(a-a')$ et $n|(b-b')$, alors

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

i.e.

$$n|\big((a+b)-(a'+b')\big) \text{ et } n|\big((a\cdot b)-(a'\cdot b')\big).$$

Ces derniers identités sont immédiates vu que $(a+b)-(a'+b') = (a-a')+(b-b')$ et $(a\cdot b)-(a'\cdot b') = (a-a')\cdot b + a'\cdot(b-b')$.

(*b*) On laisse au lecteur la vérification immédiate.

(*c*) On considère l'application $\iota : [\![0, n-1]\!] \to \mathbb{Z}/n\mathbb{Z}$ donnée par la composition de l'inclusion $[\![0, n-1]\!] \to \mathbb{Z}$ et de la projection canonique $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. On affirme que ι est bijectif. D'ailleurs, ι est injectif, car $\iota(k) = \iota(k')$, pour $k, k' \in [\![0, n-1]\!]$, implique $n|(k-k')$, ce qui nous dit que $k = k'$, car $|k-k'| < n$. En outre, ι est surjectif, car étant donné $m \in \mathbb{Z}$, il existe $(q, r) \in \mathbb{Z} \times [\![0, n-1]\!]$ unique tel que $m = qn + r$, ce qui nous dit que $\iota(r) = \bar{m}$. On conclut que l'ordre de $(\mathbb{Z}/n\mathbb{Z}, +)$ est n.

(*d*) Soit $m \in \mathbb{Z}$. On affirme que $\bar{m} \in \mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement si m et n sont premiers entre eux. En effet, $\bar{m} \in \mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement s'il existe $k \in \mathbb{Z}$ tel que $\bar{k}\cdot\bar{m} = \bar{1}$, *i.e.* $n|(km-1)$, ce qui équivaut à l'existence de $\ell \in \mathbb{Z}$ tel que $\ell n + km = 1$, *i.e.* m et n sont premiers entre eux.

(*e*) On affirme que si $(A, +, \cdot)$ est un anneau commutatif (avec unité), alors

$$A^\times = \{a \in A : \text{ il existe } b \in A \text{ tel que } b\cdot a = 1_A\}$$

est un groupe pour $\cdot$. En effet, c'est clair que $a\cdot a' \in A$ si $a, a' \in A^\times$, car dans ce cas $b\cdot a = b'\cdot a' = 1_A$, ce qui nous dit que $b\cdot b'\cdot a\cdot a' = b\cdot a\cdot b'\cdot a' = 1_A$. En plus, on voit bien que $1_A \in A^\times$ et 1_A est l'unité de $A^\times$ pour $\cdot$. Enfin, si $a \in A^\times$, il existe $b \in A$ tel que $b\cdot a = 1_A$, ce qui nous dit que $b \in A^\times$ est l'inverse de a.

(*f*) On voit bien $|\mathbb{Z}/n\mathbb{Z}| = 1$ si $n = 1$, ce qui nous dit que $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est nul. Si n est premier, alors l'item (d) nous dit que $(\mathbb{Z}/n\mathbb{Z})^\times = \mathbb{Z}/n\mathbb{Z} \setminus \{\bar{0}\}$, *i.e.* $\mathbb{Z}/n\mathbb{Z}$ est un corps. Enfin, si $n = pq$ avec $p, q \in \mathbb{N}^*$ et $p, q > 1$, on voit bien que $\bar{p}, \bar{q} \neq \bar{0}$ mais $\bar{0} = \bar{n} = \bar{p}\cdot\bar{q}$ *i.e.* $\mathbb{Z}/n\mathbb{Z}$ est non-intègre.

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 $f(t) = e^{it}$.

Solution.

(*a*) On voit vien que $\sim_f$ est réflexive car $x \sim_f x$ équivaut à $f(x) = f(x)$. En outre, $\sim_f$ est symétrique, car $x \sim_f y$ pour $x, y \in E$ équivaut à $f(x) = f(y)$, ce qui implique $y \sim_f x$. Enfin, $\sim_f$ est transitive, car $x \sim_f y$ et $y \sim_f z$ pour $x, y, z \in E$ équivalent à $f(x) = f(y)$ et $f(y) = f(z)$, ce qui implique $f(x) = f(z)$, *i.e.* $x \sim_f z$.
En plus, c'est clair que $[x] = f^{-1}(f(x))$, pour tout $x \in E$.

(*b*) On définit l'application $\bar{f} : E/\sim_f \to F$ via $\bar{f}([x]) = f(x)$, pour $x \in E$. Cette application est bien définie car $x \sim_f y$ implique $f(x) = f(y)$. Par définition, $f = \bar{f} \circ p$. L'unicité de $\bar{f}$ suit de la surjectivité de p. Enfin, si $\bar{f}([x]) = \bar{f}([y])$, *i.e.* $f(x) = f(y)$, implique $x \sim_f y$, *i.e.* $[x] = [y]$, ce qui nous dit que $\bar{f}$ est injectif.

(*c*) On voit bien que $g_1 \sim_f g_2$, *i.e.* $f(g_1) = f(g_2)$, équivaut à $f(g_1^{-1} g_2) = 1_{G'}$, *i.e.* $g_1^{-1} g_2 \in \mathsf{Ker}(f)$. En conséquence, les relations d'équivalence$\sim_f$ et $\sim_{\mathsf{Ker}(f)}$ coïncident, ce qui implique que leurs classes d'équivalence coïncident aussi.

(*d*) Les items précédents impliquent que l'application $f : \mathbb{R} \to \mathbb{C}^*$ définie par $f(t) = e^{it}$ induit une application injective $\bar{f} : \mathbb{R}/2\pi\mathbb{Z} \to \mathbb{C}^*$ telle que $f = \bar{f} \circ p$.

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 $|H \times K| = |HK||H \cap K|$.

Solution.

(*a*) Étant donné $(h,k) \in H \times K$, on considère l'application $\phi_{(h,k)} : H \cap K \to [(h,k)]$ définie par $\phi_{(h,k)}(g) = (hg, g^{-1}k)$, pour $g \in H \cap K$. Elle est bien définie car $(hg, g^{-1}k) \in H \times K$ et $f \circ \phi_{(h,k)}(g) = hgg^{-1}k = hk = f(h,k)$, pour $g \in H \cap K$. On affirme que $\phi_{(h,k)}$ est bijectif. En effet, $\phi_{(h,k)}$ est injectif, car $\phi_{(h,k)}(g) = \phi_{(h,k)}(g')$ pour $g \in H \cap K$ implique $hg = h'g$, ce qui nous dit que $g = g'$. En outre, $\phi_{(h,k)}$ est surjectif, car, étant donné $(h',k') \sim_f (h,k)$, *i.e.* $h'k' = hk$ implique que $h^{-1}h' = kk'^{-1} \in H \cap K$ et $(h',k') = \phi_{(h,k)}(h^{-1}h') = (hh^{-1}h', k'k^{-1}k)$, vu que $(h^{-1}h')^{-1} = (kk'^{-1})^{-1} = k'k^{-1}$.

(*b*) Soit $s : HK \to H \times K$ une section de f, *i.e.* $f \circ s = \mathsf{id}_{HK}$. Noter que s est injectif. On définit l'application $\phi : HK \times (H \cap K) \to H \times K$ via $\phi(x,g) = \phi_{s(x)}(g)$, pour $x \in HK$ et $g \in H \cap K$. On affirme que ϕ est bijectif. En effet, ϕ est injectif, car $\phi_{s(x)}(g) = \phi(x,g) = \phi(x',g') = \phi_{s(x')}(g')$ pour $g, g' \in H \cap K$ et $x, x' \in HK$ implique $[s(x)] = [s(x')]$, *i.e.* $x = x'$, ce qui implique aussi $g = g'$, vu que $\phi_{s(x)}$ est injectif. En outre, ϕ est surjectif, car, étant donné $(h,k) \in H \times K$, $f(s(hk)) = hk$ implique qu'il existe $g \in H \cap K$ tel que $\phi_{s(hk)}(g) = (h,k)$, et enconséquence $\phi(s(hk), g) = (h,k)$. En conséquence, $|H \times K| = |HK||H \cap K|$.

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.

Solution.

(*a*) On voit bien que l'application $\bar{f} : E/\sim \to F$ telle que $f = \bar{f} \circ p$ existe est bien définie si et seulement si $\sim \subseteq \sim_f$, *i.e.* $x \sim y$ implique $x \sim_f y$. En effet, $f = \bar{f} \circ p$ implique que $f(x) = \bar{f}(p(x)) = \bar{f}(p(y)) = f(y)$ si $x \sim y$. Réciproquement, si $x \sim y$ implique $x \sim_f y$, alors l'application $\bar{f} : E/\sim \to F$ donnée par $\bar{f}([x]) = f(x)$ est bien définie. Par définition, elle satisfait $f = \bar{f} \circ p$. L'unicité de $\bar{f}$ suit de la surjectivité de l'application canonique $E \to E/\sim$.

(*b*) (i) On note que $[x]^{\sim_g} = \{\pm x\}$, pour tout $x \in \mathbb{R}$, ce qui nous dit que $\bar{f}$ existe pour $\sim = \sim_g$ associée à la fonction g donnée par $g(x) = |x|$ pour $x \in \mathbb{R}$, si et seulement si $f(x) = f(-x)$, pour tout $x \in \mathbb{R}$, *i.e.* f est une fonction paire.

(ii) On note que $[x]^{\sim_H} = \{x + ka : k \in \mathbb{Z}\}$, pour tout $x \in \mathbb{R}$, ce qui nous dit que $\bar{f}$ existe pour $\sim = \sim_H$ associée au sous-groupe $H = a\mathbb{Z}$ si et seulement si $f(x) = f(x + ak)$, pour tous $x \in \mathbb{R}$ et $k \in \mathbb{Z}$, *i.e.* f est une fonction périodique de période (au moins) a.

(*c*) Comme p est surjetif, l'identité $f = \bar{f} \circ p$ nous dit que $\mathsf{Img}(f) = \mathsf{Img}(\bar{f})$. En outre, $\bar{f}$ est injective si et seulement si $\bar{f}([x]) = \bar{f}([y])$ implique $[x] = [y]$ pour tous $x, y \in E$, ce qui équivaut à $f(x) = f(y)$ implique que $x \sim y$ pour tous $x, y \in E$, *i.e.* $\sim_f \subseteq \sim$. En conséquence, $\bar{f}$ 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 ?

Solution. On va utiliser le résultat suivant : étant donné deux sous-groupes H and K de G, $\sim_H \subseteq \sim_K$ si et seulement si $H \subseteq K$. En effet, si $\sim_H \subseteq \sim_K$, on voit bien que, étant donné $h \in H$, $1_G \sim_H h$, ce qui implique $1_G \sim_K h$, *i.e.* $h \in K$. On trouve alors, $H \subseteq K$. La réciproque est immédiate.

(*a*) D'après l'exercice **4**, (c), on sait que $\sim_f = \sim_{\mathsf{Ker}(f)}$. D'après l'exercice **6**, (a), l'existence de l'application $\bar{f} : G/H \to G'$ telle que $f = \bar{f} \circ p$ est équivalente à $\sim_{\mathsf{Ker}(f)} = \sim_f \subseteq \sim_H$. Le résultat précédent nous dit que la condition précédente est équivalente à $\mathsf{Ker}(f) \subseteq H$.

(*b*) D'après l'exercice **6**, (c), l'injectivité de l'application $\bar{f} : G/H \to G'$ est équivalente à $\sim_{\mathsf{Ker}(f)} = \sim_f = \sim_H$. Le résultat précédent nous dit que la condition précédente est équivalente à $\mathsf{Ker}(f) = H$.

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

$$\not{p} : \mathsf{GL}(K^2) \to \mathsf{Aut}_{\mathsf{Ens}}(\mathbb{P}^1(K))$$

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 $h = \mathsf{Ad}_{\bar{f}} \circ \not{p} \circ g$, 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 $n \in \mathbb{N}$.

Solution.

(*a*) C'est clair que $\sim$ est réflexive, var $v = 1v$, pour tout $v \in E$. En plus, $\sim$ est symétrique, car si $v \sim w$, il existe $\lambda \in K \setminus \{0\}$ tel que $v = \lambda w$, ce qui implique que $w = \lambda^{-1}v$, *i.e.* $w \sim v$. Enfin, $\sim$ est transitive, car si $u \sim v$ et $v \sim w$, il existe $\lambda, \mu \in K \setminus \{0\}$ tels que $u = \lambda v$ et $v = \mu w$, ce qui nous dit que $u = \lambda\mu w$, *i.e.* $u \sim w$. On voit bien que la classe d'équivalence de $v \in E$ est donnée par $\{\lambda v : \lambda \in K \setminus \{0\}\}$.

(*b*) Soient $v = (x, y) \in E$. Si $y = 0$, alors $f(\lambda(x, y)) = \infty$ pour tout $\lambda \in K \setminus \{0\}$. En outre, $f(\lambda(x, y)) = \lambda x/(\lambda y) = x/y = f(x, y)$, si $y \neq 0$. D'après l'exercice **6**, (a), il existe une application $\bar{f} : E/\sim \to K \sqcup \{\infty\}$ telle que $f = \bar{f} \circ p$. Comme f est surjective, $\bar{f}$ l'est aussi. En outre, $\bar{f}$ est injectif. En effet, soient $(x, y), (x', y') \in E$ tels que $\bar{f}([(x, y)]) = \bar{f}([(x', y')])$, *i.e.* $f(x, y) = f(x', y')$. Par définition de f, $y = 0$ si etseulement si $y' = 0$, et dans ce cas $[(x, y)] = [(x', y')]$. Par ailleurs, si $y \neq 0$, alors $x/y = f(x, y) = f(x', y') = x'/y'$, implique que $(y'/y) \cdot (x, y) = (x', y')$, *i.e.* $[(x, y)] = [(x', y')]$.

(*c*) Le résultat est immédiat.

(*d*) Pour montrer l'existence de $\hat{\phi}$, on pose $\hat{\phi}([v]) = [\phi(v)]$, pour $v \in E$. Il suffit de montrer que cette expression est bien définie, ce qui suit du fait que $[\phi(\lambda v)] = [\lambda\phi(v)] = [\phi(v)]$, pour tous $v \in E$ et $\lambda \in K \setminus \{0\}$, car ϕ est linéaire. L'unicité de $\hat{\phi}$ est une conséquence de l'identité $\hat{\phi} \circ p = p \circ \phi|_E$ et de la surjectivité de p. En outre, on a que $\widehat{\psi \circ \phi} = \hat{\psi} \circ \hat{\phi}$, pour tous $\phi, \psi \in \mathsf{GL}(K^2)$, en raison de la propriété d'unicité précédente et les identités

$$\hat{\psi} \circ \hat{\phi} \circ p = \hat{\psi} \circ p \circ \phi|_E = p \circ \psi|_E \circ \phi|_E = p \circ (\psi \circ \phi)|_E = \widehat{\psi \circ \phi} \circ p.$$

De la même façon, on a que $\hat{\mathsf{id}}_{K^2} = \mathsf{id}_{\mathbb{P}^1(K)}$, en raison de la propriété d'unicité précédente et les identités

$$\hat{\mathsf{id}}_{K^2} \circ p = p \circ \mathsf{id}_{K^2}|_E = p \circ \mathsf{id}|_E = p = \mathsf{id}_{\mathbb{P}^1(K)} \circ p.$$

On conclut alors que $\hat{\phi} \in \mathsf{Aut}_{\mathsf{Ens}}(\mathbb{P}^1(K))$ pour tout $\phi \in \mathsf{GL}(K^2)$. En effet,

$$\widehat{\phi^{-1}} \circ \hat{\phi} = \widehat{\phi^{-1} \circ \phi} = \hat{\mathsf{id}}_{K^2} = \mathsf{id}_{\mathbb{P}^1(K)} = \hat{\phi} \circ \widehat{\phi^{-1}} = \widehat{\phi \circ \phi^{-1}}.$$

Cela nous dit 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*) C'est clair que

$$\mathsf{Ad}_f(\psi \circ \phi) = f \circ \psi \circ \phi \circ f^{-1} = f \circ \psi \circ f \circ f^{-1} \circ \phi \circ f^{-1} = \mathsf{Ad}_f(\psi) \circ \mathsf{Ad}_f(\phi),$$

pour tous $\phi, \psi \in \mathsf{Aut}_{\mathsf{Ens}}(X)$, ce qui implique que Ad_f est un morphisme de groupes. En plus, c'est clair que $\mathsf{Ad}_f \circ \mathsf{Ad}_{f^{-1}} = \mathsf{id}_{\mathsf{Aut}_{\mathsf{Ens}}(Y)}$ et $\mathsf{Ad}_{f^{-1}} \circ \mathsf{Ad}_f = \mathsf{id}_{\mathsf{Aut}_{\mathsf{Ens}}(X)}$, ce qui implique que Ad_f est bijectif.

(*f*) Comme g et Ad_f son isomorphismes de groupes, $\mathsf{Ker}(\mathsf{Ad}_f \circ \wp) = \mathsf{Ker}(\wp)$ et $\mathsf{Ker}(h) = g^{-1}(\mathsf{Ker}(\wp))$. Il suffit donc de calculer $\mathsf{Ker}(\wp)$. On affirme que $\mathsf{Ker}(\wp) = \{\lambda \mathsf{id}_{K^2} : \lambda \in K \setminus \{0\}\}$. C'est clair que $\lambda \mathsf{id}_{K^2} \in \mathsf{Ker}(\wp)$ pour tout $\lambda \in K \setminus \{0\}$. Réciproquement, on voit bien que, par définition de $\wp$, $\phi \in \mathsf{GL}(K^2)$ est dans le noyau de $\wp$ si et seulement si $[\phi(v)] = [v]$ pour tout $v \in E$, *i.e.* pour tout $v \in E$ il existe $\lambda_v \in K \setminus \{0\}$ tel que $\phi(v) = \lambda_v v$. On affirme que $\lambda_v = \lambda_w$ pour tous $v, w \in E$. Pour le démontrer, soit $\{e_1, e_2\}$ una base de K^2. On voit alors que $\lambda_{e_1+e_2}(e_1 + e_2) = \phi(e_1 + e_2) = \phi(e_1) + \phi(e_2) = \lambda_{e_1} e_1 + \lambda_{e_2} e_2$, ce qui implique que $\lambda_{e_1} = \lambda_{e_2}$, que l'on notera λ, et en conséquence

$$\phi(\alpha e_1 + \beta e_2) = \alpha\phi(e_1) + \beta\phi(e_2) = \alpha\lambda e_1 + \beta\lambda e_2 = \lambda(\alpha e_1 + \beta e_2),$$

comme on voulait démontrer. Par conséquent, $\mathsf{Ker}(h) = g^{-1}(\mathsf{Ker}(\wp)) = K^* I_2$. Le premier théorème de l'isomorphisme nous dit que $\mathsf{GL}_2(K)/(K^* I_2) \simeq \mathsf{Img}(h)$.

(*g*) Si $c \neq 0$, un calcul direct nous dit que

$$h_M(z) = \frac{az + b}{cz + d}$$

pour tout $z \in \mathbb{C} \setminus \{-d/c\}$, $h_M(-d/c) = \infty$ et $h_M(\infty) = a/c$. Par ailleurs, si $c = 0$ (et donc $d \neq 0$), on vérifie directement que

$$h_M(z) = \frac{az + b}{d}$$

pour tout $z \in \mathbb{C}$ et $h_M(\infty) = \infty$.

Finalement, comme h est un morphisme de groupes, on voit bien que $h_M^{-1}(z) = h_{M^{-1}}(z)$, où

$$M^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

(*h*) Comme g_M est inversible, c'est clair que (x, y) est un vecteur propre de g_M si et seulement s'il existe $\lambda \in K \setminus \{0\}$ tel que $g_M(x, y) = \lambda(x, y)$, ce qui équivaut à que $\hat{g}_M([(x, y)]) = [(x, y)]$, *i.e.* $\hat{g}_M \circ \hat{f}^{-1}(f(x, y)) = f(x, y)$, *i.e.* $f(x, y)$ est un point fixe de h_M. Par ailleurs, d'après l'item précédent on voit bien que :

(i) ∞ un point fixe de h_M si et seulement si $c = 0$;

(ii) ∞ est le seul point fixe de h_M si et seulement si $c = 0$ (et donc $d \neq 0$), et soit $a \neq d$ ou $b \neq 0$;

(iii) 0 est un point fixe de h_M si et seulement si $b = 0$.

(*i*) Comme ∞ n'est pas un point fixe de h_M, on a $c \neq 0$. Étant donné la matrice M, on voit bien que les valeurs propres de M sont les racines du polynôme $X^2-(a+d)X+(ad-bc)=0$, *i.e.*

$$\lambda_\pm = \frac{(a+d) \pm \sqrt{(a-d)^2+4bc}}{2}.$$

Comme $c \neq 0$, la deuxième ligne de la matrice $M - r_\pm I_2$ nous dit alors que le vecteurs propre respectif est

$$v_\pm = \Big(\underbrace{\frac{(a-d) \pm \sqrt{(a-d)^2+4bc}}{2c}}_{r_\pm}, 1 \Big).$$

D'après l'item précédent on voit bien que h_M possède soit deux points fixes distincts, si $\lambda_+ \neq \lambda_-$, soit un seul point fixe, si $\lambda_+ = \lambda_-$. Noter que $\lambda_+ = \lambda_-$ si et seulement si $a=d$ et $b=0$, et dans ce cas $\lambda_+ = \lambda_- = a$. Le point fixe est dans ce cas $r_+ = r_- = 0$, et $v_- = v_+ = (0,1)$. Si $\lambda_+ \neq \lambda_-$, les points fixes de h_M sont r_+ et r_-.

Si $\lambda_+ \neq \lambda_-$ on voit bien que la matrice

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

est la matrice de passage de la base $\{v_-, v_+\}$ vers la base canonique, ce qui nous dit que

$$D = P^{-1}MP = \begin{pmatrix} \lambda_- & 0 \\ 0 & \lambda_+ \end{pmatrix},$$

et

$$\begin{aligned} w_n &= h_{P^{-1}}(z_n) = h_{P^{-1}}\big(h_{M^n}(z_0)\big) = h_{P^{-1}M^n}(z_0) = h_{D^nP^{-1}}(z_0) = h_{D^n}\big(h_{P^{-1}}(z_0)\big) \\ &= \left(\frac{\lambda_-}{\lambda_+}\right)^n h_{P^{-1}}(z_0), \end{aligned}$$

pour tout $n \in \mathbb{N}$.

Si $\lambda_+ = \lambda_-$ on voit bien que la matrice

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

est la matrice de passage de la base $\{(0,1),(1,0)\}$ vers la base canonique, ce qui nous dit que

$$T = P^{-1}MP = \begin{pmatrix} a & c \\ 0 & a \end{pmatrix},$$

et

$$\begin{aligned} w_n &= h_{P^{-1}}(z_n) = h_{P^{-1}}\big(h_{M^n}(z_0)\big) = h_{P^{-1}M^n}(z_0) = h_{T^nP^{-1}}(z_0) = h_{T^n}\big(h_{P^{-1}}(z_0)\big) \\ &= h_{P^{-1}}(z_0) + n\frac{c}{a}, \end{aligned}$$

pour tout $n \in \mathbb{N}$.

(*j*) Dans ce cas la matrice

$$M = \begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix}$$

possède les valeurs propres $\lambda_- = 1$ et $\lambda_+ = 5$, avec vecteurs propres $v_- = (-3, 1)$ et $v_+ = (1, 1)$. On choisit P comme dans l'item précédent. En conséquence, $h_{P^{-1}}(z_0) = 1/3$ et les calculs dans l'item précédent nous disent que

$$z_n = h_P(w_n) = h_P\left(\frac{1}{3.5^n}\right) = 3\frac{5^n - 1}{3.5^n + 1},$$

pour tout $n \in \mathbb{N}$.