Algèbre - Devoir à la maison II

*Le devoir est à rendre au plus tard le **jeudi 16 Décembre avant 17h**. Vous pouvez le rédiger en **français ou en anglais**. Le devoir est à rendre de l'une des façons suivantes : **à mon bureau** (2C22 au bâtiment 307) OU **dans mon casier** à l'entrée du bâtiment 307 OU **par mail en un UNIQUE fichier pdf avec votre nom** dans le nom du fichier à l'adresse kevin.destagnol@universite-paris-saclay.fr. Vous pouvez également me contacter à cette adresse mail en cas de questions ou si vous repérez ce qui vous semble être une erreur d'énoncé.*

Problème 1 — Localisation de modules et autres platitudes.

Soit A un anneau commutatif. On rappelle qu'une partie $S \subseteq A$ est dite *multiplicative* si $1 \in S$ et si pour tous $s_1, s_2 \in S$, alors $s_1 s_2 \in S$. On définit alors $S^{-1}A$ le *localisé* de A en S comme le quotient de $A \times S$ par la relation d'équivalence $(a, s) \sim (b, t)$ si, et seulement s'il existe $u \in S$ tel que $u(at - bs) = 0$. On rappelle qu'on peut munir $S^{-1}A$ d'une structure d'anneau commutatif via les opérations

$$\forall (a,s),(b,t) \in A \times S, \quad \frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st} \quad \text{et} \quad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.$$

On a alors un morphisme d'anneaux canonique $f : A \longrightarrow S^{-1}A$ donné par $a \mapsto \frac{a}{1}$ qui est injectif si S ne contient aucun diviseur de 0. Dans le cas où $S = A \setminus \mathfrak{P}$, on note $A_{\mathfrak{P}} := S^{-1}A$, qui est un anneau local[1]. On rappelle enfin qu'un A-module est dit *plat* si pour toute suite exacte de $A-$modules $0 \longrightarrow M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \longrightarrow 0$, alors la suite suivante de $A-$modules

$$0 \longrightarrow M_1 \otimes_A M \xrightarrow{f \otimes \mathrm{Id}_M} M_2 \otimes_A M \xrightarrow{g \otimes \mathrm{Id}_M} M_3 \otimes_A M \longrightarrow 0 ,$$

est exacte.

1. Décrire les idéaux de $S^{-1}A$. Montrer que $S^{-1}A$ est intègre si A l'est, et que $S^{-1}A$ est principal si A l'est et si $0 \notin S$.
2. Soit $\varphi : A \longrightarrow B$ un morphisme d'anneaux. Montrer qu'il existe un unique morphisme $\tilde{\varphi} : S^{-1}A \longrightarrow B$ tel que $\tilde{\varphi} \circ f = \varphi$ si, et seulement si, $\varphi(S) \subseteq B^{\times}$.
3. Soit S est une partie multiplicative de A et $\sim$ la relation d'équivalence définie sur $M \times S$ par $(m, s) \sim (m', t)$ si, et seulement s'il existe $u \in S$ tel que $u(t \cdot m - s \cdot m') = 0$. Expliquer comment munir $S^{-1}M := (M \times S)/\sim$ d'une structure de $S^{-1}A$-module compatible avec celle rappelée en introduction dans le cas où $M = A$. On dit que $S^{-1}M$ est le *localisé* de M en S. *On notera si $S = A \setminus \mathfrak{P}$ avec $\mathfrak{P}$ un idéal premier de A, $S^{-1}M := M_{\mathfrak{P}}$.*
4. Soit M un A-module. Montrer, en considérant pour $x \in M$ l'ensemble $\{a \in A \ : \ a \cdot x = 0\}$, que $M = 0$ si, et seulement si, $M_{\mathfrak{m}} = 0$ pour tout idéal maximal $\mathfrak{m}$ de A.
5. Montrer que pour S une partie multiplicative de A, on a un isomorphisme de $S^{-1}A$-modules $M \otimes_A S^{-1}A \cong S^{-1}M$.
6. Soit S une partie multiplicative de A et $M \longrightarrow N \longrightarrow P$ une suite exacte de A-modules. Montrer qu'elle induit une suite exacte de $S^{-1}A$-modules
$$S^{-1}M \longrightarrow S^{-1}N \longrightarrow S^{-1}P.$$
7. Établir que $S^{-1}A$ est un A-module plat.
8. Montrer que le morphisme naturel $M \longrightarrow \prod_{\mathfrak{m}} M_{\mathfrak{m}}$ (où le produit porte sur tous les idéaux maximaux de A) est injectif. On se donne alors une suite de A-modules $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$. En déduire que cette suite est exacte si, et seulement si, la suite $0 \longrightarrow M_{\mathfrak{m}} \longrightarrow N_{\mathfrak{m}} \longrightarrow P_{\mathfrak{m}} \longrightarrow 0$ l'est pour tout idéal maximal $\mathfrak{m}$ de A.
Indication : Pour le sens indirect, on pourra pour la surjectivité de g, montrer que l'idéal $I = \{a \in A \ : \ ap \in Im(g)\}$ n'est contenu dans aucun idéal maximal $\mathfrak{m}$. Pour cela, considérer $p_{\mathfrak{m}} = \frac{p}{1}$.
9. Soit A intègre de corps de fractions k. On définit le rang d'un A-module M comme la dimension du k-espace vectoriel $M \otimes_A k$. Montrer que si $0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0$ est une suite exacte, alors $\mathrm{rang}(N) = \mathrm{rang}(M) + \mathrm{rang}(P)$.
10. **(Bonus)** Soit M un A-module. Montrer alors qu'on a la série d'équivalences suivante :
    (i) M est plat sur A ;
    (ii) $M_{\mathfrak{P}}$ est plat sur $A_{\mathfrak{P}}$ pour tout idéal premier $\mathfrak{P}$ de A ;
    (iii) $M_{\mathfrak{m}}$ est plat sur $A_{\mathfrak{m}}$ pour tout idéal maximal $\mathfrak{m}$ de A.
    *Indication : On pourra utiliser que si B est une A-algèbre et que M est un A-module plat sur A, alors $M \otimes_A B$ est plat sur B ainsi que la question **6**.*

1. Autrement dit $A_{\mathfrak{P}}$ possède un unique idéal maximal.

11. Montrer que si $0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0$ est une suite exacte de A-modules avec P plat, alors pour tout A-module Q, on a une suite exacte $0 \longrightarrow M \otimes_A Q \longrightarrow N \otimes_A Q \longrightarrow P \otimes_A Q \longrightarrow 0$.
Indication : On pourra écrire Q comme le quotient d'un module libre L par un sous-module K et considérer la suite exacte $0 \longrightarrow K \longrightarrow L \longrightarrow Q \longrightarrow 0$ puis tensoriser par M, N et P et effectuer une chasse au diagramme.

12. **(DIFFICILE, BONUS)** Rappeler pourquoi un module libre est plat et préciser si la réciproque est valable en général. On suppose à présent que A est un anneau local. Montrer alors que M de type fini est plat si, et seulement si, M est libre. En déduire que M est plat si, et seulement s'il est *localement libre*, c'est-à-dire que $M_{\mathfrak{m}}$ est libre pour tout idéal premier $\mathfrak{m}$ de A.
Indication : On note $\mathfrak{m}$ l'unique idéal maximal de A et $k = A/\mathfrak{m}$. Montrer qu'une famille $(x_1, \dots, x_n)$ dont l'image est k-libre dans $M/\mathfrak{m}M$ est A-libre dans M. Pour ce faire, considérer une relation de liaison $\sum_i a_i x_i = 0$ ainsi que l'application $f : A^n \longrightarrow A$ définie par $(b_1, \dots, b_n) \mapsto \sum_i x_i b_i$ et tensoriser par M. Pour finir, utiliser le lemme de Nakayama.

13. En étudiant le cas de $A = \mathbf{C} \times \mathbf{C}$ et M l'idéal engendré par $(1, 0)$, peut-on dire que M est libre si, et seulement si, $M_{\mathfrak{m}}$ l'est pour tout idéal maximal $\mathfrak{m}$ de A ?

SOLUTION.
Je vous invite à relire l'exercice 2 du TD III avant de vous lancer dans cet exercice !

1. Établissons que tout idéal I de $S^{-1}A$ est de la forme

$$S^{-1}J = \left\{ \frac{a}{s} \ : \ a \in J, \ s \in S \right\}$$

avec J un idéal de A. On a clairement que $S^{-1}J$ est un idéal (c'est en fait celui engendré par $f(J)$ mais on peut le vérifier aisément à la main) et réciproquement pour tout idéal I de $S^{-1}A$, l'ensemble

$$J = \left\{ a \in A \ : \ \exists s \in S, \text{ tel que } \frac{a}{s} \in I \right\}$$

est un idéal de A vérifiant $S^{-1}J = I$. En effet, si $\frac{a}{s} \in S^{-1}J$ avec $a \in J$ et $s \in S$, par définition, il existe $s' \in S$ tel que $\frac{a}{s'} \in I$ et donc

$$\frac{a}{s} = \frac{s'}{s}\frac{a}{s'} \in I$$

car I est un idéal de $S^{-1}A$. Pour l'inclusion réciproque, il suffit de voir que si $\frac{a}{s} \in I$ avec $a \in A$ et $s \in S$, alors $a \in J$ et donc $\frac{a}{s} \in S^{-1}J$.
En particulier, les idéaux premiers de $S^{-1}A$ s'identifient aux idéaux premiers de A ne rencontrant pas S. En effet, si $\mathfrak{P}$ est un idéal premier de A, alors on obtient immédiatement que $S^{-1}\mathfrak{P}$ est un idéal vérifiant que pour tous $\frac{a}{s}, \frac{b}{t}$ tels que $\frac{a}{s} \cdot \frac{b}{t} \in S^{-1}\mathfrak{P}$, alors $\frac{a}{s}$ ou $\frac{b}{t} \in S^{-1}\mathfrak{P}$. Seulement, s'il existe $s \in S \cap \mathfrak{P}$, alors $\frac{s}{1} \in S^{-1}\mathfrak{P}$ mais est inversible dans $S^{-1}A$ (qui n'est autre que $\frac{1}{s}$ qui est bien défini dans $S^{-1}A$) et donc $S^{-1}\mathfrak{P} = S^{-1}A$ tandis que si $S \cap \mathfrak{P} = \varnothing$, alors $1 \notin S^{-1}\mathfrak{P}$ qui est donc distinct de $S^{-1}A$. On conclut de ces quelques remarques élémentaires que si $\mathfrak{P}$ est un idéal premier de A qui ne rencontre pas S, alors $S^{-1}\mathfrak{P}$ est un idéal premier de $S^{-1}A$. On obtient réciproquement qu'un idéal premier I de $S^{-1}A$ est de la forme $I = S^{-1}J$ pour J un idéal de A. On vérifie alors aisément que puisque $I \neq S^{-1}A$, $1 \notin S^{-1}J$ et donc J ne rencontre pas S et on montre immédiatement que J est premier. Les propriétés suivantes découlent facilement des définitions et de cette description des idéaux de $S^{-1}A$ pour S une partie multiplicative ne contenant pas 0 :

- Si A est intègre, alors $S^{-1}A$ est intègre[2] ;
- Si A est principal, alors $S^{-1}A$ est principal[3] ;
- Si A est factoriel, alors $S^{-1}A$ est factoriel[4].

On peut aussi montrer que (*cf.* TD V exercice 4 sur les modules pour la définition d'une limite projective)

$$S^{-1}A = \varinjlim_{s \in S} A\left[\frac{1}{s}\right]$$

où on voit S comme un ensemble ordonné filtrant pour la divisibilité (en particulier, si $s, s' \in S$, alors $ss' \in S$ et est supérieur à s et s') et où l'on considère les applications de transition $f_{ss'} : A\left[\frac{1}{s}\right] \longrightarrow A\left[\frac{1}{s'}\right]$ pour $s \leqslant s'$ (soit $s' = ss''$) définie par $\frac{a}{s^n} \mapsto \frac{a}{s'^n}$. Le morphisme $f : A \longrightarrow S^{-1}A$ fournit un morphisme pour tout $s \in S$, $A\left[\frac{1}{s}\right] \longrightarrow S^{-1}A$. Ces morphismes sont compatibles entre eux et par la propriété universelle de la limite inductive, il vient un morphisme

$$\Phi : \varinjlim_{s \in S} A\left[\frac{1}{s}\right] \longrightarrow S^{-1}A.$$

2. Si $\frac{a}{s} \cdot \frac{b}{t} = 0$ alors il existe $u \in S$ tel que $uab = 0$ soit $a = 0$ ou $b = 0$ (car $0 \notin S$ par hypothèse et par intégrité de A).
3. Un tel idéal I est de la forme $S^{-1}J$ pour $J = (a)$ par principalité de A et donc $I = \left(\frac{a}{1}\right)$.
4. Commencer par établir que les inversibles de $S^{-1}A$ sont les $\frac{a}{s}$ avec a divisant un élément de S et que les irréductibles de $S^{-1}A$ sont (modulo les inversibles) les $\frac{p}{1}$ avec p irréductible de A ne divisant aucun élément de S.

Réciproquement, on a un morphisme naturel $A \longrightarrow \varinjlim_{s\in S} A\left[\frac{1}{s}\right]$ qui fournit par propriété universelle de la localisation un morphisme

$$\Psi : S^{-1}A \longrightarrow \varinjlim_{s\in S} A\left[\frac{1}{s}\right]$$

dont on vérifie qu'il est l'inverse de Φ.

2. Si une telle application existe, alors pour tout $t = \varphi(s) \in \varphi(S)$, l'élément $\frac{1}{s}$ a un sens dans $S^{-1}A$ et vérifie $\frac{1}{s}\cdot\frac{s}{1} = 1$ de sorte que, puisque $\tilde{\varphi}$ est un morphisme d'anneaux, il vient

$$1 = \tilde{\varphi}\left(\frac{1}{s}\right)\tilde{\varphi}\left(\frac{s}{1}\right).$$

Or, $\tilde{\varphi}\left(\frac{s}{1}\right) = \tilde{\varphi}\left(f(s)\right) = \varphi(s) = t$ de sorte que

$$1 = \tilde{\varphi}\left(\frac{1}{s}\right)\cdot t \quad \text{avec} \quad \tilde{\varphi}\left(\frac{1}{s}\right) \in B.$$

On en déduit bien que $t \in B^\times$ et par conséquent que $\varphi(S) \subseteq B^\times$.
Réciproquement, supposons que $\varphi(S) \subseteq B^\times$. On commence par construire une application $\theta : A\times S \to B$ donnée par $\theta(a,s) = \varphi(s)^{-1}\varphi(a)$ pour $a \in A$ et $s \in S$. Il est alors clair que si $\frac{a}{s} = \frac{b}{s}$, autrement dit s'il existe $u \in S$ tel que $u(at - bs) = 0$, il vient (puisque φ est un morphisme)

$$\varphi(u)(\varphi(a)\varphi(t) - \varphi(b)\varphi(s)) = 0 \quad \text{soit} \quad \varphi(s)^{-1}\varphi(a) = \varphi(t)^{-1}\varphi(b)$$

car $\varphi(u), \varphi(s)$ et $\varphi(t)$ sont dans $B^\times$. On obtient ainsi au quotient une application $\tilde{\varphi} : S^{-1}A \to B$ telle que $\tilde{\varphi}\left(\frac{a}{s}\right) = \varphi(s)^{-1}\varphi(a)$. On vérifie aisément qu'il s'agit d'un morphisme d'anneaux pour la structure d'anneau de $S^{-1}A$ et que $\tilde{\varphi}\circ f = \varphi$. Pour conclure, une telle application est unique car tout élément de $S^{-1}A$ s'écrit sous la forme $\frac{a}{s} = \frac{a}{1}\cdot\frac{1}{s}$ et l'image de $\frac{a}{1} = f(a)$ est fixée par la relation $\tilde{\varphi}\circ f = \varphi$. Reste donc à voir que celle de $\frac{1}{s}$ aussi. On utilise alors la même astuce que précédemment, à savoir que, puisque $1 = \frac{1}{s}\cdot\frac{s}{1}$ et le fait que φ soit un morphisme pour en conclure que nécessairement $\tilde{\varphi}\left(\frac{1}{s}\right) = \varphi\left(s\right)^{-1}$.

3. On notera de même $\frac{m}{s}$ pour la classe de (m,s) avec $m \in M$ et $s \in S$ et pose de même

$$\forall s,s' \in S, \quad \forall m \in M, \quad \forall a \in A, \quad \frac{m}{s} + \frac{m'}{s'} = \frac{s'\cdot m - s\cdot m'}{ss'} \quad \text{et} \quad \frac{a}{s}\cdot\frac{m}{s'} = \frac{am}{ss'}$$

et on vérifie que cela munit $S^{-1}M$ d'une structure de $S^{-1}A$-module de manière immédiate. Noter que si $0 \in S$, on a $S^{-1}A = S^{-1}M = \{0\}$.

4. Il est clair que si $M = \{0\}$, alors pour tout idéal maximal $\mathfrak{m}$ de A, on a $M_\mathfrak{m} = \{0\}$ par définition.
Réciproquement, on suppose que pour tout idéal maximal $\mathfrak{m}$ de A, on a $M_\mathfrak{m} = \{0\}$. Soit $x \in M$. On suit l'indication de l'énoncé et on considère $\mathrm{Ann}(x) = \{a \in A \ : \ a\cdot x = 0\}$ et on voit immédiatement qu'il s'agit d'un idéal de A. Si cet idéal est différent de A, alors par le théorème de Krull, il existe un idéal maximal $\mathfrak{m}$ de A tel que $\mathrm{Ann}(x) \subseteq \mathfrak{m}$. Or, $\frac{x}{1} \in M_\mathfrak{m} = \{0\}$ de sorte que par définition il existe $s \in A\setminus\mathfrak{m}$ tel que $s\cdot x = 0$, autrement dit $s \in \mathrm{Ann}(x) \subseteq \mathfrak{m}$, contradiction ! On en déduit que $\mathrm{Ann}(x) = A$ et en particulier, $1 \in \mathrm{Ann}(x)$ et $x = 0$. On a par conséquent $M = 0$. Noter qu'on a ici une sorte de *principe local-global* où pour vérifier que $M = 0$ (propriété globale), il suffit de vérifier que tous les localisés $M_\mathfrak{m}$ en des idéaux maximaux de A sont nuls (propriétés locales).

5. Établissons que $S^{-1}M \cong S^{-1}A\otimes_A M$ en tant que $S^{-1}A$-modules. On considère l'application A-bilinéaire $\varphi : S^{-1}A\times M \to S^{-1}M$ définie par $\left(\frac{a}{s}, m\right) \mapsto \frac{am}{s}$ qui donne lieu à une application A-linéaire $f : S^{-1}A\otimes_A M \to S^{-1}M$. Cette application est surjective car $\frac{x}{s} = f\left(\frac{1}{s}\otimes x\right)$. Montrons alors qu'elle est injective. On voit que

$$f\left(\frac{1}{s}\otimes x\right) = 0 \iff \frac{x}{s} = 0 \iff \exists u \in S \text{ tel que } ux = 0.$$

On a alors si $f\left(\frac{1}{s}\otimes x\right) = 0$ que $\frac{1}{s}\otimes x = \frac{u}{us}\otimes x = \frac{1}{us}\otimes ux = 0$ par A-linéarité. Maintenant, tout élément de $S^{-1}A\otimes_A M$ est de la forme (quitte à réduire au même dénominateur)

$$\sum_i \frac{a_i}{s}\otimes x_i = \frac{1}{s}\otimes\left(\sum_i a_i x_i\right)$$

et un élément du noyau est donc nul par ce qui précède et f est injective, ce qui démontre la bijectivité[5]. Reste à voir que cette application est en fait $S^{-1}A$-linéaire :

$$f\left(\frac{a}{s}\cdot\left(\frac{b}{t}\otimes m\right)\right) = f\left(\frac{ab}{st}\otimes m\right) = \frac{abm}{st} = \frac{a}{s}\cdot\frac{bm}{t} = \frac{a}{s}\cdot f\left(\frac{b}{t}\otimes m\right)$$

ce qui termine la démonstration. Noter qu'on a donc un isomorphisme de A-modules **et** de $S^{-1}A$-modules.

5. On pouvait aussi voir que $\frac{m}{s} \mapsto \frac{1}{s}\otimes m$ est un morphisme bien défini et inverse de notre application de départ.

6. On se donne une suite exacte de A-modules $M \xrightarrow{f} N \xrightarrow{g} P$. On obtient alors la suite de $S^{-1}A$-modules suivante $S^{-1}M \xrightarrow{\tilde{f}} S^{-1}N \xrightarrow{\tilde{f}} S^{-1}P$ où

$$\tilde{f} : \begin{cases} S^{-1}M & \longrightarrow & S^{-1}N \\ \frac{m}{s} & \longmapsto & \frac{f(m)}{s} \end{cases}$$

et de même pour $\tilde{g}$. Cette application est clairement $S^{-1}A$-linéaire car

$$\tilde{f}\left(\frac{a}{s}\cdot\frac{m}{t}\right) = \tilde{f}\left(\frac{am}{st}\right) = \frac{f(am)}{st} = \frac{af(m)}{st} = \frac{a}{s}\cdot\frac{f(m)}{t} = \frac{a}{s}\cdot\tilde{f}\left(\frac{m}{t}\right).$$

Montrons alors que la suite $S^{-1}M \xrightarrow{\tilde{f}} S^{-1}N \xrightarrow{\tilde{f}} S^{-1}P$ est exacte, autrement dit que $\mathrm{Ker}(\tilde{g}) = \mathrm{Im}(\tilde{f})$. Il est clair d'après les définitions que si $\frac{a}{s} \in \mathrm{Im}(\tilde{f})$, alors $\frac{a}{s} = \frac{f(m)}{s}$ pour $m \in M$ de sorte que

$$\tilde{g}\left(\frac{a}{s}\right) = \tilde{g}\left(\frac{f(m)}{s}\right) = \frac{g\circ f(m)}{s} = 0$$

car $g \circ f = 0$ car la suite initiale est exacte. Reste à établir que $\mathrm{Ker}(\tilde{g}) \subseteq \mathrm{Im}(\tilde{f})$. Soit $\frac{a}{s} \in \mathrm{Ker}(\tilde{g})$. On a donc $\frac{g(a)}{s} = 0$ dans $S^{-1}N$ de sorte qu'il existe $u \in S$ tel que $ug(a) = 0$. Or g est A-linéaire donc $g(u\cdot a) = 0$ et $u \cdot a \in \mathrm{Ker}(g) = \mathrm{Im}(f)$ de sorte qu'il existe $m \in M$ tel que $u \cdot a = f(m)$. On vérifie alors que

$$\tilde{f}\left(\frac{m}{us}\right) = \frac{f(m)}{us} = \frac{u\cdot a}{us} = \frac{a}{s}$$

et on a l'inclusion désirée.

7. Remarquons que M est plat si, et seulement si, pour toute application linéaire injective $f : M_1 \to M_2$, l'application linéaire

$$f \otimes \mathrm{Id}_M : M_1 \otimes_A M \longrightarrow M_2 \otimes_A M$$

est injective. Si M est plat, la condition est immédiate. Réciproquement, le reste de la suite exacte provient directement du cours, Théorème 2.16.

Il suffit donc de montrer qu'une application $f : N \to P$ injective (qui donne par conséquent lieu à une suite exacte $0 \longrightarrow N \xrightarrow{f} P$) donne lieu à une application injective $f \otimes \mathrm{Id}_{S^{-1}A} : N \otimes_A S^{-1}A \longrightarrow P \otimes_A S^{-1}A$ (soit une suite exacte de A-modules $0 \longrightarrow N \otimes_A S^{-1}A \xrightarrow{f\otimes \mathrm{Id}_{S^{-1}A}} P \otimes_A S^{-1}A$). On a alors le diagramme commutatif suivant

$$\begin{array}{ccccc} 0 & \longrightarrow & N\otimes_A S^{-1}A & \xrightarrow{f\otimes \mathrm{Id}_{S^{-1}A}} & P\otimes_A S^{-1}A \\ & & \downarrow{\scriptstyle \varphi_N} & & \downarrow{\scriptstyle \varphi_P} \\ 0 & \longrightarrow & S^{-1}N & \xrightarrow{\tilde{f}} & S^{-1}P \end{array}$$

avec φ_N et φ_P les isomorphismes de la question **5.** et $\tilde{f}$ le morphisme correspondant à f de la question **6.** Ce diagramme est commutatif car

$$\varphi_P\left(f\otimes \mathrm{Id}_{S^{-1}A}\left(n\otimes\frac{a}{s}\right)\right) = \varphi_P\left(f(n)\otimes\frac{a}{s}\right) = \frac{af(n)}{s} \quad \text{et} \quad \tilde{f}\left(\varphi_N\left(n\otimes\frac{a}{s}\right)\right) = \tilde{f}\left(\frac{an}{s}\right) = \frac{f(an)}{s} = \frac{af(n)}{s}$$

si bien que $\varphi_P \circ f \otimes \mathrm{Id}_{S^{-1}A} = \tilde{f}\circ\varphi_N$ car les tenseurs purs sont générateurs. Il est alors facile de voir que l'application $f \otimes \mathrm{Id}_{S^{-1}A}$ est injective si, et seulement si, $\tilde{f}$ l'est (car les flèches verticales sont des isomorphismes). Or la ligne horizontale du bas est exacte d'après **6.** avec $M = \{0\}$ donc en particulier $\tilde{f}$ est injective et on a le résultat !

8. Le morphisme naturel est donné par

$$\theta : \begin{cases} M & \longrightarrow & \prod_{\mathfrak{m}} M_{\mathfrak{m}} \\ m & \longmapsto & \left(\frac{m}{1}\right)_{\mathfrak{m}}. \end{cases}$$

Montrons dans un premier temps que ce morphisme est injectif. En effet, si $m \in \mathrm{Ker}(\theta)$, alors $\frac{m}{1} = \frac{0}{1}$ dans chaque $M_{\mathfrak{m}}$ pour $\mathfrak{m}$ idéal maximal de A. Il existe donc $u \notin \mathfrak{m}$ tel que $u \cdot m = 0$ par définition du localisé. En particulier, si on considère à nouveau

$$\mathrm{Ann}(m) = \{a \in A \ : \ a\cdot m = 0\},$$

alors on obtient un idéal de A qui n'est pas contenu dans $\mathfrak{m}$, ce qui implique (par Krull et puisque ceci est valable pour tout idéal maximal) que $\mathrm{Ann}(m) = A$ et en particulier pour $a = 1$, que $m = 0$ et ainsi que θ est injective !

Le sens direct découle alors directement de la question **6.** Pour le sens réciproque, supposons que la suite
$0 \longrightarrow M_{\mathfrak{m}} \xrightarrow{\tilde{f}} N_{\mathfrak{m}} \xrightarrow{\tilde{g}} P_{\mathfrak{m}} \longrightarrow 0$ au sens de la question **5.** soit exacte. Montrons alors que la suite initiale
$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$ est exacte. On a alors le diagramme commutatif suivant

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{f} & N & \xrightarrow{g} & P & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \theta_M} & & \downarrow{\scriptstyle \theta_N} & & \downarrow{\scriptstyle \theta_P} & & \\ 0 & \longrightarrow & \prod_{\mathfrak{m}} M_{\mathfrak{m}} & \xrightarrow{\tilde{f}} & \prod_{\mathfrak{m}} N_{\mathfrak{m}} & \xrightarrow{\tilde{g}} & \prod_{\mathfrak{m}} P_{\mathfrak{m}} & \longrightarrow & 0 \end{array}$$

ce diagramme est commutatif car par exemple

$$\theta_N(f(m)) = \left(\frac{f(m)}{1}\right) \quad \text{et} \quad \tilde{f}(\theta_M(m)) = \tilde{f}\left(\frac{m}{1}\right) = \left(\frac{f(m)}{1}\right).$$

On vérifie de même que le second carré commute. Par hypothèse, la ligne du bas est exacte et les flèches verticales sont injectives par la première partie de la question. Il s'ensuit alors immédiatement que f est injective car si $m \in \mathrm{Ker}(f)$, alors $f(m) = 0$ et donc $\theta_N(f(m)) = 0$ et donc $\tilde{f}(\theta_M(m)) = 0$ si bien que par injectivité de $\tilde{f}$ et de θ_M, alors $m = 0$. De même, on obtient immédiatement $g \circ f = 0$ car pour $m \in M$, $g(f(m))$ est dans le noyau de θ_P. En effet, $\theta_P \circ g(f(m)) = \tilde{g} \circ \theta_N(f(m)) = \tilde{g} \circ \tilde{f}(\theta_M(m)) = 0$ par exactitude de la ligne du bas.
Montrons alors que g est surjective. Pour ce faire, considérons $p \in P$ et $I = \{a \in A \ : \ ap \in \mathrm{Im}(g)\}$. On voit immédiatement que l'on a un idéal de A car g est A-linéaire. Montrons que $I = A$. Sinon, il existe un idéal maximal $\mathfrak{m}$ de A tel que $I \subseteq \mathfrak{m}$. On envoie alors $p \in P$ dans $P_{\mathfrak{m}}$ via f. Autrement dit, $\frac{p}{1} \in P_{\mathfrak{m}}$ et par exactitude, il existe $n_{\mathfrak{m}} = \frac{n}{s} \in N_{\mathfrak{m}}$ tel que $g(n_{\mathfrak{m}}) = \frac{p}{1}$. On a donc $\frac{g(n)}{s} = \frac{p}{1}$ soit l'existence de $u \notin \mathfrak{m}$ tel que $u(g(n) - ps) = 0$. Ainsi, $su \in I \subseteq \mathfrak{m}$ mais u et s par définition ne sont pas dans $\mathfrak{m}$. On a une contradiction puisque $\mathfrak{m}$ est maximal et donc en particulier premier. Ainsi $I = A$ et on en déduit que $p \in \mathrm{Im}(g)$ et g est surjective.
Pour conclure, il reste à établir l'inclusion $\mathrm{Ker}(g) \subseteq \mathrm{Im}(f)$. Soit $n \in \mathrm{Ker}(g)$. Considérons de façon analogue $I = \{a \in A \ : \ an \in \mathrm{Im}(f)\}$. On voit immédiatement que l'on a un idéal de A car f est A-linéaire. Montrons que $I = A$. Sinon, il existe un idéal maximal $\mathfrak{m}$ de A tel que $I \subseteq \mathfrak{m}$. On envoie alors $n \in N$ dans $N_{\mathfrak{m}}$. Autrement dit, $\frac{n}{1} \in N_{\mathfrak{m}}$ et $g\left(\frac{n}{1}\right) = \frac{g(n)}{1} = 0$ car n est dans le noyau de g. On a donc $\frac{n}{1}$ dans le noyau de g et par exactitude, il existe $m_{\mathfrak{m}} = \frac{m}{s} \in M_{\mathfrak{m}}$ tel que $\frac{f(m)}{s} = \frac{n}{1}$. On a donc l'existence de $u \notin \mathfrak{m}$ tel que $u(f(m) - ns) = 0$. Ainsi, $su \in I \subseteq \mathfrak{m}$ mais u et s par définition ne sont pas dans $\mathfrak{m}$. On conclut de la même façon.
On a à nouveau un exemple de principe local-global.

9. On commence par remarquer que $k = S^{-1}A$ avec $S = A \setminus \{0\}$ qui est bien multiplicatif car A est intègre. On déduit alors des questions **6.** et **7.** (puisque k est un A-module plat) qu'on a alors une suite exacte $0 \longrightarrow M \otimes_A k \longrightarrow N \otimes_A k \longrightarrow P \otimes_A k \longrightarrow 0$ qui est une suite exacte de k-espaces vectoriels. On sait alors que dans ce cas, on peut identifier $M \otimes_A k$ à un sous-espace vectoriel de $N \otimes_A k$. Par ailleurs, comme on a affaire à des espaces vectoriels, on a toujours un supplémentaire de $M \otimes_A k$ dans $N \otimes_A k$, ce supplémentaire étant isomorphe au quotient $N \otimes_A k / M \otimes_A k \cong P \otimes_A k$. On en déduit donc immédiatement la relation demandée[6].

10. Commençons par établir que (i) $\Rightarrow$ (ii). Supposons que M est plat sur A et pour $\mathfrak{P}$ un idéal premier de A, le morphisme $f : A \longrightarrow S^{-1}A$ fait de $S^{-1}A$ une A-algèbre. On déduit alors de l'indication que $M \otimes_A S^{-1}A \cong S^{-1}M$ est plat sur $S^{-1}A$ via la question **5.** Il reste donc à expliquer pourquoi l'indication est vraie. Supposons donc donnée une A-algèbre B. On se donne une suite exacte de B-modules $0 \longrightarrow M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \longrightarrow 0$. On cherche à savoir si l'application $f \otimes \mathrm{Id} : M_1 \otimes_B (M \otimes_A B) \longrightarrow M_2 \otimes_B (M \otimes_A B)$ est injective (le reste étant automatique par les propriétés du produit tensoriel). Or, on sait que $M_i \otimes_B (M \otimes_A B) \cong M_i \otimes_A M$ en tant que B-modules et ainsi l'application $f \otimes \mathrm{Id} : M_1 \otimes_B (M \otimes_A B) \longrightarrow M_2 \otimes_B (M \otimes_A B)$ s'identifie à $f \otimes \mathrm{Id} : M_1 \otimes_A M \longrightarrow M_2 \otimes_A M$ qui est injective par exactitude de M.
L'implication (ii) $\Rightarrow$ (iii) est claire pusiqu'un idéal maximal est en particulier premier.
Reste donc à établir (iii) $\Rightarrow$ (i). Il suffit d'établir que pour toute application injective $g : N_1 \longrightarrow N_2$ de A-modules, alors $g \otimes \mathrm{Id} : M \otimes_A N_1 \longrightarrow M \otimes_A N_2$ est injective. Si l'on note L son noyau, on a une suite exacte $0 \longrightarrow L \longrightarrow M \otimes_A N_1 \xrightarrow{g \otimes \mathrm{Id}} M \otimes_A N_2$.
Par la question **7.**, il vient pour tout idéal maximal $\mathfrak{m}$ de A une suite exacte

$$0 \longrightarrow L \otimes_A A_{\mathfrak{m}} \longrightarrow (M \otimes_A N_1) \otimes_A A_{\mathfrak{m}} \xrightarrow{g \otimes \mathrm{Id}} (M \otimes_A N_2) \otimes_A A_{\mathfrak{m}}$$

Or, on a par associativité et commutativité du produit tensoriel, par **3.**

$$(M \otimes_A N_i) \otimes_A A_{\mathfrak{m}} \cong (M \otimes_A A_{\mathfrak{m}}) \otimes_A N_i \cong M_{\mathfrak{m}} \otimes_A N_i.$$

6. Une autre façon de voir les choses et de considérer des bases (e_i) de $M \otimes_A k$ et $(f_j = g(u_j))$ de $P \otimes_A k$ (ce qui est possible avec des espaces vectoriels). On montre alors que la famille $(f(e_i), u_j)$ est libre et génératrice et donc une base de $N \otimes_A k$ (s'inspirer de la question 4 de l'exercice 15 du TD V pour cela).

Enfin, on sait que

$$M_{\mathfrak{m}} \otimes_A N_i \cong M_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} (N_i \otimes_A A_{\mathfrak{m}}) \cong M_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} (N_i)_{\mathfrak{m}}.$$

Tous ces isomorphismes sont en tant que $A_{\mathfrak{m}}$-modules. Ainsi, $L \otimes_A A_{\mathfrak{m}} \cong L_{\mathfrak{m}}$ s'identifie au noyau de $M_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} (N_1)_{\mathfrak{m}} \to M_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} (N_2)_{\mathfrak{m}}$ donné par $\mathrm{Id} \otimes \tilde{f}$ avec $\tilde{f} : (N_1)_{\mathfrak{m}} \to (N_2)_{\mathfrak{m}}$ qui est injective par **6.** Par exactitude de $M_{\mathfrak{m}}$, on en déduit que $L_{\mathfrak{m}} = \{0\}$ pour tout idéal maximal et la question **4.** entraîne finalement $L = \{0\}$ et l'injectivité recherchée, ce qui permet de conclure la preuve.

11. On suppose donnée $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$ une suite exacte de A-modules avec P un A-module plat. Montrons que pour tout A-module Q, alors $f \otimes \mathrm{Id} : M \otimes_A Q \to N \otimes_A Q$ est injective. Pour cela, on utilise que Q possède une famille génératrice [7] $(x_i)_{i\in I}$. On a donc une application surjective $A^{(I)} \to Q$ de noyau K. Il s'ensuit une suite exacte $0 \longrightarrow K \xrightarrow{i} A^{(I)} \xrightarrow{p} Q \longrightarrow 0$. On a alors le diagramme commutatif suivant [8] (en effet on a vu en TD qu'un module libre était plat)

$$\begin{array}{ccccccc}
 & & M\otimes_A K & \xrightarrow{\mu} & N\otimes_A K & \xrightarrow{\theta} & P\otimes_A K \\
 & & \downarrow{\scriptstyle\pi} & & \downarrow{\scriptstyle\omega} & & \downarrow{\scriptstyle\alpha} \\
0 & \longrightarrow & M\otimes_A A^{(I)} & \xrightarrow{\gamma} & N\otimes_A A^{(I)} & \xrightarrow{\varphi} & P\otimes_A A^{(I)} \\
 & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\delta} & & \\
 & & M\otimes_A Q & \xrightarrow{f\otimes\mathrm{Id}} & N\otimes_A Q & & \\
 & & \downarrow & & & & \\
 & & 0 & & & &
\end{array}$$

On a alors puisque P est plat que α est injective. Il ne reste plus qu'à effectuer une petite chasse au diagramme ! On se fixe ainsi x dans le noyau de $f \otimes \mathrm{Id}$ (donc dans $M \otimes_A Q$. Par surjectivité de β, il existe $y \in M \otimes A^{(I)}$ tel que $x = \beta(y)$ et comme le diagramme commute, $\gamma(y)$ est dans le noyau de δ si bien que par exactitude, il existe $z \in N \otimes_A K$ tel que $\gamma(y) = \omega(z)$. Mais comme $\gamma(y)$ est dans l'image de γ, il est dans le noyau de φ et donc $\varphi(\gamma(y)) = \varphi(\omega(z)) = 0$. par commutativité du diagramme, il s'ensuit que $\alpha(\theta(z)) = 0$ et puisque α est injective, $\theta(z) = 0$. Par exactitude de la première ligne, on a $t \in M \otimes_A K$ tel que $z = \mu(t)$. Alors $\gamma(y) = \omega(\mu(t)) = \gamma(\pi(t))$. Par injectivité de γ, on obtient $y = \pi(y)$ et finalement $x = \beta(\pi(t)) = 0$ par exactitude de la première colonne ! On a donc finalement le résultat ! Ouf !

12. On a vu dans le TD V qu'un module libre était plat et la question suivante permet d'exhiber un contre-exemple à cette affirmation !
On suppose à présent A local et M un A-module de type fini. Il suffit de montrer que si M est plat, alors M est libre. Supposons donc M plat. On note $\mathfrak{m}$ l'unique idéal maximal de A et $k = A/\mathfrak{m}$ qui est un corps. On sait qu'on a alors $M/\mathfrak{m}M \cong M \otimes_A k = M \otimes_A A/\mathfrak{m}$ qui est muni d'une structure de k-espace vectoriel. On notera $\pi : M \to M/\mathfrak{m}M$ la projection canonique. Considérons $(x_1, \ldots, x_n)$ des éléments de M tels que $(\pi(x_1), \ldots, \pi(x_n))$ forme une famille libre de ce k-espace vectoriel $M/\mathfrak{m}M$. Montrons alors que $(x_1, \ldots, x_n)$ est A-libre. Pour ce faire, soient $\lambda_1, \ldots, \lambda_n$ dans A tels que

$$\sum_{i=1}^{n} \lambda_i x_i = 0.$$

On pose alors l'application A-linéaire $f : A^n \to A$ définie par $f(a_1, \ldots, a_n) = \sum_{i=1}^{n} \lambda_i a_i$. On a alors clairement une suite exacte $0 \longrightarrow L := \mathrm{Ker}(f) \longrightarrow A^n \xrightarrow{f} A$ qui donne lieu (puisque M est plat) à une suite exacte $0 \longrightarrow L \otimes_A M \longrightarrow A^n \otimes_A M \xrightarrow{f\otimes\mathrm{Id}} A \otimes_A M$. On montre comme en TD que l'application $f \otimes \mathrm{Id} : A^n \otimes_A M \cong M^n \to A \otimes_A M \cong M$ s'identifie à $f_M : M^n \to M$ donnée par $f(m_1, \cdots, m_n) = \sum_{i=1}^{n} \lambda_i m_i$. En particulier $(x_1, \ldots, x_n)$ est dans le noyau de f_M donc, si $(e_1, \ldots, e_n)$ désigne la base canonique de A^n, alors $\sum_{i=1}^{n} e_i \otimes x_i$ est dans $L \otimes M$. Il existe donc $(\mathbf{b}_1, \ldots, \mathbf{b}_r) \in \mathrm{Ker}(f)^r$ avec $\mathbf{b}_i = (b_{1i}, \ldots, b_{ni}) \in A^n$ et $y_1, \ldots, y_r \in M$ tels que

$$\sum_{i=1}^{n} e_i \otimes x_i = \sum_{j=1}^{r} \mathbf{b}_j \otimes y_j = \sum_{i=1}^{n} e_i \otimes \left(\sum_{j=1}^{r} b_{ij} y_j \right) \quad \text{autrement dit} \quad x_i = \sum_{j=1}^{r} b_{ij} y_j$$

7. Par exemple, prendre tous les éléments de Q.
8. Par exemple,

$$\gamma(\pi(m \otimes k)) = \gamma(m \otimes i(k)) = f(m) \otimes i(k) \quad \text{et} \quad \omega(\mu(m \otimes k)) = \omega(f(m) \otimes k) = f(m) \otimes i(k)$$

et de même pour tous les autres carrés !

en identifiant $A^n \otimes_A M$ avec M^n. Si tout les b_{ij} sont dans $\mathfrak{m}$, alors $\pi(x_i) = 0$ pour tout i, ce qui contredit la liberté des x_i. Ainsi, il existe i, j tels que $b_{ij} \notin \mathfrak{m}$ donc inversible ! On peut supposer sans perte de généralités que $b_{11} \in A^\times$. Mais du fait que $\mathbf{b}_1 \in \mathrm{Ker}(f)$, il découle

$$b_{11}\lambda_1 = -\sum_{i=2}^{n} b_{1i}\lambda_i \quad \text{soit} \quad \lambda_1 = -\sum_{i=2}^{n} c_i\lambda_i$$

avec $c_i = b_{i1}b_{11}^{-1}$. On peut alors raisonner par récurrence. Si $n = 1$, ce raisonnement fournit $\lambda_1 = 0$ et le résultat ! Sinon, cela fournit que

$$\sum_{i=1}^{n} \lambda_i x_i = \sum_{i=2}^{n} \lambda_i (x_i - c_i x_1) = 0.$$

On vérifie alors immédiatement que si les images des x_i dans $M/\mathfrak{m}M$ sont libres, alors celles des $x_i - c_i x_1$ le sont aussi et donc en appliquant notre hypothèse de récurrence, il vient que $\lambda_2 = \cdots = \lambda_n = 0$ et on est ramené au cas $n = 1$ qui fournit $\lambda_1 = 0$. On a donc le résultat annoncé.

Pour conclure, puisque $M/\mathfrak{m}M$ est un espace vectoriel sur k de dimension finie car M est de type fini (et donc $M/\mathfrak{m}M$ aussi et il possède donc une famille génératrice finie), on peut en trouver une base de la forme (par surjectivité de π) $(\pi(x_1), \ldots, \pi(x_n))$. Cette famille étant libre sur k, on vient de voir que la famille $(x_1, \ldots, x_n)$ est A-libre dans M. Reste ainsi à montrer qu'elle est génératrice pour conclure. On considère pour ce faire N le sous-module de M engendré par les x_i (qui est donc un module libre) et établissons que $M = N$. On a une suite exacte $0 \longrightarrow N \longrightarrow M \longrightarrow N/M \longrightarrow 0$ qui donne lieu à une suite exacte de k-espaces vectoriels $N \otimes_A k \xrightarrow{g} M \otimes_A k \longrightarrow (N/M) \otimes_A k \longrightarrow 0$. Montrons alors que g est surjective. Pour cela, on utilise le fait que $M \otimes_A k \cong M/\mathfrak{m}M$ via $M \otimes \overline{a} \mapsto \pi(a \cdot m)$. Ainsi, un tenseur pur $m \otimes \overline{a}$ s'identifie à $\pi(a \cdot m)$ soit à une combinaison linéaire à coefficients dans k des $\pi(x_i)$, ainsi

$$\pi(a \cdot m) = \sum_{i=1}^{r} \pi(\lambda_i \cdot x_i)$$

et il est alors clair que l'image de $\sum_{i=1}^{r} x_i \otimes \overline{\lambda_i} \in N \otimes_A k$ est l'élément de départ $m \otimes \overline{a}$. Ainsi, on a la surjectivité et par exactitude, cela entraîne $(M/N) \otimes_A k = \{0\}$. Montrons alors à l'aide du lemme de Nakayama que cela implique $M/N = \{0\}$, soit $M = N$ et on aura (enfin !) gagné ! Si l'on pose $L = M/N$, on a donc $L \otimes_A k \cong L/\mathfrak{m}L = \{0\}$ donc $L = \mathfrak{m}L$ et le lemme de Nakayama implique immédiatement $L = \{0\}$.

13. Il est clair que tout élément de la forme $(z_1, z_2) \in A$ avec $z_1 z_2 \neq 0$ est inversible d'inverse (z_1^{-1}, z_2^{-1}). Par ailleurs, l'idéal I_1 engendré par $(1, 0)$ (qui n'est autre que $\mathbf{C} \times \{0\}$) est maximal car $A/I_1 \cong \mathbf{C}$ et de même pour l'idéal I_2 engendré par $(0, 1)$. Soit alors I un idéal non nul de A. Si I contient un élément $(z_1, z_2) \in A$ avec $z_1 z_2 \neq 0$, alors $I = A$. On peut donc supposer que tout élément non nul de I est de la forme $(z, 0)$ ou $(0, z')$ avec $z \neq 0$ et $z' \neq 0$. Si on a un élément de I de chaque forme, alors $(z, 0) + (0, z') = (z, z') \in I \cap A^\times$ et $I = A$. On peut donc supposer que tout élément de I est de la forme $(z, 0)$. Ainsi $z^{-1}(z, 0) = (1, 0) \in I$ et I contient l'idéal maximal I_1 de sorte que $I = A$ ou $I = I_1$. On raisonne de même dans le cas $(0, z')$. On en déduit qu'on a quatre idéaux dans A, $\{0\}$, I_1, I_2 et A.

On voit immédiatement que M n'est pas libre en tant que A-module car pour $z \neq 0$, on a $(0, z) \cdot (1, 0) = (0, 0)$ et ainsi $(1, 0)$ est de torsion. Il reste alors à voir que $M_{\mathfrak{m}}$ est libre pour tout idéal maximal $\mathfrak{m}$ de A pour en conclure que la liberté n'est en revanche pas une propriété qui passe du local au global. On a vu qu'on avait seulement deux idéaux maximaux $\mathfrak{m}_1 = I_1$ et $\mathfrak{m}_2 = I_2$. Commençons par déterminer $M_{\mathfrak{m}_1}$. Un élément de ce module est une classe d'équivalence $\frac{(z,0)}{(z_1,z_2)}$ avec $(z, 0) \in M$ et $(z_1, z_2) \notin \mathfrak{m}_1$, autrement dit $z_2 \neq 0$. On a alors

$$\frac{(z, 0)}{(z_1, z_2)} = \frac{(0, 0)}{(1, 1)} \quad \text{car} \quad (0, 1) \cdot ((z, 0)(1, 1) - (0, 0)(z_1, z_2)) = (0, 1) \cdot (z, 0) = (0, 0)$$

avec $(0, 1) \notin \mathfrak{m}_1$. On obtient ainsi le module nul qui est libre (de base indexée par $\emptyset$). Reste donc à traiter le cas de $M_{\mathfrak{m}_2}$. Un élément de ce module est une classe d'équivalence $\frac{(z,0)}{(z_1,z_2)}$ avec $(z, 0) \in M$ et $(z_1, z_2) \notin \mathfrak{m}_2$, autrement dit $z_1 \neq 0$. On a alors immédiatement et de même que $\frac{(z,0)}{(z_1,z_2)} = \frac{(\frac{z}{z_1},0)}{(1,1)}$. On obtient alors que le morphisme $M_{\mathfrak{m}_2} \to \mathbf{C}$ donné par $\frac{(z,0)}{(z_1,z_2)} \mapsto \frac{z}{z_1}$ est linéaire injectif et surjectif et donc que $M_{\mathfrak{m}_2} \cong \mathbf{C}$ est libre de rang 1. On parle de module *localement libre* mais non libre. Avec les questions précédentes, on en conclut que $\mathbf{C} \times \mathbf{C}$ est un exemple de module plat non libre.

Problème 2 — Groupes de Galois en petit degré.

Dans tout l'exercice, on se fixe un corps k de caractéristique différente de 2. On fixe dans un premier temps $P \in k[X]$ un polynôme irréductible séparable de degré n et on rappelle que l'on définit son *groupe de Galois* comme $\mathrm{Gal}_k(P) := \mathrm{Gal}(L/k)$ où L est le corps de décomposition de P sur k. On note de plus $r_1, \ldots, r_n$ les racines de P dans L. On définit alors le *discriminant* de P comme étant

$$\Delta_P = \prod_{1 \leqslant i < j \leqslant n} (r_i - r_j)^2.$$

1. Rappeler pourquoi $\mathrm{Gal}_k(P)$ peut être vu comme un sous-groupe transitif de $\mathfrak{S}_n$ et déterminer $\mathrm{Gal}_k(P)$ dans le cas où $n = 2$.
Dans la suite, on verra toujours $Gal_k(P)$ comme un sous-groupe de $\mathfrak{S}_n$.
2. Justifier que $\Delta_P \in k$ et que $k(\sqrt{\Delta_P})$ est une extension galoisienne de k de degré 1 ou 2.
3. Montrer qu'un élément $\sigma \in \mathrm{Gal}_k(P)$ fixe $\sqrt{\Delta_P}$ si, et seulement si, $\sigma \in \mathrm{Gal}_k(P) \cap \mathfrak{A}_n$. En déduire que $k(\sqrt{\Delta_P})$ est l'extension de k correspondant au sous-groupe $\mathrm{Gal}_k(P) \cap \mathfrak{A}_n$ de $\mathrm{Gal}_k(P)$ puis que Δ_P est un carré dans k si, et seulement si, $\mathrm{Gal}_k(P) \subseteq \mathfrak{A}_n$. Où utilise-t-on l'hypothèse sur la caractéristique de k ?
4. On considère dans cette question $k = \mathbf{R}$ et $n = 3$. Montrer que P a des racines multiples si, et seulement si, $\Delta_P = 0$, que P a trois racines réelles si, et seulement si, $\Delta_P > 0$ et deux racines complexes conjuguées et une racine réelle si, et seulement si, $\Delta_P < 0$.
5. Montrer que si $n = 3$, alors si Δ_P est un carré dans k, $\mathrm{Gal}_k(P) = \mathfrak{A}_3$ tandis que si Δ_P n'est pas un carré dans k, $\mathrm{Gal}_k(P) = \mathfrak{S}_3$.

On rappelle que pour $a, b \in \mathbf{Z}$, $\Delta_{X^3+aX+b} = -4a^3 - 27b^2$.

6. Soit $k \in \mathbf{Z}$ et $a = k^2 + k + 7$. Montrer que $X^3 - aX + a$ est irréductible sur $\mathbf{Q}$ et que son groupe de Galois est $\mathfrak{A}_3$.
7. Montrer que si P est irréductible séparable de degré 3, alors si r est une racine de P, le corps de décomposition de P est donné par $k(r, \sqrt{\Delta_P})$.

À présent, on supposera que P est un polynôme séparable irréductible unitaire de degré $n = 4$.

8. Lister les sous-groupes transitifs de $\mathfrak{S}_4$.

On introduit *la résolvante cubique* $R_3(X)$ de $P(X) = X^4 + aX^3 + bX^2 + cX + d$, définie par

$$R_3(X) := (X - (r_1r_2 + r_3r_4))(X - (r_1r_3 + r_2r_4))(X - (r_1r_4 + r_2r_3)) = X^3 - bX^2 + (ac - 4d)X - (a^2d + c^2 - 4bd).$$

9. Montrer que $\Delta_P = \Delta_{R_3}$ et que R_3 est séparable. Expliquer comment vous obtiendriez les coefficients de R_3 fournis ci-dessus.
10. Montrer que si Δ_P n'est pas un carré dans k et que R_3 est irréductible sur k, alors $\mathrm{Gal}_k(P) = \mathfrak{S}_4$.
11. Montrer que si Δ_P est un carré dans k et que R_3 est irréductible sur k, alors $\mathrm{Gal}_k(P) = \mathfrak{A}_4$.
12. Montrer que si Δ_P n'est pas un carré dans k et que R_3 est réductible sur k, alors $\mathrm{Gal}_k(P) \cong \mathbf{D}_4$ ou $\mathbf{Z}/4\mathbf{Z}$.
Indication : on pourra montrer que si $Gal_k(P)$ contient un 3-cycle, alors R_3 est irréductible.
13. Montrer que si Δ_P est un carré dans k et que R_3 est réductible sur k, alors $\mathrm{Gal}_k(P)$ est isomorphe au groupe de Klein.
14. Montrer que $\mathrm{Gal}_k(P)$ est le groupe de Klein si, et seulement si, R_3 est scindé sur k et diédral ou $\mathbf{Z}/4\mathbf{Z}$ si, et seulement si, R_3 possède une unique racine dans k.
15. Dans le cas de $\mathbf{Q}$, montrer que si le groupe de Galois est $\mathbf{Z}/4\mathbf{Z}$, alors $\Delta_P > 0$.
16. On suppose ici que Δ_P n'est pas un carré dans k et que R_3 est réductible sur k. Montrer alors que le groupe de Galois est diédral si, et seulement si, P est irréductible sur $k(\sqrt{\Delta_P})$ tandis qu'il est isomorphe à $\mathbf{Z}/4\mathbf{Z}$ si, et seulement si, P est réductible sur $k(\sqrt{\Delta_P})$.
17. Étudier les cas particuliers de $X^4 + bX^2 + d$ avec b, d entiers et $k = \mathbf{Q}$ ainsi que de $X^4 - X - 1$.
Indication : On pourra utiliser que $\Delta_{X^4+aX+b} = -27a^4 + 256b^3$ et $\Delta_{X^4+aX^2+b} = 16b(a^2 - 4b)^2$.
18. **(Bonus)** Dans cette question, on supposera que k est une extension finie de $\mathbf{Q}$. On appelle une telle extension *un corps de nombres.* Soit $f \in \mathbf{Z}[X_1, \ldots, X_n]$ et $G \leqslant \mathfrak{S}_n$. On note H le sous-groupe des $\sigma \in G$ telles que $\sigma \cdot f = f$. On introduit alors

$$R_G(f, P) = \prod_{\overline{\sigma} \in G/H} (X - f(r_{\sigma(1)}, \ldots, r_{\sigma(n)})) \in L[X].$$

Montrer si $\mathrm{Gal}_k(P) \subseteq G$, alors $R_G(f, P) \in k[X]$ et que si $R_G(f, P)$ a une racine simple dans k, alors $\mathrm{Gal}_k(P)$ est conjugué à un sous-groupe de H.

Solution.
Comme on travaille dans un corps, on supposera sans perte de généralité dans toute la suite que P est unitaire.

1. Je vous renvoie au début de la section 5 du polycopié de théorie de Galois pour la justification que $\mathrm{Gal}_k(P)$ peut se voir comme un sous-groupe transitif de $\mathfrak{S}_n$. On a en particulier que pour tout $\sigma \in \mathrm{Gal}(L/k)$, $\sigma(r_i) = r_{\sigma(i)}$. Lorsque P est de degré 2 irréductible, on sait déterminer les racines de P qui vivent dans[9] $k(\sqrt{\Delta_P})$ qui est de degré 2 (car le polynôme minimal de $\sqrt{\Delta_P}$ sur k est $X^2 - \Delta_P$ irréductible car Δ_P n'est pas un carré car P est irréductible). Ainsi, $L = k(\sqrt{\Delta_P})$ est le corps de décomposition de P sur k et $\mathrm{Gal}_k(P) = \mathrm{Gal}(L/k) \cong \mathbf{Z}/2\mathbf{Z}$ engendré par la conjugaison dans $k(\sqrt{\Delta_P})$.

9. Remarquer que ces racines de $X^2 + bX + c$ sont $\frac{-b \pm \sqrt{b^2-4c}}{2}$ de sorte que

$$\Delta_P = \left(\frac{-b + \sqrt{b^2 - 4c}}{2} - \frac{-b - \sqrt{b^2 - 4c}}{2}\right)^2 = b^2 - 4c$$

et les deux notions de discriminants coïncident heureusement !

2. On a immédiatement que Δ_P est invariant par le groupe de Galois de L (qui permute les racines de P) et donc est élément de k. On a donc soit $\sqrt{\Delta_P} \in k$ auquel cas on est galoisien de degré 1 soit $\sqrt{\Delta_P} \notin k$ et comme précédemment $k(\sqrt{\Delta_P})$ est galoisienne de degré 2.

3. Il est clair que pour tout $\sigma \in \mathrm{Gal}(L/K)$, on a

$$\sigma(\sqrt{\Delta_P}) = \prod_{i<j} \left(r_{\sigma(j)} - r_{\sigma(i)}\right) = \varepsilon(\sigma)\sqrt{\Delta_P}$$

par définition de la signature [10]. On a alors immédiatement la première partie du résultat.
Il est alors immédiat que $k(\sqrt{\Delta_P}) \subseteq L^{\mathrm{Gal}(L/k)\cap\mathfrak{A}_n}$. Si maintenant $\sqrt{\Delta_P} \in k$, on déduit de la première partie de la question que $\mathrm{Gal}(L/k) \cap \mathfrak{A}_n = \mathrm{Gal}(L/k)$ (auquel cas $\mathrm{Gal}_K(P) \subseteq \mathfrak{A}_n$) et on a le résultat par correspondance de Galois car $k(\sqrt{\Delta_P}) = k$. Si $\sqrt{\Delta_P} \notin k$, alors il existe $\sigma \in \mathrm{Gal}(L/k)$ ne fixant pas $\sqrt{\Delta_P}$, autrement dit de signature -1. Ainsi, $\mathrm{Gal}(L/k) \cap \mathfrak{A}_n$ est un sous groupe strict de $\mathrm{Gal}(L/k)$. Il est d'indice [11] 2 dans G, ce qui permet de conclure que $k(\sqrt{\Delta_P}) = L^{\mathrm{Gal}(L/k)\cap\mathfrak{A}_n}$ par correspondance de Galois.
Noter qu'en caractéristique 2, l'extension $L = k(\sqrt{\Delta_P})$ n'est pas galoisienne dans le cas où Δ_P n'est pas un carré dans k ! Il s'agit bien du corps de décomposition du polynôme irréductible $X^2 - \Delta_P$ mais cette extension n'est pas séparable car dans L, $X^2 - \Delta_P = (X - \sqrt{\Delta_P})^2$.
En particulier, le résultat de cette question ne peut être valide car il impliquerait (pusiqu'un sous-groupe d'indice 2 est distingué) que cette extension est galoisienne ! Le problème vient du fait qu'en caractéristique 2, on a également

$$\forall \sigma \in \mathrm{Gal}(L/k), \quad \sigma(\sqrt{\Delta_P}) = \prod_{i<j} \left(r_{\sigma(j)} - r_{\sigma(i)}\right) = \varepsilon(\sigma)\sqrt{\Delta_P} = \sqrt{\Delta_P}.$$

4. Le cas d'une racine multiple est évident d'après la définition du discriminant

$$\Delta = \prod_{i<j} (r_i - r_j)^2.$$

On peut donc supposer que P a 3 racines distinctes dans L. On a deux cas : si une racine est complexe, alors comme P est à coefficients réels, on sait que le conjugué de cette racine est aussi solution et la troisième solution est nécessairement réelle soit P a trois racines réelles. Dans le dernier cas, il est clair que $\Delta > 0$ et dans le premier il est clair que $\Delta < 0$. On a donc que $\Delta > 0$ si, et seulement si, P a trois racines réelles. En effet, si $r_1 = a + bi$, $r_2 = a - bi$, avec $a, b \in \mathbb{R}$, $b \neq 0$ et $r_3 \neq 0$ sont les racines de P dans L, alors $\Delta = -4b^2((a - r_3)^2 + b^2) < 0$.

5. On sait que $\mathrm{Gal}_k(P)$ est un sous-groupe transitif de $\mathfrak{S}_3$. On sait que les sous-groupes de $\mathfrak{S}_3$ sont $\{\mathrm{Id}\}$, d'ordre 2 engendré par une transposition, $\mathfrak{A}_3$ (engendré par un 3-cycle) ou $\mathfrak{S}_3$. Les seuls sous-groupes transitifs sont clairement $\mathfrak{A}_3$ ou $\mathfrak{S}_3$. La question **3.** fournit alors le résultat immédiatement.

►**REMARQUE.–** On peut alors montrer [12] que pour toutes les valeurs de $c \neq 3$ pour lesquelles il est irréductible, $\mathrm{Gal}_k(X^3 - cX - 1) = \mathfrak{S}_3$ et plus généralement que pour tout $b \in \mathbf{Z}^*$, il existe un nombre fini d'entiers a tels que $X^3 + aX + b$ soit réductible ou tel que $X^3 + aX + b$ soit irréductible et $\mathrm{Gal}_k(X^3 + aX + b) = \mathfrak{A}_3$. Il est donc intéressant de chercher une famille infinie de polynômes de groupe de Galois $\mathfrak{A}_3$. Le monde étant bien fait, c'est l'objet de la question suivante !

6. On constate que $k^2 + k + 7 \equiv 1 \pmod 2$ car $k^2 + k \equiv 0 \pmod 2$ pour tout entier k. On en déduit que $X^3 - aX + a \equiv X^3 + X + 1 \pmod 2$. Or, ce polynôme est irréductible sur $\mathbf{F}_2$ car il n'y a aucune racine. On en déduit (puisque P_a est unitaire) comme dans le TD IV que $P_a = X^3 - aX + a$ est irréductible sur $\mathbf{Q}$ (et sur $\mathbf{Z}$ car primitif). On déduit alors de la question **5.** que la détermination du groupe de Galois de P_a dépend de son discriminant

$$\Delta_{P_a} = 4a^3 - 27a^2 = a^2(4a - 27)$$

et ce discriminant est un carré si, et seulement si, $4a - 27$ est un carré. Or, on a par définition de a que

$$4a - 27 = 4k^2 + 4k + 28 - 27 = 4k^2 + 4k + 1 = (2k + 1)^2$$

et on en déduit bien le résultat. Vous pouvez d'ailleurs vous convaincre qu'il s'agit des seules valeurs de a tels que $P_a = X^3 - aX + a$ soit de groupe de Galois $\mathfrak{A}_3$.

10. Dont je rappelle que l'on peut la définir comme

$$\varepsilon(\sigma) = \prod_{i<j} \mathrm{signe}(\sigma(j) - \sigma(i)).$$

11. En effet, on obtient via la signature un morphisme surjectif $\mathrm{Gal}(L/k) \to \{\pm 1\}$ de noyau $\mathrm{Gal}(L/k) \cap \mathfrak{A}_n$.

12. Ce qui fait appel de manière surprenante au grand théorème de Fermat pour $n = 3$. En effet, traitons le cas de $X^3 - cX - 1$ avec c entier and établissons que son groupe de Galois n'est $\mathfrak{A}_3$ que si $c = 3$. Un tel polynôme est irréductible si, est seulement si, $c \notin \{0, 2\}$, ce qui se voit facilement en étudiant ses racines (car on est en degré 3). On suppose donc $c \neq 0, 2$ et on sait que le groupe de Galois est $\mathfrak{A}_3$ si, et seulement si, $4c^3 - 27$ est un carré, autrement dit si l'équation $y^2 = 4x^3 - 27$ a une solution entière en (x, y) avec $x \neq 0, 2$. On voit facilement que $(3, \pm 9)$ sont deux solutions, donnant bien que si $c = 3$, on a un groupe de Galois $\mathfrak{A}_3$. On obtient en réalité *une courbe elliptique* et on peut alors plus généralement chercher ses solutions ou points rationnels (à savoir les x, y solutions dans $\mathbf{Q}$. À travers le changement de variables $r = \frac{9-y}{6x}$ et $s = \frac{9+y}{6x}$ (d'inverse $x = \frac{3}{r+s}$ et $y = \frac{-9(r-s)}{r+s}$), on voit que le problème revient à résoudre $s^3 + t^3 = 1$ dont on sait par le grand théorème de Fermat qu'elle n'admet aucune solution différente de $(1, 0)$ et $(0, 1)$ (ces solutions redonnant les points $(3, \pm 9)$ solutions de l'équation originale !). On peut traiter de manière similaire le cas de $X^3 + aX + b$ en se ramenant à des résultats profonds concernant les points entiers sur une courbe elliptique. Le grand théorème de Fermat est bien sûr hors de portée de ce cours mais le cas $n = 3$ est tout à fait faisable et faisait l'objet du premier DM de l'an dernier !

7. On écrit $P = (X - r)g(X)$ avec $g \in k(r)[X]$ de degré 2 et $g(r) \neq 0$ par séparabilité. On sait alors (car on en est caractéristique différente de 2), que g a pour corps de décomposition $k(r)(\sqrt{\Delta_g})$. Si l'on note r', r'' les racines de g, on a que le corps de décomposition L de P sur k est donné par $L = k(r, r', r'') = k(r)(\sqrt{\Delta_g})$. Or, on obtient que

$$\Delta_p = (r - r')^2(r - r'')^2(r' - r'')^2 = (r - r')^2(r - r'')^2\Delta_g = g(r)^2\Delta_g$$

de sorte que $k(r)(\sqrt{\Delta_g}) = k(r)(\sqrt{\Delta_P})$ et finalement $L = k(r)(\sqrt{\Delta_f}) = k(r, \sqrt{\Delta_f})$.

►**Remarque.–**Noter qu'à nouveau la caractéristique 2 est là encore essentielle ! Le résultat est faux si k est de caractéristique 2. Par exemple sur $k = \mathbf{F}_2(T)$ et $P = X^3 + TX + T \in k[X]$. Alors P est irréductible (par exemple par Eisenstein avec T) et de discriminant T^2 de sorte que $k(r, \sqrt{\Delta_P}) = k(r)$ mais on peut montrer que le corps de décomposition de P est de degré 6 sur k. En particulier, le groupe de Galois de ce polynôme n'est pas $\mathfrak{A}_3$ mais $\mathfrak{S}_3$ bien que son discriminant soit un carré. Pour le démontrer, on peut recourir à la théorie des résolvantes comme par exemple ici. Dans ce cas, le groupe de Galois est $\mathfrak{A}_3$ si, et seulement si, le polynôme de degré 2 suivant $X^2 + uX + u^3 + u^2$ est réductible et $\mathfrak{S}_3$ sinon. Or, ce polynôme n'a pas de racine dans k.

8. On peut dresser (comme dans le cas $\mathfrak{S}_3$ ou $\mathfrak{A}_4$ traité dans l'exercice 1 du TD I), la liste de tous les sous-groupes de $\mathfrak{S}_4$ et vérifier s'ils sont transitifs ou non. On a $\#\mathfrak{S}_4 = 24$. Le seul sous-groupe d'ordre 1 est $\{\mathrm{Id}\}$ non transitif. Les sous-groupes d'ordre 2 sont engendrés par un élément d'ordre 2 donc soit par une transposition (et fixent donc deux éléments de $\{1, \ldots, 4\}$) et sont donc non transitifs soit par une double transposition et alors ils ne sont pas non plus transitifs (par exemple $(12)(34)$ ne peut pas envoyer 1 sur 4). Idem pour les sous-groupes d'ordre 3 engendrés par un élément d'ordre 3, autrement dit par un 3-cycle. Les sous-groupes d'ordre 4 sont soit $\mathbf{Z}/4\mathbf{Z}$ engendré par un 4-cycles (et donc transitifs) soit $(\mathbf{Z}/2\mathbf{Z})^2$ engendré par deux éléments d'ordre deux qui commutent. On obtient ainsi le sous-groupe engendré par les doubles transpositions qui est transitif (car il contient toutes les doubles transpositions) et les sous-groupes engendrés par deux transpositions à supports disjoints qui n'est pas transitif[13]. Les sous-groupes d'ordre 6 sont isomorphes à $\mathfrak{S}_3$ (et sont en fait le fixateur d'un élément et donc non transitifs) engendré par une transposition et un 3-cycle (on n'a pas d'élément d'ordre 2 qui commutent avec un élément d'ordre 3 et si on contient un 3-cycle et une double tansposition, alors on contient tous les 3-cycles et donc $\mathfrak{A}_4$). Ces sous-groupes ne sont pas transitifs. Passons alors aux sous-groupes d'ordre 8. On voit facilement qu'on n'a pas de tel groupe abélien car pas d'élément d'ordre 8, ni de triplet d'éléments d'ordre 2 qui commutent 2 à 2 ni d'élément d'ordre 4 commutant à un élément d'ordre 2. On sait qu'alors à isomorphisme près, il ne reste que $\mathbf{D}_4$ et $\mathbf{H}_8$ comme groupes d'ordre 8 et on n'a pas de copie de $\mathbf{H}_8$ (car on n'a pas trois éléments d'ordre 4 vérifiant les relations du groupe des quaternions). Il vient qu'on obtient des copies de $\mathbf{D}_4$ engendrés par un 4-cycle et une transposition (voir l'exercice sur le groupe diédral du TD I et le treillis de $\mathfrak{S}_4$). Ces sous-groupes sont transitifs (car ils contiennent un 4-cycle). Pour l'ordre 12, on a uniquement $\mathfrak{A}_4$ qui est transitif et pour 24, $\mathfrak{S}_4$ qui est transitif.
En conclusion, les sous-groupes transitifs de $\mathfrak{S}_4$ sont $\mathfrak{S}_4$, $\mathfrak{A}_4$, les trois copies de $\mathbf{D}_4$ engendrés par un 4-cycle et une transposition (qui sont en fait les 2-Sylows), le groupe de Klein $(\mathbf{Z}/2\mathbf{Z})^2$ engendré par les doubles transpositions et les trois groupes $\mathbf{Z}/4\mathbf{Z}$ engendrés par un 4-cycle. De manière plus élémentaire pour les sous-groupes d'ordre 8, on peut voir qu'il ne peut pas contenir que des éléments d'ordre 2 (sinon on a toutes les transpositions qui engendre $\mathfrak{S}_4$). On a donc nécessairement un élément d'ordre 2 et un élément d'ordre 4. Si on a une double transposition et un 4-cycle, on obtient à nouveau $\mathfrak{S}_4$ tout entier. On a donc un 4-cycle et une transposition et on reconnaît la relation du groupe diédral. On pouvait aussi dire qu'il s'agit d'un 2-Sylow et que tous ces groupes sont conjugués et en exhiber un ! Noter que puisque le cardinal d'une orbite doit diviser le cardinal du sous-groupe transitif, un tel sous-groupe transitif est toujours de cardinal divisible par 4 (et par n dans $\mathfrak{S}_n$) et on pouvait donc commencer notre liste aux sous-groupes de cardinal 4.

9. Par définition, on a

$$\Delta_{R_3} = (r_1r_2 + r_3r_4 - r_1r_3 - r_2r_4)^2(r_1r_2 + r_3r_4 - r_1r_4 - r_2r_3)^2(r_1r_3 + r_2r_4 - r_1r_4 - r_2r_3)^2.$$

On a alors par exemple

$$r_1r_2 + r_3r_4 - r_1r_3 - r_2r_4 = r_1(r_2 - r_3) - r_4(r_2 - r_3) = (r_1 - r_4)(r_2 - r_3)$$

et il en découle immédiatement que $\Delta_{R_3} = \Delta_P$. On a donc que si P est séparable (ce qui est équivalent à $\Delta_P \neq 0$), alors $\Delta_{R_3} \neq 0$ et R_3 est sans racine multiple donc séparable. Pour obtenir l'expression de R_3, on utiliserait l'algorithme permettant d'exprimer les polynômes symétriques en fonction de spolynômes symétriques élémentaires (qui eux ont une expression en fonction des coefficients de P grâce aux relations racines-coefficients).

10. On suppose ici que Δ_P n'est pas un carré dans k et que R_3 est irréductible sur k. La première hypothèse implique que $\mathrm{Gal}_k(P)$ n'est pas contenu dans $\mathfrak{A}_4$. Par ailleurs, si R_3 est irréductible sur k, alors $k(r_1r_2 + r_3r_4)$ est une sous-extension de L de degré 3 (un corps de rupture de R_3). On en déduit que le degré de L (et donc celui du groupe de Galois $\mathrm{Gal}_k(P)$) est divisible par 3. Mais il contient aussi un corps de rupture $k(r_1)$ de P et est donc aussi divisible par 4. Il s'ensuit qu'il est divisible par 12 et comme il n'est pas contenu dans $\mathfrak{A}_4$, on obtient $\mathrm{Gal}_k(P) = \mathfrak{S}_4$.

11. Le même raisonnement fournit que le cardinal de $\mathrm{Gal}_k(P)$ est divisible par 12 et que $\mathrm{Gal}_k(P) \subseteq \mathfrak{A}_4$ donc $\mathrm{Gal}_k(P) = \mathfrak{A}_4$.

13. Penser à $\{\mathrm{Id}, (12), (34), (12)(34)\}$.

12. Supposons que Δ_P n'est pas un carré dans k et que R_3 est réductible sur k. À nouveau, on en déduit que $\mathrm{Gal}_k(P)$ n'est pas contenu dans $\mathfrak{A}_4$ et a un cardinal divisible par 4. Il suffit alors de montrer que $\mathrm{Gal}_k(P) \neq \mathfrak{S}_4$. Si on avait $\mathrm{Gal}_k(P) = \mathfrak{S}_4$, alors en particulier, $\sigma = (123)$ serait un élément du groupe de Galois et

$$\sigma(r_1r_2 + r_3r_4) = r_2r_3 + r_1r_4 \quad \text{et} \quad \sigma^2(r_1r_2 + r_3r_4) = r_3r_1 + r_2r_4$$

et ainsi puisque les trois racines de R_3 sont distinctes, on a exhibé un élément du groupe de Galois qui ne fixe aucune des racines de R_3, contredisant le fait qu'il soit réductible sur k (un polynôme de degré 3 est réductible si, et seulement s'il a une racine). Dit autrement, on voit que l'action du groupe de Galois est transitive sur l'ensemble des racines de R_3 et on sait que cela impliquerai que R_3 est irréductible sur k. On a donc le résultat.

13. De même, on obtient que $\mathrm{Gal}_k(P) \subseteq \mathfrak{A}_4$ et donc d'après la question **8.**, on a que $\mathrm{Gal}_k(P) = \mathfrak{A}_4$ ou $\mathrm{Gal}_k(P) \cong (\mathbf{Z}/2\mathbf{Z})^2$. Comme $\mathfrak{A}_3$ est engendré par les 3-cycles et que la copie du groupe de Klein n'en contient aucun, on conclut comme dans la question précédente !

14. On a vu en question précédente, que $\mathrm{Gal}_k(P)$ est le groupe de Klein si, et seulement si, R_3 est réductible et Δ_P est un carré. Or, R_3 réductible et $\Delta_{R_3} = \Delta_P$ et le corps de décomposition de R_3 est donné par $k(r_1r_2 + r_3r_4, \sqrt{\Delta_{R_3}}) = k(\sqrt{\Delta_{R_3}})$ d'après **7.** et en prenant r la racine de R_3 dans k. On a alors $\sqrt{\Delta_{R_3}} = \sqrt{\Delta_P} \in k$ et donc ce corps de décomposition n'est autre que k et on a donc bien que R_3 est scindé sur k. La réciproque est évidente car dans ce cas, Δ_{R_3} est un carré dans k et R_3 est réductible.
Si maintenant le groupe de Galois est $\mathbf{Z}/4\mathbf{Z}$ ou diédral, alors R_3 est réductible et donc possède une racine $r \in k$ et Δ_{R_3} n'est pas un carré dans k. Un corps de décomposition de R_3 est alors $k(\sqrt{\Delta_{R_3}})$ qui est une extension de degré 2 et ainsi R_3 n'est pas scindé sur k et donc comme il est de degré 3, il possède une unique racine dans k. Réciproquement, on voit que si R_3 n'a qu'une racine dans k, son discriminant de peut être un carré (sinon on peut factoriser la partie quadratique restante en caractéristique différente de 2). On a donc le résultat !

15. Supposons ici que $\mathrm{Gal}_k(P) \cong \mathbf{Z}/4\mathbf{Z}$. On obtient alors que L est de degré 4 et comme elle contient un corps de rupture de P aussi de degré 4, on a que le corps de décomposition est égal à tout corps de rupture de P. On en déduit que si P possède une racine réelle r, alors $L = k(r)$ est réel et toutes les racines de P sont réelles. On a donc deux cas : soit P n'a que des racines réelles et alors clairement $\Delta_P > 0$ soit P possède uniquement des racines complexes non réelles conjuguées 2 à 2, que l'on notera $z, \overline{z}$ et $w, \overline{w}$. Un calcul fournit alors

$$\Delta_P = (z-\overline{z})(z-w)(z-\overline{w})(\overline{z}-w)(\overline{z}-\overline{w})(w-\overline{w}) = |z-w|^2|z-\overline{w}|^2(z-\overline{z})(w-\overline{w}).$$

Si on écrit alors $z = a + ib$ et $w = c + id$, on a alors $(z-\overline{z})(w-\overline{w}) = -4bd$ avec $bd \neq 0$ car les racines ne sont pas réelles. Le résultat est alors immédiat en prenant le carré !

On a ainsi un premier critère (non suffisant !) : si le discriminant n'est pas un carré et que R_3 est réductible et $\Delta_P < 0$, alors $\mathrm{Gal}_k(P) \cong \mathbf{D}_4$.

16. Supposons ici que R_3 est réductible et ne possède qu'une seule racine dans k et que Δ_P n'est pas un carré dans k. Si le groupe de Galois est donné par $\mathbf{Z}/4\mathbf{Z}$, engendré par[14] σ, on a vu que $L = k(r_1)$ pour raisons de degré et on a par correspondance de Galois une unique sous-extension de degré 2 engendrée par σ^2. On a alors que le corps de décomposition de R_3 est $k(\sqrt{\Delta_P})$ de degré 2 et qui est contenu dans L (par définition du discriminant ou car L est normale et $X^2 - \Delta$ admet une racine dans L). On en déduit que $k(\sqrt{\Delta_P}) = L^{\langle\sigma^2\rangle}$ et donc $[L : k(\sqrt{\Delta_P})] = 2$ et donc P est réductible sur $k(\sqrt{\Delta_P})$ (sinon $L = k(r_1) = k(\sqrt{\Delta_P})(r_1)$ serait un corps de rupture et donc de degré 4).
Si maintenant le groupe de Galois est diédral. On va utiliser à nouveau la correspondance de Galois. On a que G est engendré par une transposition τ et par un 4-cycle σ. Si on impose que $r_1r_2 + r_3r_4$ est la racine dans k, on peut choisir $\sigma = (1324)$ et $\tau = (34)$. On a alors $\mathrm{Gal}_k(P) = \langle\sigma, \tau\rangle$. On a alors que le corps fixé par τ n'est autre que $k(r_1)$. En effet, ce corps est de degré 4 donc correspond à un sous-groupe d'ordre 2 et il est clair que $\tau = (34)$ fixe r_1. De même, $k(\sqrt{\Delta_P})$ correspond au sous-groupe d'ordre 4 $\langle\sigma^2, \sigma\tau\rangle$ car il correspond au sous-groupe du groupe de Galois des permutations de signature 1 d'après les questions précédentes. On en déduit que $k(r_1, \sqrt{\Delta_P})$ est fixé par un élément du groupe de Galois si, et seulement si, cet élément fixe r_1 et fixe $\sqrt{\Delta_P}$, autrement dit si, et seulement si, cet élément est l'identité ou τ et appartient à $\langle\sigma^2, \sigma\tau\rangle = \{\mathrm{Id}, (12)(34), (13)(24), (14)(23)\}$. On a donc que $k(r_1, \sqrt{\Delta_P}) = L^{\mathrm{Id}} = L$ et le corps de décomposition de P est donc $k(r_1, \sqrt{\Delta_P})$. On en déduit, puisque $k(\sqrt{\Delta_P})$ est de degré 2, que $[k(r_1, \sqrt{\Delta_P}) : k(\sqrt{\Delta_P})] = 4$. Ainsi, $L = k(\sqrt{\Delta_P})(r_1)$ est un corps de rupture de P sur $k(\sqrt{\Delta_P})$ est de degré 4 donc P (qui est de degré 4) est irréductible sur $k(\sqrt{\Delta_P})$. Comme tous les cas sont mutuellement exclusifs, on obtient le résultat !

17. Il suffit d'appliquer les résultats des questions précédentes ! Le discriminant de $P = X^4 + bX^2 + d$ est $\Delta_P = 16d(b^2 - 4d)^2$. On impose donc que $d \neq 0$ et $4d \neq b^2$ afin que le polynôme soit séparable. On cherche alors les valeurs de b et d tels que ce polynôme soit irréductible. Il est facile de voir que P n'a pas de racines dans $\mathbf{Q}$ si, et seulement si $b^2 - 4d$ n'est pas un carré ou si $b^2 - 4d$ est un carré mais que $\frac{-b\pm\sqrt{b^2-4d}}{2}$ n'en est pas un (on exploite l fait que l'équation soit bicarrée). Si maintenant on avait une factorisation comme un produit de deux polynômes de degré 2, on aurait

$$X^4 + bX^2 + d = (X^2 + \alpha X + \beta)(X^2 - \alpha X + \beta) = X^4 + (2\beta - \alpha^2)X^2 + \beta^2 \quad \text{ou} \quad X^4 + bX^2 + d = (X^2 - \beta)(X^2 - \beta').$$

On obtient donc dans le premier cas qu'on doit imposer que d n'est pas un carré ou alors si d est un carré, $\pm 2\sqrt{d} - b \neq \square$ tandis que dans le second cas on a $\beta + \beta' = -b$ et $\beta\beta' = d$ ce qui impose que β et β' sont les racines de $X^2 - bX + d$. On a alors puisque

14. En fait, on n'a pas le choix, $\sigma = (1324)$ ou son inverse en étudiant l'effet de chaque 4-cycle sur $r_1r_2 + r_3r_4$ si l'on suppose que $r_1r_2 + r_3r_4$ est l'unique racine de R_3 dans k.

b^2-4d n'est pas un carré dans $\mathbf{Q}$ que ce polynôme n'a pas de racines rationnelles. Supposons alors que le polynôme est irréductible. C'est un carré dans $\mathbf{Q}$ si, et seulement, si d n'est pas un carré car sinon b^2-4d serait un carré ce qui contredit l'irréductibilité ! On a alors la cubique résolvante

$$X^3-bX^2-4dX+4bd=(X-b)(X^2-4d)$$

qui est toujours réductible. On obtient donc le résultat suivant

- Si d est un carré dans $\mathbf{Q}$, $\mathrm{Gal}_k(P)\cong(\mathbf{Z}/2\mathbf{Z})^2$;
- Si d n'est pas un carré dans $\mathbf{Q}$, et $(b^2-4d)d$ est un carré dans $\mathbf{Q}$, alors $\mathrm{Gal}_k(P)\cong\mathbf{Z}/4\mathbf{Z}$;
- Si d n'est pas un carré dans $\mathbf{Q}$, et $(b^2-4d)d$ n'est pas un carré dans $\mathbf{Q}$, alors $\mathrm{Gal}_k(P)\cong\mathbf{D}_4$.

En effet, dans le cas $d\neq\square$, il s'agit de déterminer si $P=X^4+bX^2+d$ est irréductible ou non sur $\mathbf{Q}(\sqrt{d})$. On voit que P est bicarré et le discriminant de T^2+bT+d est b^2-4d et on constate que cette quantité est un carré dans $\mathbf{Q}(\sqrt{d})$ si, et seulement si,

$$(\alpha+\beta\sqrt{d})^2=\alpha^2+d\beta^2+2\alpha\beta\sqrt{d}=b^2-4d$$

avec $\alpha\neq0$ par irréductibilité sur $\mathbf{Q}$. On en déduit donc (puisque $(1,\sqrt{d})$ est libre sur $\mathbf{Q}$) que $\alpha=0$ et donc $\beta^2d=b^2-4d$ soit si, et seulement si, $d(b^2-4d)$ est un carré de $\mathbf{Q}$. Dans ce cas, il est clair que $P=\left(X^2-\frac{-b+\beta\sqrt{d}}{2}\right)\left(X^2-\frac{-b-\beta\sqrt{d}}{2}\right)$ est réductible sur $\mathbf{Q}(\sqrt{d})$. Dans le cas contraire, si $d(b^2-4d)$ n'est pas un carré de $\mathbf{Q}$, alors on déduit de ce qui précède que le polynôme P n'a pas de racine $\mathbf{Q}(\sqrt{d})$. pour déterminer s'il est irréductible ou non, reste à voir s'il peut s'écrire comme un produit de deux polynômes irréductibles de degré 2 sur $\mathbf{Q}(\sqrt{d})$. Si on a

$$X^4+bX^2+d=(X^2+\alpha X+\beta)(X^2-\alpha X+\beta)=X^4+(2\beta-\alpha^2)X^2+\beta^2$$

alors $\beta=\pm\sqrt{d}$ et la relation $2\beta-\alpha^2=b$ fournit en écrivant $\alpha=\gamma+\delta\sqrt{d}$ avec $\gamma,\delta\in\mathbf{Q}$, il vient dans la base $(1,\sqrt{d})$ la relation $\gamma\delta=1$ et

$$\gamma^2+d\delta^2+b=0\quad\text{soit}\quad\gamma^4+b\gamma^2+d=0$$

ce qui n'est pas possible car P est irréductible sur $\mathbf{Q}$. La seule factorisation possible est donc de la forme

$$X^4+bX^2+d=(X^2-\beta)(X^2-\beta').$$

On aurait alors $\beta\beta'=d$ et $\beta+\beta'=-b$ donc β et β' sont racine du polynôme X^2-bX+d de discriminant b^2-4d qui est un carré dans $\mathbf{Q}(\sqrt{d})$ mais pas dans $\mathbf{Q}$ si, et seulement si, $d(b^2-34d)$ est un carré. On en déduit le résultat.
Passons [15] à $P=X^4-X-1$. On obtient l'irréductibilité comme dans la question 3 du TD 4 exercice 13 ou l'exercice 12. Le discriminant vaut alors -283 qui n'est pas un carré. On a alors $R_3=X^3+4X-1$. On vérifie alors que R_3 n'a pas de racine rationnelle car une telle racine $x=\frac{p}{q}$ avec p et q premiers entre eux donnerait lieu à

$$p^3=-4pq^3+q^4$$

de sorte que $q\in\{\pm1\}$ et donc $p(p^2+4q^3)=1$ et $p\in\{\pm1\}$ et on vérifie que ni 1 ni -1 n'est racine. Ainsi comme on est en degré 3, R_3 est irréductible et on en déduit que $\mathrm{Gal}_k(P)=\mathfrak{S}_4$. Un exemple de groupe de Galois $\mathfrak{A}_4$ est donné par $X^4+8X+12$ et ainsi tous les cas apparaissent ! Il est d'ailleurs intéressant de s'interroger sur la fréquence de chacun des cas ! Cela nous emmènerait trop loin mais on peut démontrer (dans un sens précis) que 100% des polynômes irréductibles de degré n sur $\mathbf{Q}$ ont pour groupe de Galois $\mathfrak{S}_n$ et ces questions sont toujours un sujet de recherche actif et passionnant, en témoigne l'article récent suivant du médaillé Fields Manjul Bhargava ! Cela pose aussi le problème de Galois inverse, à savoir de construire un polynôme de groupe de Galois donné.

►**Remarque.–** On remarque que la distinction entre le cas diédral et $\mathbf{Z}/4\mathbf{Z}$ n'est pas optimal car il n'est pas immédiat en général d'étudier l'irréductibilité d'un polynôme de degré 4. On peut, dans l'esprit de la question suivante, introduire des résolvantes quadratiques. En effet, si on note [16] r' l'unique racine de P sur k, on pose $R_2(X)=X^2+aX+(b-r')$ et $r_2(X)=X^2-r'X+d$ si $P=X^4+aX^3+bX^2+cX+d$. On peut alors montrer à l'aide de la correspondance de Galois que $\mathrm{Gal}_k(P)$ est $\mathbf{Z}/4\mathbf{Z}$ si R_2 et r_2 sont réductibles sur $k(\sqrt{\Delta_P})$ et diédral sinon. Une preuve est disponible ici. Pour un polynôme de degré 2, il est facile de détecter une telle irréductibilité en calculant le discriminant. On peut alors établir que si Δ_P n'est pas un carré, alors si $(a^2-4(b-r'))\Delta_P$ et $(r'^2-4d)\Delta_P$ sont des carrés dans k, alors $\mathrm{Gal}_k(P)\cong\mathbf{Z}/4\mathbf{Z}$ tandis que dans le cas contraire, il est diédral.

18. Pa définition de H, le polynôme $R_G(f,P)$ est bien défini. Supposons que $\mathrm{Gal}_k(P)\leqslant G$. On a alors que pour tout $\sigma\in\mathrm{Gal}_k(P)$, l'application $\overline{\mu}\mapsto\overline{\sigma\circ\mu}$ est une bijection de G/H. En effet, par cardinalité, il suffit de montrer l'injectivité et si $\overline{\sigma\circ\mu}=\overline{\sigma\circ\mu'}$, alors il existe $h\in H$ tel que $\sigma\circ\mu=\sigma\circ\mu'\circ h$ et en simplifiant par σ qui est une bijection, il vient $\overline{\mu}=\overline{\mu'}$. On a donc

$$\begin{aligned}\sigma(R_G(f,P))=\prod_{\overline{\mu}\in G/H}\left(X-\sigma(f(r_{\mu(1)},\dots,r_{\mu(n)}))\right)&=\prod_{\overline{\mu}\in G/H}\left(X-f(r_{\sigma\circ\mu(1)},\dots,r_{\sigma\circ\mu(n)})\right)\\&=\prod_{\overline{\mu'}\in G/H}\left(X-f(r_{\mu'(1)},\dots,r_{\mu'(n)})\right)=R_G(f,P)\end{aligned}$$

15. De manière générale, on peut établir que le polynôme X^n-X-1 est irréductible de groupe de Galois $\mathfrak{S}_n$ pour tout entier n (voir ici).
16. Noter qu'une telle racine rationnelle est facile à déterminer !

en posant $\overline{\mu'} = \overline{\sigma \circ \mu}$. On a donc bien dans ce cas que $R_G(f,P) \in k[X]$. Noter qu'on prend G/H pour éviter les facteurs carrés car deux éléments égaux modulo H donnent lieu au même facteur!

Supposons alors à présent que $R_G(f,P)$ possède une racine simple $f(r_{\sigma(1)},\dots,r_{\sigma(n)})$ dans k avec $\sigma \in G$. On a en particulier, pour tout $\tau \in \mathrm{Gal}_k(P)$,

$$\tau(f(r_{\sigma(1)},\dots,r_{\sigma(n)})) = f(r_{\tau\circ\sigma(1)},\dots,r_{\tau\circ\sigma(n)}) = f(r_{\sigma(1)},\dots,r_{\sigma(n)}).$$

On en déduit que $\overline{\tau\circ\sigma} = \overline{\sigma}$ car sinon, on obtiendrait que $f(r_{\sigma(1)},\dots,r_{\sigma(n)})$ est une racine au moins double. On a donc que $\sigma^{-1}\tau\sigma \in H$ et ainsi $\sigma^{-1}\mathrm{Gal}_k(P)\sigma \leqslant H$ et on en déduit le résultat. Il s'agit même d'une équivalence.

►**Compléments.–** Tout ce qui précède peut se réécrire en termes de résolvante et en réalité, il s'agit de la méthode utilisée pour calculer en pratique des groupes de Galois de façon effective. Je vous renvoie pour cela par exemple à l'ouvrage *A course in computational algebraic number theory* de H. Cohen section 6.3. La méthode est en gros la suivante : On fait la liste des sous-groupes transitifs de[17] $\mathfrak{S}_n$. On considère ensuite un par un les sous-groupes transitifs maximaux. Pour chaque tel sous-groupe H de $G = \mathfrak{S}_n$, on détermine un polynôme f tel que H soit le stabilisateur de f et on calcule $R_G(f,P)$ (s'il admet des facteurs carrés, on dispose de méthode pour se ramener au cas sans facteur carré comme expliqué dans le Cohen). On cherche alors les racines rationnelles de $R_G(f,P)$ (ce qui est classique et aisé). Si pour tout sous-groupe transitif maximal, on ne trouve aucune racine, alors $\mathrm{Gal}_k(P) \cong \mathfrak{S}_n$ et sinon, à conjugaison près, on peut supposer qu'on a trouvé un H transitif maximal tel que $\mathrm{Gal}_k(P) \leqslant H$. On remplace alors G par H et on itére le procédé avec les sous-groupes transitifs maximaux contenus dans H. On en déduit alors que soit $\mathrm{Gal}_k(P) \cong H$ soit que $\mathrm{Gal}_k(P)$ est contenu (à conjugaison près) dans un sous-groupe transitifs strict de H. On peut ainsi écarter une à une les possibilités jusqu'à obtenir le groupe de Galois. On peut évidemment être plus rapide en choisissant judicieusement les f comme dans le Cohen.

Dans l'exercice, la question **3.** et le cas de $\mathfrak{S}_3$ découlent du cas $G = \mathfrak{S}_n$, $H = \mathfrak{A}_n$ et

$$f = \prod_{i<j}(X_i - X_j) \quad \text{fournissant} \quad R_G(f,P) = X^2 - \Delta_P.$$

On a ensuite dans le cas $n = 4$, que (où en fait ici H est diédral)

$$R_3(X) = R_{\mathfrak{S}_4}(X_1X_2 + X_3X_4, P).$$

On aurait aussi pu utiliser $R_{\mathfrak{S}_4}((X_1+X_2)(X_3+X_4),P)$ ou une résolvante plus compliquée *a priori* mais qui ne nécessite pas de seconde résolvante utilisée dans le Cohen. Ensuite, pour distinguer entre le cas diédral et $\mathbf{Z}/4\mathbf{Z}$, on peut déduire de la question **18.** qu'à conjugaison près, $\mathrm{Gal}_k(P)$ est contenu dans un groupe diédral. On a alors besoin d'une nouvelle résolvante et on peut utiliser celle du Cohen ou celles de la remarque en fin de question **17.** qui correspondent à

$$R_{\mathbf{D}_4}(X_1+X_2,P) \quad \text{et} \quad R_{\mathbf{D}_4}(X_1X_2,P)$$

avec H cyclique d'ordre 4. La nécessité d'utiliser deux résolvantes s'explique ici par le fait qu'on s'assure ainsi que l'une ou l'autre soit sans facteur carré. Je vous renvoie pour plus de détails ici ou ici.

17. Connu à l'heure actuelle jusqu'à $n = 32$.