Algèbre et Arithmétique 3

Devoir maison : ensemble quotient, groupe quotient, corps des fractions (version longue).

Relations d'équivalence

1. Soit E un ensemble. Se donner une *relation* $\mathcal{R}$ sur E, c'est se donner une condition portant sur les couples (x, y) d'éléments de E, qui pour chaque couple est soit vraie, soit fausse. Si elle est vraie pour le couple (x, y) on écrit « $x\mathcal{R}y$ ». Par exemple, la condition
$$\forall (x, y) \in \mathbf{R}^2, \quad x\mathcal{R}y \Leftrightarrow x < y$$
définit une relation $\mathcal{R}$ sur $\mathbf{R}$.
En d'autre termes, et plus formellement, se donner une relation revient à se donner une partie F de $E \times E$. La relation $\mathcal{R}$ associée à cette partie est alors définie par
$$\forall (x, y) \in E^2, \quad x\mathcal{R}y \Leftrightarrow (x, y) \in F.$$
2. Soient E et F des ensembles et $f : E \to F$ une application. On définit une relation $\mathcal{R}$ sur E par
$$\forall (x, y) \in E^2, \quad x\mathcal{R}y \Leftrightarrow f(x) = f(y)$$
Vérifier que la relation $\mathcal{R}$ est
– *symétrique*, c'est-à-dire vérifie $\forall (x, y) \in E^2, \quad x\mathcal{R}y \Leftrightarrow y\mathcal{R}x$
– *réflexive*, c'est-à-dire vérifie $\forall x \in E, \quad x\mathcal{R}x$
– *transitive*, c'est-à-dire vérifie $\forall (x, y, z) \in E^3, \quad (x\mathcal{R}y \text{ et } y\mathcal{R}z) \Rightarrow x\mathcal{R}z$
Plus généralement, une relation sur E qui vérifie ces trois propriétés est appelée une *relation d'équivalence sur E*.
3. La notion d'ensemble quotient par une relation d'équivalence, qui va être discutée ci-dessous, peut d'un certain point de vue se résumer de la façon suivante : le « plus généralement » dans la dernière phrase du numéro précédent est en fait de trop. On va voir que *n'importe quelle* relation d'équivalence sur E peut se définir à partir d'une certaine application $f : E \to F$ (pour un certain ensemble F) par la condition $(*)$ ci-dessus.
4. Soit E un ensemble et $\mathcal{R}$ une relation d'équivalence sur E. On définit une relation $\mathcal{R}'$ sur $E \times E$ par
$$\forall ((x_1, y_1), (x_2, y_2)) \in (E \times E)^2, \quad (x_1, y_1)\mathcal{R}'(x_2, y_2) \Leftrightarrow (x_1\mathcal{R}x_2 \text{ et } y_1\mathcal{R}y_2)$$
Vérifier que $\mathcal{R}'$ est une relation d'équivalence sur $E \times E$.

Ensemble quotient : définition par propriété universelle

5. Soit E un ensemble et $\mathcal{R}$ une relation d'équivalence sur E. Si F est un ensemble et $\pi : E \to F$ est une application, on dit que π est *compatible à* $\mathcal{R}$ si on a la propriété
$$\forall (x, y) \in E^2, \quad x\mathcal{R}y \Rightarrow \pi(x) = \pi(y).$$
Soit $\pi : E \to F$ une application compatible à $\mathcal{R}$ et $\varphi : F \to G$ une application. **Vérifier** que l'application $\varphi \circ \pi : E \to G$ est compatible à $\mathcal{R}$.
Un *ensemble quotient de E par $\mathcal{R}$* est un couple (F, π) où F est un ensemble et π une application de E vers F compatible à $\mathcal{R}$, qui vérifie en outre la propriété suivante, appelée *propriété universelle de l'ensemble quotient* : pour tout ensemble G et tout morphisme $\varphi : E \to G$ compatible à $\mathcal{R}$, il existe une *unique* application $\varphi' : F \to G$ vérifiant $\varphi' \circ \pi = \varphi$.

Groupe quotient d'un groupe commutatif : définition par propriété universelle

6. Soit $\mathcal{G}$ un groupe et $\mathcal{H}$ un sous-groupe de $\mathcal{G}$. Soit $\mathcal{I}$ et $\mathcal{J}$ des groupes, $\pi : \mathcal{G} \to \mathcal{I}$ un morphisme de noyau contenant $\mathcal{H}$ et $\varphi : \mathcal{I} \to \mathcal{J}$ un morphisme. **Vérifier** que le noyau de $\varphi \circ \pi : \mathcal{G} \to \mathcal{J}$ contient $\mathcal{H}$.

   On suppose désormais $\mathcal{G}$ commutatif. Un *quotient du groupe* $\mathcal{G}$ *par le sous-groupe* $\mathcal{H}$ est un couple $(\mathcal{I}, \pi)$ où $\mathcal{I}$ est un groupe commutatif et π un morphisme de groupes de $\mathcal{G}$ vers $\mathcal{I}$ de noyau contenant $\mathcal{H}$, qui vérifie en outre la propriété suivante, appelée *propriété universelle du groupe quotient* : pour tout groupe $\mathcal{J}$ et tout morphisme $\varphi : \mathcal{G} \to \mathcal{J}$ tel que $\mathrm{Ker}(\varphi)$ contient $\mathcal{H}$, il existe un *unique* morphisme $\varphi' : \mathcal{I} \to \mathcal{J}$ vérifiant $\varphi' \circ \pi = \varphi$.

7. Nous allons montrer dans la suite qu'un ensemble ou un groupe quotient existe toujours, par une construction explicite.

   Mais nous allons d'abord voir, en admettant provisoirement l'existence d'ensembles ou de groupes quotients, comment un certain nombre de leurs propriétés peuvent se retrouver directement à partir de la propriété universelle.

   Le but est de soutenir le slogan suivant : « peu importe finalement la façon dont on construit un quotient, ce qui sert vraiment est la propriété universelle ».

   On verra en particulier que la propriété universelle implique qu'un ensemble ou un groupe quotient, s'il existe, est en un certain sens unique. On pourra donc parler de « l' » ensemble quotient ou « du » groupe quotient (pour peu qu'ils existent).

Deux résultats utiles

8. Soient E et F des ensembles et $\tau : E \to F$ une application. **Montrer** que τ est surjective si et seulement si pour tout ensemble G et toute paire φ_1, φ_2 d'applications $F \to G$, on a $\varphi_1 \circ \tau = \varphi_2 \circ \tau$ si et seulement si $\varphi_1 = \varphi_2$.

9. Soit $\mathcal{G}$ un groupe commutatif (noté additivement) et $\mathcal{H}$ un sous-groupe de $\mathcal{G}$. On note $i : \mathcal{H} \to \mathcal{G}$ le morphisme injectif déduit de l'inclusion $\mathcal{H} \subset \mathcal{G}$. On suppose qu'il existe un morphisme $j : \mathcal{G} \to \mathcal{H}$ tel qu'on ait $j \circ i = \mathrm{Id}_{\mathcal{H}}$. **Montrer** qu'on a $j^2 = j$. Soit $\mathcal{I}$ le noyau de j. **Montrer** que pour tout $g \in \mathcal{G}$, on a $g - j(g) \in \mathcal{I}$. **Montrer** que l'application $g \mapsto g - j(g)$ est un morphisme de groupes surjectif de $\mathcal{G}$ vers $\mathcal{I}$ de noyau $\mathcal{H}$.

Propriétés de l'ensemble quotient

10. Dans les numéros 10 à 13, E est un ensemble, $\mathcal{R}$ une relation d'équivalence sur E et (F, π) est un ensemble quotient de E par $\mathcal{R}$.

11. **Déduire** du critère du numéro 8 que π est surjective (appliquer la propriété universelle de (F, π) à $\varphi_1 \circ \pi = \varphi_2 \circ \pi$).

12. Soit $x \in E$ et $E \to \{0, 1\}$ l'application définie par

    $$\forall y \in E, \quad \varphi(y) = 0 \Leftrightarrow x\mathcal{R}y.$$

    Vérifier qu'elle est compatible à $\mathcal{R}$. En appliquant la propriété universelle de (F, π) à φ, **montrer** que pour tout $y \in E$ vérifiant $\pi(y) = \pi(x)$, on a $\varphi(y) = 0$ (c'est-à-dire $x\mathcal{R}y$). En particulier on a $\pi(x) = \pi(y)$ si et seulement si $x\mathcal{R}y$.

    Pour résumer, on a donc démontré à partir de la propriété universelle qu'un ensemble quotient (F, π), s'il existe, vérifie toujours les propriétés suivantes :

    (a) π est surjective ;

(b) pour tout $(x, y) \in E^2$, on a $\pi(x) = \pi(y)$ si et seulement si $x\mathcal{R}y$.

13. Soient (F_1, π_1) et (F_2, π_2) deux ensembles quotients de E par $\mathcal{R}$. **Vérifier** qu'il existe une unique application $\varphi_{F_1,F_2} : F_1 \to F_2$ vérifiant $\varphi_{F_1,F_2} \circ \pi_1 = \pi_2$ (utiliser la propriété universelle de (F_1, π_1)). Soient (F_3, π_3) un autre ensemble quotient de E par $\mathcal{R}$. **Montrer** qu'on a $\varphi_{F_2,F_3} \circ \varphi_{F_1,F_2} = \varphi_{F_1,F_3}$. **En déduire** qu'il existe une unique bijection φ de F_1 sur F_2 vérifiant $\varphi \circ \pi_1 = \pi_2$.

    On voit ainsi que les ensembles quotients (F_1, π_1) et (F_2, π_2) sont uniquement déterminés à une bijection unique près. Pour cette raison on peut parler de « l' » ensemble quotient (avec un article défini). On le note $(E/\mathcal{R}, \pi)$.

Propriétés du groupe quotient

14. Dans les numéros 14 à 17, $\mathcal{G}$ est un groupe commutatif, $\mathcal{H}$ est un sous-groupe de $\mathcal{G}$ et $(\mathcal{I}, \pi)$ un quotient du groupe $\mathcal{G}$ par le sous-groupe $\mathcal{H}$

    Soit $\widetilde{\pi} : \mathcal{G} \to \pi(\mathcal{G})$ l'application qui à $g \in G$ associe $\pi(g)$. **Vérifier** que $\mathrm{Ker}(\widetilde{\pi})$ contient $\mathcal{H}$. En appliquant la propriété universelle de $(\mathcal{I}, \pi)$ à $\widetilde{\pi}$ **montrer** qu'il existe un morphisme $j : \mathcal{I} \to \pi(\mathcal{G})$ vérifiant $j \circ i = \mathrm{Id}_{\pi(\mathcal{G})}$. En utilisant le numéro 9, **montrer** alors que π est surjective.

15. On suppose qu'il existe un groupe $\mathcal{J}$ et un morphisme $\mathcal{G} \to \mathcal{J}$ de noyau $\mathcal{H}$. **Montrer** que $\mathrm{Ker}(\pi) = \mathcal{H}$.

16. Soit $\mathscr{X}$ l'ensemble des parties de $\mathcal{G}$ qui sont de la forme $g + \mathcal{H}$ où g est un élément de $\mathcal{G}$. À tout élément g de $\mathcal{G}$ on associe l' application $\tau_g : \mathscr{X} \to \mathscr{X}$ qui à une partie A associe $g + A$. **Vérifier** que τ_g est bien définie et est une bijection. **Montrer** que l'application $\mathcal{G} \to \mathfrak{S}_{\mathscr{X}}$ qui à g associe τ_g est un morphisme de groupes de noyau $\mathcal{H}$. Notez que d'après 15, on en déduit que π est de noyau $\mathcal{H}$.

    Pour résumer, on a montré à partir la propriété universelle qu'un groupe quotient $(\mathcal{I}, \pi)$, s'il existe, satisfait toujours les propriétés suivantes :

    (a) π est surjectif ;

    (b) $\mathrm{Ker}(\pi) = \mathcal{H}$.

    Pour la deuxième propriété, il n'est en fait pas tout à fait vrai qu'on a utilisé uniquement la propriété universelle : la construction utilisée revient en fait quasiment à une construction explicite du groupe quotient, comme on va le voir plus loin.

17. Soient $(\mathcal{I}_1, \pi_1)$ et $(\mathcal{I}_2, \pi_2)$ deux groupes quotients de $\mathcal{G}$ par $\mathcal{H}$. **Montrer** qu'il existe un unique isomorphisme $\varphi : \mathcal{I}_1 \to \mathcal{I}_2$ vérifiant $\varphi \circ \pi_1 = \pi_2$ (indication : on peut recopier presque mot à mot la démonstration utilisée dans le cas des ensembles quotient).

    On voit que les groupes quotients $(\mathcal{I}_1, \pi_1)$ et $(\mathcal{I}_2, \pi_2)$ sont uniquement déterminés à un isomorphisme unique près. Pour cette raison on peut parler « du » groupe quotient de $\mathcal{G}$ par $\mathcal{H}$ (avec un article défini). On le note $(\mathcal{G}/\mathcal{H}, \pi)$.

Construction de l'ensemble quotient

18. Soit E un ensemble et $\mathcal{R}$ une relation d'équivalence sur E. Dans ce numéro et dans 19, nous construisons un ensemble quotient de E par $\mathcal{R}$. Soit $\pi : E \to F$ une application surjective et qui vérifie
$$\forall (x, y) \in E^2, \quad x\mathcal{R}y \Leftrightarrow \pi(x) = \pi(y) \quad (*).$$
    Vérifier que (F, π) est un ensemble quotient de E par $\mathcal{R}$ (en d'autres termes montrer que (F, π) satisfait la propriété universelle du quotient).

19. Pour $x \in E$, soit $E(x) = \{y \in E, \quad x\mathcal{R}y\}$. **Vérifier** que pour tous $x, y \in E$ on a $E(x) = E(y)$ si et seulement si $x\mathcal{R}y$. Soit F l'ensemble des parties de E qui sont de la forme $E(x)$ pour un certain $x \in E$ et π l'application qui à $x \in E$ associe l'ensemble $E(x) \in F$. **Vérifier** que π est surjective et satisfait la propriété $(*)$. Ainsi (F, π) est bien un ensemble quotient de E par $\mathcal{R}$.
20. Soit $\mathcal{R}'$ la relation d'équivalence sur $E \times E$ définie au numéro 4. Soit $(E/\mathcal{R}, \pi)$ l'ensemble quotient de E par $\mathcal{R}$. Soit $\pi \times \pi$ l'application $E \times E \to E/\mathcal{R} \times E/\mathcal{R}$ définie par $(x, y) \mapsto (\pi(x), \pi(y))$. **Montrer** que $(E/\mathcal{R} \times E/\mathcal{R}, \pi \times \pi)$ est un ensemble quotient de $E \times E$ par $\mathcal{R}'$.

Construction(s) du groupe quotient

21. Soit $\mathcal{G}$ un groupe commutatif et $\mathcal{H}$ un sous-groupe de $\mathcal{G}$. Dans les numéros 21 à 24, nous construisons un groupe quotient $(\mathcal{I}, \pi)$ de $\mathcal{G}$ par $\mathcal{H}$. Nous allons en fait donner deux constructions : l'une à partir de la construction du numéro 16, et l'autre utilisant la notion d'ensemble quotient.

    Soit $\mathcal{I}$ un groupe et $\pi : \mathcal{G} \to \mathcal{I}$ un morphisme surjectif de noyau $\mathcal{H}$. **Vérifier** que $(\mathcal{I}, \pi)$ est un groupe quotient de $\mathcal{G}$ par $\mathcal{H}$, en d'autres termes que $\mathcal{I}$ est commutatif et que $(\mathcal{I}, \pi)$ satisfait la propriété universelle du groupe quotient.
22. *Première construction du groupe quotient*

    On considère à nouveau le morphisme $\mathcal{G} \to \mathfrak{S}_{\mathscr{X}}$ défini au numéro 16. Soit $\mathcal{I}$ l'image de $\mathcal{G}$ dans $\mathfrak{S}_{\mathscr{X}}$ et $\pi : \mathcal{G} \to \mathcal{I}$ le morphisme induit. **Vérifier** que $(\mathcal{I}, \pi)$ est un quotient de $\mathcal{G}$ par $\mathcal{H}$.
23. *Seconde construction du groupe quotient*

    Soit $\mathcal{R}_{\mathcal{H}}$ la relation définie sur $\mathcal{G}$ par $g\mathcal{R}g'$ si et seulement si $g - g' \in \mathcal{H}$. **Vérifier** que $\mathcal{R}_{\mathcal{H}}$ est une relation d'équivalence sur $\mathcal{G}$ et que $(\mathcal{G}/\mathcal{R}_{\mathcal{H}}, \pi)$ est un ensemble quotient de $\mathcal{G}$ par $\mathcal{R}_{\mathcal{H}}$.
24. Le numéro précédent nous incite à construire un groupe quotient de $\mathcal{G}$ par $\mathcal{H}$ en mettant une structure de groupe sur l'ensemble quotient sur $\mathcal{G}/\mathcal{R}_{\mathcal{H}}$. Rappelons que l'on note π l'application quotient $\pi : \mathcal{G} \to \mathcal{G}/\mathcal{R}_{\mathcal{H}}$.

    Soit $\mathcal{G} \times \mathcal{G} \to \mathcal{G}/\mathcal{R}_{\mathcal{H}}$ l'application définie par $(x, y) \mapsto \pi(x + y)$. **Montrer** qu'il existe une unique application $s : \mathcal{G}/\mathcal{R}_{\mathcal{H}} \times \mathcal{G}/\mathcal{R}_{\mathcal{H}} \to \mathcal{G}/\mathcal{R}_{\mathcal{H}}$ vérifiant

    $$\forall (x, y) \in \mathcal{G}^2, \quad s(\pi(x), \pi(y)) = \pi(x + y).$$

    (utiliser le numéro 20 et la propriété universelle de $(\mathcal{G}/\mathcal{R}_{\mathcal{H}} \times \mathcal{G}/\mathcal{R}_{\mathcal{H}}, \pi \times \pi)$. **Vérifier** les propriétés suivantes

    $$\forall (x, y, z) \in \mathcal{G}^3, \quad s(\pi(x), s[\pi(y), \pi(z)]) = s(s[\pi(x), \pi(y)], \pi(z))$$

    $$\forall (x, y) \in \mathcal{G}^2, \quad s(\pi(x), \pi(y)) = s(\pi(y), \pi(x))$$

    $$\forall x \in \mathcal{G}, \quad s(\pi(x), \pi(0)) = \pi(x)$$

    $$\forall x \in \mathcal{G}, \quad s(\pi(x), \pi(-x)) = \pi(0).$$

    En déduire que la loi de composition interne s munit $\mathcal{G}/\mathcal{R}_{\mathcal{H}}$ d'une structure de groupe commutatif, d'élément neutre $\pi(0)$, et que $\pi : \mathcal{G} \to \mathcal{G}/\mathcal{R}_{\mathcal{H}}$ est alors un morphisme de groupes. En utilisant 21, **vérifier** que $(\mathcal{G}/\mathcal{R}_{\mathcal{H}}, \pi)$ est un quotient du groupe $\mathcal{G}$ par le sous-groupe $\mathcal{H}$.

Le cas des groupes non commutatifs

25. Soit $\mathcal{G}$ un groupe, non nécessairement commutatif et $\mathcal{H}$ un sous-groupe de $\mathcal{G}$. Un quotient du groupe $\mathcal{G}$ par le sous-groupe $\mathcal{H}$ est un couple $(\mathcal{I}, \pi)$ où $\mathcal{I}$ est un groupe et π un morphisme de groupes de $\mathcal{G}$ vers $\mathcal{I}$ de noyau $\mathcal{H}$, qui vérifie en outre la propriété suivante : pour tout groupe $\mathcal{J}$ et tout morphisme $\varphi : \mathcal{G} \to \mathcal{J}$ tel que $\operatorname{Ker}(\varphi)$ contient $\mathcal{H}$, il existe un *unique* morphisme $\varphi' : \mathcal{I} \to \mathcal{J}$ vérifiant $\varphi' \circ \pi = \varphi$.

    On suppose désormais $\mathcal{H}$ distingué dans $\mathcal{G}$. **Reprendre** alors, en faisant les adaptations nécessaires, la démarche entreprise pour les groupes commutatifs (c'est-à-dire les numéros 14 à 17 puis 21 à 24). On montrera en particulier que si $\mathcal{H}$ est distingué dans $\mathcal{G}$, un quotient de $\mathcal{G}$ par $\mathcal{H}$ existe, est uniquement déterminé à isomorphisme unique près, et est caractérisé par la propriété d'être un morphisme surjectif de noyau $\mathcal{H}$. On pourra remplacer l'utilisation du résultat du numéro 9 par l'utilisation du résultat suivant, que l'on admettra (la démonstration n'utilise pas d'outils hors programme, mais est difficile) : soient $\mathcal{G}$ et $\mathcal{G}'$ des groupes et $\tau : \mathcal{G} \to \mathcal{G}'$ un morphisme ; alors τ est surjectif si et seulement si pour tout groupe $\mathcal{G}''$ et toute paire φ_1, φ_2 de morphismes $\mathcal{G}' \to \mathcal{G}''$, on a $\varphi_1 \circ \tau = \varphi_2 \circ \tau$ si et seulement si $\varphi_1 = \varphi_2$. On notera l'analogie de ce résultat avec celui du numéro 8.

Corps des fractions : définition par propriété universelle

26. Soit A un anneau commutatif intègre (rappelons qu'en particulier $A \setminus \{0_A\}$ n'est pas vide). On dit qu'un morphisme d'anneaux $\iota : A \to B$ *rend les éléments non nuls de A inversibles* si on a $\varphi(A \setminus \{0_A\}) \subset B^\times$. Si $\iota : A \to B$ est un tel morphisme et $\varphi : B \to C$ un morphisme d'anneaux, **vérifier** que $\varphi \circ \iota$ rend les éléments non nuls de A inversibles. **Vérifier** qu'un morphisme rendant les éléments non nuls de A inversibles est injectif.

    Un *corps des fractions de A* est un couple (B, ι) où B est un anneau commutatif et ι un morphisme d'anneaux de A vers B rendant les éléments non nuls de A inversibles et qui vérifie en outre la propriété suivante, appelée *propriété universelle du corps des fractions* : pour tout anneau commutatif C et tout morphisme d'anneaux $\varphi : A \to C$ rendant les éléments non nuls de A inversibles, il existe un *unique* morphisme d'anneaux $\varphi' : B \to C$ vérifiant $\varphi' \circ \iota = \varphi$.

27. **Montrer** que si ι est l'injection déduite de l'inclusion naturelle $\mathbf{Z} \subset \mathbf{Q}$ alors $(\mathbf{Q}, \iota)$ est un corps des fractions de $\mathbf{Z}$. La notion de corps des fractions vise à généraliser à un anneau intègre quelconque la construction de $\mathbf{Q}$ à partir de celle de $\mathbf{Z}$. Nous allons montrer plus loin qu'un corps des fractions existe toujours par une construction explicite, mais nous allons d'abord dégager quelques unes de ses propriétés à l'aide de la propriété universelle. Nous verrons en particulier qu'un corps des fractions est uniquement déterminé à un isomorphisme unique près, c'est pourquoi l'on pourra parler « du » corps des fractions.

Propriétés du corps des fractions

28. Soit (B, ι) un corps des fractions de A. Soit

    $$C = \left\{\iota(a)\iota(a')^{-1}, \quad (a, a') \in A \times A \setminus \{0_A\}\right\} \subset B.$$

    Vérifier que C est un sous-anneau de B. **Montrer** que C est un corps.

    Notons τ le morphisme injectif déduit de l'inclusion $C \subset B$. En appliquant la propriété universelle, **montrer** qu'il existe un morphisme d'anneaux $j : B \to C$ tel que $j \circ \tau = \mathrm{Id}_C$ **Montrer** que j est injectif (on pourra s'inspirer du numéro 9) et **en déduire** que $C = B$. En particulier B est un corps (ce qui justifie la terminologie « corps des fractions »).

29. Soient (B_1, ι_1) et (B_2, π_2) deux corps des fractions de A. **Vérifier** qu'il existe un unique morphisme d'anneaux $\varphi_{B_1,B_2} : B_1 \to B_2$ vérifiant $\varphi_{B_1,B_2} \circ \iota_1 = \iota_2$ (utiliser la propriété universelle de (B_1, ι_1)). Soient (B_3, ι_3) un autre corps des fractions de A. **Montrer** qu'on a $\varphi_{B_2,B_3} \circ \varphi_{B_1,B_2} = \varphi_{B_1,B_3}$. **En déduire** qu'il existe un unique isomorphisme φ de B_1 sur B_2 vérifiant $\varphi \circ \iota_1 = \iota_2$.

Construction(s) du corps des fractions

30. Passons à la démonstration de l'existence du corps des fractions. Nous allons d'abord donner une construction valable dans la situation où A est un sous-anneau d'un certain corps $\mathbf{K}$, situation très largement rencontrée dans la pratique. Puis nous passerons au cas général.
31. Soit $\iota : A \to B$ un morphisme d'anneaux rendant les éléments non nuls de A inversibles. On suppose qu'on a

$$B = \left\{\iota(a)\iota(a')^{-1}, \quad (a, a') \in A \times A \setminus \{0_A\}\right\}.$$

Montrer que (B, ι) est un corps des fractions de A.

32. On suppose que A est un sous-anneau d'un corps $\mathbf{K}$.
Soit

$$B = \left\{\frac{a}{a'}, \quad (a, a') \in A \times A \setminus \{0\}\right\} \subset \mathbf{K}.$$

Vérifier que B est un sous-anneau de $\mathbf{K}$ contenant A. Notons ι le morphisme d'anneaux déduit de l'inclusion $A \subset B$. **Montrer** que (B, ι) est le corps des fractions de A.
Quel est le corps des fractions de $\mathbf{Z}[i]$?

33. On pose $\mathcal{B} = A \times A \setminus \{0_A\}$. **Vérifier** que les formules

$$(a_1, a_1') \oplus (a_2, a_2') = (a_1\, a_2' + a_2\, a_1', a_1'\, a_2')$$

et

$$(a_1, a_1') \otimes (a_2, a_2') = (a_1\, a_2, a_1'\, a_2')$$

définissent des lois de compositions internes $\oplus$ et $\otimes$ sur $\mathcal{B}$, et que ces lois sont associatives et commutatives. $(\mathcal{B}, \oplus)$ **est-il** un groupe ? La loi $\otimes$ **est-elle** distributive par rapport à la loi $\oplus$?
On définit une relation $\mathcal{R}$ sur $\mathcal{B}$ par

$$\forall ((a_1, a_1')(a_2, a_2')) \in \mathcal{B}^2, \quad (a_1, a_1')\mathcal{R}(a_2, a_2') \Leftrightarrow a_1\, a_2' = a_2\, a_1'.$$

Vérifier que $\mathcal{R}$ est une relation d'équivalence sur $\mathcal{B}$. Soit $(\mathcal{B}/\mathcal{R}, \pi)$ l'ensemble quotient.
Montrer qu'il existe une unique application $s : \mathcal{B}/\mathcal{R} \times \mathcal{B}/\mathcal{R} \to \mathcal{B}/\mathcal{R}$ vérifiant

$$\forall (x, y) \in \mathcal{B}^2, \quad s(\pi(x), \pi(y)) = \pi(x \oplus y)$$

et une unique application $m : \mathcal{B}/\mathcal{R} \times \mathcal{B}/\mathcal{R} \to \mathcal{B}/\mathcal{R}$ vérifiant

$$\forall (x, y) \in \mathcal{B}^2, \quad m(\pi(x), \pi(y)) = \pi(x \otimes y).$$

(utiliser le numéro 20 et la propriété universelle de l'ensemble quotient $(\mathcal{B}/\mathcal{R} \times \mathcal{B}/\mathcal{R}, \pi \times \pi)$.
Vérifier les propriétés suivantes

$$\forall (x, y, z) \in \mathcal{B}^3, \quad s(\pi(x), s[\pi(y), \pi(z)]) = s(s[\pi(x), \pi(y)], \pi(z))$$

$$\forall (x,y,z) \in \mathcal{B}^3, \quad m(\pi(x), m[\pi(y), \pi(z)]) = m(m[\pi(x), \pi(y)], \pi(z))$$
$$\forall (x,y) \in \mathcal{B}^2, \quad s(\pi(x), \pi(y)) = s(\pi(y), \pi(x))$$
$$\forall (x,y) \in \mathcal{B}^2, \quad m(\pi(x), \pi(y)) = m(\pi(y), \pi(x))$$
$$\forall x \in \mathcal{B}, \quad s(\pi(x), \pi(0_A, 1_A)) = \pi(x)$$
$$\forall x \in \mathcal{B}, \quad m(\pi(x), \pi(1_A, 1_A)) = \pi(x)$$
$$\forall x = (a, a') \in \mathcal{B}, \quad s(\pi(x), \pi(-a, a')) = \pi((0_A, 1_A))$$
$$\forall x = (a, a') \in \mathcal{B}, \quad m(\pi(x), \pi(a', a) = \pi((1_A, 1_A))$$
$$\forall (x,y,z) \in \mathcal{B}^3, \quad m(\pi(x), s[\pi(y), \pi(z)]) = s(m[\pi(x), \pi(y)], m[\pi(x), \pi(z)])$$

En déduire que $(\mathcal{B}/\mathcal{R}, s, m)$ est un anneau commutatif. **Montrer** que l'application $\iota : A \to \mathcal{B}/\mathcal{R}$ à a associe $\pi(a, 1_A)$ est un morphisme d'anneaux qui rend les éléments non nuls de A inversibles. En utilisant le numéro 31, **montrer** que $(\mathcal{B}/\mathcal{R}, \pi)$ est un corps des fractions de A.

Dans la pratique, pour $(a, a') \in (A \setminus \{0_A\})^2$, l'élément $\pi(a, a') \in \mathcal{B}/\mathcal{R}$ est noté $\frac{a}{a'}$, et pour $x, y \in \mathcal{B}/\mathcal{R}$, on note $s(x,y) = x + y$ et $m(x,y) = x \times y$ ou $x\,y$.

Vérifier qu'on retrouve les règles usuelles de calcul des fractions (a, b désignent des éléments de A et a', b' des éléments de $A \setminus \{0_A\}$:

$$\frac{a}{a'} + \frac{b}{b'} = \frac{a\,b' + a'\,b}{b\,b'}$$
$$\frac{a}{a'} \times \frac{b}{b'} = \frac{a\,a'}{b\,b'}$$
$$\frac{a}{a'} = \frac{b}{b'} \Leftrightarrow a\,b' = b\,a'.$$