Algèbre et théorie de Galois - TD1

Exercice 1 : Donner une représentation fidèle M de S_n sur un $\mathbb{Z}$-module convenable. En déduire une description matricielle des éléments de S_n. Si $\sigma \in S_n$, que vaut $\det(\sigma)$?

Exercice 2 : Expliciter les classes de conjugaison dans S_3 et S_4. Déterminer la cardinalité et l'ordre commun de tous les éléments de chaque classe de conjugaison.

Exercice 3 : Soit $n \geq 3$.

a) Montrer que le produit de deux transpositions distinctes est un 3-cycle ou un produit de deux 3-cycles. En déduire que le groupe A_n est engendré par les 3-cycles.

b) Montrer qu'un sous-groupe $H \subset S_n$ d'ordre $n!/2$ est forcément égal à $H = A_n$.

Exercice 4 : Montrer que si un groupe simple G agit transitivement sur un ensemble X tel que $|X| \geq 2$, alors l'action est fidèle. Que se passe-t'il si G n'est pas simple ?

Exercice 5 : Conjugaison dans S_n et A_n.

a) Pour tout $\sigma \in S_n$, déterminer $|C_{S_n}(\sigma)|$ en termes de la longueur des cycles disjoints dans la notation cyclique de σ.

b) Soit $\sigma \in A_n$ ($n \geq 2$). Montrer qu'il y a deux cas possibles :

i) $C_{S_n}(\sigma) \subset A_n \Rightarrow C_{S_n}(\sigma) \subset C_{A_n}(\sigma) \Rightarrow$ la classe de conjugaison de σ and S_n est une réunion de deux classes de conjugaison dans A_n.

ii) $C_{S_n}(\sigma) \subsetneq A_n \Rightarrow C_{A_n}(\sigma)$ est un sous-groupe de $C_{S_n}(\sigma)$ d'indice $2 \Rightarrow$ la classe de conjugaison de σ dans S_n est égale à la classe de conjugaison de σ dans A_n.

c) Distinguer les deux cas précédents en termes du type cyclique de σ.

d) Expliciter les classes de conjugaison dans A_3 et A_4.

Exercice 6 : Si $X \subset \mathbb{R}^d$ est un sous-ensemble, on note $G(X) = \{g \in O(n) |\, g(X) = X\}$ et $G^+(X) = \{g \in O^+(n) |\, g(X) = X\}$. Soit $C_n \subset \mathbb{R}^n$ l'hypercube de sommets $(\pm 1, \ldots, \pm 1)$.

a) Montrer que l'action de $G(C_3)$ sur les 4 diagonales de C_3 induit un isomorphisme $G^+(C_3) \xrightarrow{\sim} S_4$.

b) En déduire que $G(C_3)$ est isomorphe à $S_4 \times \{\pm 1\}$.

c) Ecrire explicitement toutes les matrices de $G(C_3) \subset O(3)$.

d) Calculer l'ordre de $G(C_n)$.

e) Ecrire explicitement toutes les matrices de $G(C_n)$.

f) Montrer que le groupe $G(C_n)$ contient un sous-groupe N (resp. H) isomorphe à $\{\pm 1\}^n$ (resp. à S_n). Décrire la structure de $G(C_n)$ en termes de N et H.

Exercice 7 : Soit T le tétraèdre régulier de centre l'origine. En choisissant une numérotation des quatres sommets de T, on obtient un morphisme de groupes $\alpha : G(T) \to S_4$. Montrer que α définit des isomorphismes $G(T) \xrightarrow{\sim} S_4$ et $G^+(T) \xrightarrow{\sim} A_4$.

Exercice 8 : Le "corps à un élément" (Tits). Soit K un corps fini et $q = |K|$. Calculer ($n \geq 1$) :

a) $|\mathrm{GL}_n(K)|$, $|\mathrm{SL}_n(K)|$.

b) $|\mathrm{Gr}_n^k(K)|$ où $\mathrm{Gr}_n^k(K)$ est l'ensemble $\{V \subset K^n |\, V$ sous-espace vectoriel de dimension $k\}$, pour $1 \leq k \leq n-1$.

c) $|\mathrm{GA}_n(K)|$.

d) $|\mathrm{Graff}_n^k(K)|$ pour $\mathrm{Graff}_n^k(K) = \{V \subset K^n | \, V \text{ sous-espace affine de dimension } k\}$, pour $1 \leq k \leq n-1$.

e) Pour chaque domaine X de l'exercice, on note $|X(\mathbb{F}_1)| := \lim_{q \to 1}(q-1)^{-k}|X(\mathbb{F}_q)|$ où k est le plus petit entier naturel pour lequel cette limite n'est pas nulle. Calculer $|X(\mathbb{F}_1)|$ pour chaque domaine X. Donner des ensembles naturels, qu'on notera $X(\mathbb{F}_1)$, représentant ces cardinaux.

Exercice 9 : (Difficile) Construire un ensemble naturel à 5 éléments muni d'une action de $\mathrm{PSL}_2(\mathbb{F}_5)$. En déduire un isomorphisme $\mathrm{PSL}_2(\mathbb{F}_5) \cong A_5$.

Exercice 10 : Soit C un groupe cyclique d'ordre $n \geq 1$. Soit σ un générateur de C.

a) Montrer que tout sous-groupe de C est cyclique.

b) Pour tout $a \in \{1, \ldots, n\}$, montrer que l'ordre de σ^a est égal au dénominateur d (on écrit $\frac{a}{n} = \frac{p}{d}$ avec $(p,d) = 1$) de la fraction $\frac{a}{n}$.

c) Montrer que, pour tout diviseur d de n, le nombre d'éléments de C d'ordre d est égal à $\varphi(d)$.

Exercice 11 : Montrer que $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

Exercice 12 :

a) Montrer qu'il n'y a que quatre anneaux (commutatifs, unitaires) à 4 éléments, à savoir $A = \mathbb{Z}/4\mathbb{Z}$, $\mathbb{F}_2 \times \mathbb{F}_2$, $\mathbb{F}_4$, $\mathbb{F}_2[\epsilon]/(\epsilon^2)$.

b) Dans chacun des cas, déterminer la structure des groupes $A^\times$ et $GA_1(A) \subset S_A \xrightarrow{\sim} S_4$.

Exercice 13 :

a) Montrer que l'ordre du groupe $G = \mathrm{PGL}_3(\mathbb{F}_2) = \mathrm{GL}_3(\mathbb{F}_2) = \mathrm{SL}_3(\mathbb{F}_2) = \mathrm{PSL}_3(\mathbb{F}_2)$ est égal à $168 = |\mathrm{PSL}_2(\mathbb{F}_7)|$.

b) Définir un morphisme injectif de groupe $G \hookrightarrow S_7$.

Exercice 14 : Sous-groupes finis de $\mathrm{SO}(3)$**.** Soit G un sous-groupe fini de $\mathrm{SO}(3)$. On considère l'action naturelle de $\mathrm{SO}(3)$ sur la sphère S^2.

a) Montrer que tout élément non trivial g de $\mathrm{SO}(3)$ a exactement deux points fixes sur S^2.

b) On note $X \subset S^2$ l'ensemble (fini) des axes des éléments de G, c'est à dire l'ensemble des points de S^2 qui ont un stabilisateur non trivial dans G. Montrer que G agit sur X.

c) On note $Y = \{(x,g) | \, x \in X,\, g \in G \backslash \{1\},\, gx = x\}$. Calculer le cardinal de Y de deux manières pour montrer l'égalité

$$2.|G| - 2 = \sum_{x \in X}(|G_x| - 1) = \sum_{[y] \in X/G} |G| - |yG|.$$

où G_x désigne le stabilisateur de x dans G et $[y] = yG$ est l'orbite de y sous G.

d) Si $n = |G|$, montrer que

$$2 - \frac{2}{n} = \sum_{y \in X/G} 1 - \frac{1}{|G_y|}.$$

e) En déduire que la somme ci-dessus ne peut contenir que $k = 2$ ou 3 termes.

f) Si $k = 2$, montrer que tous les éléments de G ont même axe de rotation : G est un groupe cyclique.

g) Si $k = 3$, on note $a \leq b \leq c$ les ordres des stabilisateurs. Montrer que les seules possibilités pour ces ordres sont $(2, 2, n/2)$ (groupe dihédral), $(2, 3, 3)$ (tétraèdre), $(2, 3, 4)$ (cube), $(2, 3, 5)$ (dodécaèdre).

Exercice 15 : Quaternions et groupes de Chevalley linéaires. Soit K un corps commutatif de caractéristique différente de 2 et $a, b \in K^\times$. On définit les quaternions $\mathbb{H}_{a,b}$ comme la K-algèbre de base 1, i, j, $k = ij$, où les éléments i, j vérifient les relations

$$i^2 = a,\ j^2 = b,\ ij = -ji.$$

Les quaternions classiques d'hamilton se retrouvent en posant $a = b = -1$. Pour $h = x+yi+zj+tk$ un quaternion, on appelle $Nm(h) = x^2 - ay^2 - bz^2 + abt^2$ la norme de h. On remarque que les quaternions peuvent s'écrire comme des matrices à coordonnées dans une extension de K contenant une racine carrée de a et de b de la forme

$$\begin{pmatrix} x + \sqrt{a}y & \sqrt{b}(z + \sqrt{a}t) \\ \sqrt{b}(z - \sqrt{a}t) & x - \sqrt{a}y \end{pmatrix}$$

et que la norme correspond alors au déterminant.

a) Donner une description du groupe spécial orthogonal de la forme quadratique $Nm(0, y, z, t)$ sur K^3 en termes des quaternions.

b) Exprimer le sous-groupe $G^+(C_3) \subset \mathrm{SO}(3)$ en termes des quaternions.

c) En déduire que pour tout nombre premier $p \neq 2$, il existe un morphisme injectif de groupes $\beta : S_4 \to \mathrm{PGL}_2(\mathbb{F}_p)$ tel que $\beta(A_4) \subset \mathrm{PSL}_2(\mathbb{F}_p)$.

d) Montrer que $\beta(S_4) \subset \mathrm{PSL}_2(\mathbb{F}_p)$ si et seulement si 2 est un carré dans $\mathbb{F}_p$ (si et seulement si $p \equiv \pm 1 \mod 8$).

e) En déduire que l'action du groupe $G_5 = \mathrm{PGL}_2(\mathbb{F}_5)$ (resp. $G_7 = \mathrm{PSL}_2(\mathbb{F}_7)$) sur l'espace homogène $X_5 = G_5/\beta(S_4)$ (resp. sur $X_7 = G_7/\beta(S_4)$) donne lieu à un morphisme de groupes $G_p \to S_{X_p}$ $(p = 5, 7)$.

f) En admettant que l'action de G_5 sur X_5 est fidèle, montrer que $\mathrm{PSL}_2(\mathbb{F}_5) = A_5$.

Exercice 16 : Montrer qu'un groupe abélien non nul est simple si et seulement si il est cyclique d'ordre p, où p est un nombre premier.

Exercice 17 :

a) Décrire tous les groupes abéliens Y (à isomorphisme près) d'ordre $|Y| = 8$.

b) Décrire tous les groupes abéliens X (à isomorphisme près) d'ordre $|X| = 16$. Pour tout X décrire tous les Y (d'ordre $|Y| = 8$) qui sont isomorphes à un sous-groupe de X.

Exercice 18 : On rappelle que si X est un groupe abélien, sa partie de p-torsion $X[p]$ est définie par $X[p] = \{x \in X \,|\, px = 0\}$ et sa partie p-primaire est définie par $X(p) = \{x \in X \,|\, \exists n,\ p^n x = 0\}$. Soit X un groupe abélien d'ordre $|X| = 216$. Déterminer la structure de X en terme de ses parties 2- et 3-primaires. Déterminer la structure de X en terme des i et j tels que $|X[2]| = 2^i$ et $|X[3]| = 3^j$. Que se passe-t-il si l'on remplace 216 par 432 ?

Exercice 19 : Soit X un groupe abélien d'ordre $|X| = n$. Montrer que, pour tout diviseur d de n il existe un sous-groupe (resp., un quotient de X) d'ordre d.

Exercice 20 :

a) Décrire tous les groupes abéliens X (à isomorphisme près) qui admettent un sous-groupe Y isomorphe à $\mathbb{Z}/4\mathbb{Z}$ tel que X/Y soit isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

b) Idem pour $Y \cong \mathbb{Z}/6\mathbb{Z}$ et $X/Y \cong \mathbb{Z}/12\mathbb{Z}$.

Algèbre et théorie de Galois - TD2

Exercice 1 : Pour résoudre un polynôme cubique de la forme $x^3 + px + q$, Cardan propose de poser $x = u + v$ et de trouver un polynôme de degré 2 dont u^3 et v^3 sont des racines.

a) Trouver les racines de $x^3 + 3x - 2$ par la méthode de Cardan.

b) Trouver les racines de $x^3 - 7x - 7$ par la méthode de Cardan.

Exercice 2 : Simplifier les expression suivantes en utilisant la méthode de Cardan :

a) $\sqrt[3]{10 + \sqrt{108}} + \sqrt[3]{10 - \sqrt{108}}$.

b) $\sqrt[3]{10 - \sqrt{108}}$.

c) $\sqrt[3]{1 + \frac{2}{3}\sqrt{\frac{7}{3}}} + \sqrt[3]{1 - \frac{2}{3}\sqrt{\frac{7}{3}}}$.

d) $\sqrt[3]{1 + \frac{2}{3}\sqrt{\frac{7}{3}}}$.

e) $\sqrt[3]{5 + \sqrt{52}}$.

Exercice 3 : (Nombres de Liouville)

a) Soit $a \in \mathbb{R}$ un nombre algébrique sur $\mathbb{Q}$ non rationel et P un polynôme irréductible de degré n tel que $P(a) = 0$. Montrer qu'il existe $c \in \mathbb{R}$ tel que

$$\forall \frac{p}{q},\ |a - \frac{p}{q}| > \frac{c}{q^n}.$$

b) Un nombre $a \in \mathbb{R}$ est dit de Liouville si pour tout entier positif n, il existe des entiers p et q avec $q > 1$ tels que

$$|x - \frac{p}{q}| < \frac{1}{q^n}.$$

Montrer que tout nombre de Liouville est transcendant, i.e., pas racine d'un polynôme à coefficients rationnels.

c) Montrer que $\sum_{i=1}^{\infty} 10^{-n!}$ est un nombre de Liouville en utilisant les suites $p_n = \sum_{j=1}^{n} 10^{n!-j!}$, $q_n = 10^{n!}$.

Exercice 4 : Pour tout ensemble ordonné $I = (i_1 \geq i_2 \geq \cdots \geq i_n)$, on note $s_I = s_{i_1,\ldots,i_n} = \sum_{\sigma \in S_n} \sigma(x^{i_1} \ldots x^{i_n})$. On a en particulier $s_{1,\ldots,1} = \sigma_n$ le polynôme symétrique élémentaire.

a) Tout polynôme symétrique $f \in A[x_1, \ldots, x_n]^{S_n}$ est une combinaison linéaire finie $f = \sum c_I s_I$ avec $c_I \in A$.

b) Pour tous I, J, on a

$$s_I s_J = s_{I+J} + \sum_{K<I+J} c_K s_K.$$

Exercice 5 :

a) Exprimer les polynômes $s_{2,2}$, $s_{3,1}$ en les variables x, y, z en termes des polynômes symétriques élémentaires.

b) Calculer $\sum x_i^4$ où x_i sont les racines du polynôme $P(x) = (x-1)(x-2)(x-3)(x-4)$.

c) Calculer $\sum x_i^7$ où x_i sont les racines de $P(x) = x^3 + px + q$.

Exercice 6 : (Critères d'irréductibilité)

a) Soit $a \in \mathbb{Z}$, non divisible par 3. Montrer que le polynôme $P(x) = x^3 - x + a$ est irréductible dans $\mathbb{Q}[X]$.

b) Le polynôme $P(x) = x^7 + 600x^6 + 284x^2 + 52x + 14$ est-il irréductible sur $\mathbb{Q}$?

c) Etudier l'irréductibilité des polynômes $P(x) = x^3 + \frac{1}{2}x^2 - \frac{5}{2}x + 1$ et $Q(x) = 30x^3 + 277x^2 - 31x - 28$ dans $\mathbb{Q}[x]$.

d) Etudier l'irréductibilité du polynôme $P(x) = x^4 - 15x^3 + 7$ dans $\mathbb{Q}[x]$.

Exercice 7 : Soit $P \in \mathbb{Q}[X]$ un polynôme. Décrire la structure de l'anneau quotient $A = \mathbb{Q}[X]/(P)$.

Exercice 8 :

a) Montrer que $\mathrm{disc}(x^n + ax + b) = ca^n + db^{n-1}$, où les constantes c, d ne dépendent que de $n \geq 2$.

b) Pour determiner d, calculer $\mathrm{disc}(x^n - e)$.

c) Trouver une relation entre $\mathrm{disc}(xf(x))$ et $\mathrm{disc}(f(x))$.

d) Calculer $\mathrm{disc}(x^n - ex)$.

e) Calculer $\mathrm{disc}(x^n + ax + b)$.

Exercice 9 : Factoriser le polynôme $P(x) = x^4 - x^2 - x - 1$ sur $\mathbb{F}_3$.

Exercice 10 : (Polynôme irréductible sur $\mathbb{Z}$ et réductible modulo p pour tout p)

a) Soit K un corps et $P \in K[X]$. Montrer que P est irréductible sur K si et seulement si il n'a pas de racines dans les extensions L de K telles que $[L : K] \leq n/2$.

b) Soit $P(x) = x^4 + 1 \in \mathbb{Z}[x]$.

i) Montrer que P est irréductible sur $\mathbb{Z}$.

ii) Montrer que P est réductible modulo 2, puis que pour p premier impair, P admet une racine dans $\mathbb{F}_{p^2}$. En déduire que P est irréductible sur tous les $\mathbb{F}_p$.

c) Soit $a \in \mathbb{Z}$, $|a| > 1$ et a sans facteur carré. On pose $P_a(x) = x^4 + 2(1-a)x^2 + (1+a)^2$.

i) Etudier l'irréductibilité de P_a sur $\mathbb{Z}$.

ii) Montrer que P_a est réductible modulo 2, et réductible modulo p pour tout diviseur premier impair p de a.

iii) Soit p premier impair ne divisant pas a. En distinguant les cas $\left(\frac{a}{p}\right) = 1$ et $\left(\frac{a}{p}\right) = -1$, factoriser P_a dans $\mathbb{F}_p[X]$.

Algèbre et théorie de Galois - TD3

Exercice 1 : Soit K un sous-corps de $\mathbb{C}$ et $a, b \in K^*$. Démontrer les énoncés suivants :

a) $K(\sqrt{a})^{*2} \cap K^* = K^{*2} \cup aK^{*2}$.

b) $K(\sqrt{a}) = K(\sqrt{b}) \iff a/b \in K^{*2}$.

c) $K(\sqrt{a}, \sqrt{b})^{*2} \cap K^* = K^{*2} \cup aK^{*2} \cup bK^{*2} \cup abK^{*2}$.

d) $[K(\sqrt{a}, \sqrt{b}) : K] = 4 \iff a, b, ab \notin K^{*2}$. Si c'est le cas, alors $1, \sqrt{a}, \sqrt{b}, \sqrt{ab}$ est une base de $K(\sqrt{a}, \sqrt{b})/K$.

e) Si L/K est une extension de corps de degré 2 ($L \subset \mathbb{C}$), alors il existe $c \in K^*$, $c \notin K^{*2}$ tel que $L = K(\sqrt{c})$.

f) Les corps $L = K, K(\sqrt{a}), K(\sqrt{b}), K(\sqrt{ab}), K(\sqrt{a}, \sqrt{b})$ sont les seuls corps intermédiaires $K \subseteq L \subseteq K(\sqrt{a}, \sqrt{b})$.

Exercice 2 : Soient a, b, c des nombres rationnels. Soient $L/K = \mathbb{Q}(\sqrt[3]{3})/\mathbb{Q}$ et $\beta = a + b\sqrt[3]{3} + c\sqrt[3]{9} \in L$. Déterminer le polynôme caractéristique $P_{\beta, L/K}(X)$ et le polynôme minimal de β sur $\mathbb{Q}$.

Exercice 3 : Montrer que l'anneau $F = \mathbb{F}_3[X]/(X^4 + X^2 + X + 1)$ est un corps. Déterminer le degré $[F : \mathbb{F}_3]$ et le nombre d'éléments de F. Soit $y = x^3 - 1 \in F$, où l'on a noté x l'image de X dans F. Déterminer $y^{-1} \in F$, le polynôme minimal de y sur $\mathbb{F}_3$ et l'ordre de x et y dans F^*.

Exercice 4 : Calculer l'inverse β^{-1} du nombre

$$\beta = 3 - 2\sqrt[3]{2} + \sqrt[3]{4} = g(\sqrt[3]{2}), \qquad g(X) = X^2 - 2X + 3$$

dans la $\mathbb{Q}$-algèbre $\mathbb{Q}[X]/(X^3 - 2)$.

Exercice 5 : Calculer le degré des extensions suivantes :

a) $\mathbb{Q}(\sqrt[3]{2}, \sqrt{2})$ sur $\mathbb{Q}(\sqrt[3]{2})$, sur $\mathbb{Q}(\sqrt{2})$ et sur $\mathbb{Q}$.

b) $\mathbb{Q}(\sqrt[3]{2}, a)/\mathbb{Q}$ avec $P(a) := a^4 + 6a + 2 = 0$.

c) $\mathbb{Q}(\sqrt{2}, \sqrt{18}, \sqrt{-7})/\mathbb{Q}$.

d) $\mathbb{Q}(5 + \sqrt{27}, \sqrt{8})/\mathbb{Q}$.

Exercice 6 : Décrire les inclusions entres les corps suivants :

a) $\mathbb{Q}(\sqrt{3}, \sqrt{2})$, $\mathbb{Q}(\sqrt{3} + \sqrt{2})$, $\mathbb{Q}(\sqrt{5 + \sqrt{24}})$, $\mathbb{Q}(\sqrt{5 - \sqrt{24}})$.

b) $\mathbb{Q}(j)$, $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(j, \sqrt[3]{2})$.

c) $\mathbb{Q}(\sqrt{3}, j)$, $\mathbb{Q}(\sqrt{3}, i, j)$, $\mathbb{Q}(\sqrt{3}, i)$, $\mathbb{Q}(i, j)$.

d) $\mathbb{Q}(\cos(\frac{2\pi}{3}))$, $\mathbb{Q}(\sin(\frac{2\pi}{3}))$, $\mathbb{Q}(\cos(\frac{2\pi}{5}))$, $\mathbb{Q}(\sin(\frac{2\pi}{3}))$.

Exercice 7 : Soit $P(x) = x^p - t \in \mathbb{F}_p(t)[x]$.

a) Montrer que $\mathbb{F}_p(\sqrt[p]{t}) := \mathbb{F}_p(t)[x]/(P)$ est un corps.

b) L'extension $\mathbb{F}_p(\sqrt[p]{t})/\mathbb{F}_p(t)$ est elle séparable ? normale ?

Algèbre et théorie de Galois - TD4

Exercice 1 : Calculer le corps de décomposition L du polynôme $f = x^3 - 2$ sur $\mathbb{Q}$. Pour les extensions intermédiaire de $L/\mathbb{Q}$ qu'on aura construites, donner leur degré, dire si elles sont galoisiennes et si c'est le cas, calculer leur groupe de Galois.

Exercice 2 : Calculer les automorphismes sur $\mathbb{Q}$ des extensions suivantes :

a) $\mathbb{Q}(\sqrt{-52})$, $\mathbb{Q}(7+3i)$.

b) Un corps de décomposition de $P = X^4 - 7$.

Exercice 3 :

a) Calculer la clôture normale L de l'extension $\mathbb{Q}(\sqrt[4]{2})$.

b) Décrire la structure du groupe de Galois de $L/\mathbb{Q}$.

c) Calculer explicitement l'action de $\mathrm{Gal}(L/\mathbb{Q})$ sur les générateurs de l'extension $L/\mathbb{Q}$.

d) Décrire explicitement tous les sous-groupes de $\mathrm{Gal}(L/\mathbb{Q})$ et dire ceux qui sont normaux.

e) Ecrire explicitement la correspondance de Galois pour $L/\mathbb{Q}$.

Exercice 4 : Calculer l'extension normale L' de l'extension L de $\mathbb{Q}$ engendrée par

a) $\sqrt{3}+\sqrt{2}$,

b) $\sqrt{3}+i$,

c) $\sqrt[3]{2}+\sqrt{2}$,

d) $\sqrt[3]{2}+i$,

e) $\sin(\frac{2\pi}{5})$,

f) $e^{\frac{2i\pi}{n}}$, $n > 1$,

g) $e^{\frac{2ik\pi}{n}}$,

h) $\sqrt{1+\sqrt{2}}$,

i) une racine de $x^6 + 3$.

On donnera aussi son groupe de Galois, et le cas échéant, les sous-groupes de ce dernier et les extensions intermédiaires de $L/\mathbb{Q}$.

Exercice 5 : Calculer le polynôme cyclotomique $\Phi_{28}(X)$.

Exercice 6 : Calculer le groupe de Galois (d'un corps de décomposition) des polynômes suivants :

a) $x^2 - 2$,

b) $(x^2-2)(x^2-3)$,

c) $x^3 - 1$,

d) $x^4 - 6$,

e) $(x^2-2x-1)(x^2-2x-7)(x^2-2x+2)$,

f) $x^3 - 2$ et $x^3 + 2$,

g) $x^4 - 1$ et $x^4 + 1$,

h) $x^4 + 2$.

Exercice 7 : (Groupe de Galois non résoluble) Montrer que le groupe de Galois de

$$f(x) = x^5 - 10x + 5$$

est isomorphe à S_5.

Exercice 8 : (Extensions d'anneaux et revêtements de schémas)

a) Soit $f : A \to B$ un morphisme d'anneaux (commutatifs unitaires dans cet exercice). Montrer que pour tout anneau C, f induit une application naturelle $\mathrm{Hom}(f, C) : \mathrm{Hom}(B, C) \to \mathrm{Hom}(A, C)$. La correspondance

$$\underline{A} : C \mapsto \underline{A}(C) := \mathrm{Hom}(A, C)$$

qui a un anneau C associe l'ensemble des morphismes d'anneaux de A dans C est appelé le *schéma* de A. L'ensemble $\underline{A}(C) := \mathrm{Hom}(A, C)$ est appelé ensemble des points de A à valeurs dans C.

b) Soient $A_2 = \mathbb{Q}[x, y]$, $C = \mathbb{Q}[x][y]/(y^2 - x)$ et $D = \mathbb{Q}[x]$. Décrire les ensembles de points des schémas $\underline{A}_2$, $\underline{C}$ et $\underline{D}$ à valeurs dans $\mathbb{R}$ et les dessiner. Expliquer les notations $\underline{A}_2$, $\underline{C}$ et $\underline{D}$ pour ces schémas.

c) On note $f : A_2 \to B$ et $g : A_2 \to C$ les applications de projection ($g(y) = 0$) et $p : D \to C$ l'inclusion naturelle. Décrire les applications correspondantes entre les points réels $\underline{C}(\mathbb{R})$, $\underline{D}(\mathbb{R})$ et $\underline{A}_2(\mathbb{R})$ et les dessiner.

d) Pour quels polynômes irréductible P de $D = \mathbb{Q}[x]$ l'application $p : D/(P) \to C/(P)$ est-elle une extension de corps. Quel est alors son degré ? Est-elle normale ? Que dire si ce n'est pas une extension de corps ?

e) Montrer que l'application $\mathbb{C} \to \underline{C}(\mathbb{C}) \subset \underline{A}_2(\mathbb{C})$ donnée par $z \mapsto (z^2, z)$ est bijective et que $p : \underline{C}(\mathbb{C}) \to \underline{D}(\mathbb{C})$ s'identifie à l'application $\mathbb{C} \to \mathbb{C}$ donnée par $z \mapsto z^2$. Représenter géométriquement cette application.

f) Calculer le groupe des automorphismes du morphisme d'anneaux $p : D \to C$. On nommera ce groupe le *groupe de Galois* du revêtement $p : \underline{C} \to \underline{D}$.

Algèbre et théorie de Galois - TD5

Définition 1. Une catégorie C est la donnée

a) d'une classe $\mathcal{O}b(C)$ appelés les objets de C,

b) pour chaque couple d'objets X, Y d'un ensemble $\mathrm{Hom}(X, Y)$ appelé ensemble des morphismes,

c) pour chaque objet X d'un morphisme $\mathrm{id}_X \in \mathrm{Hom}(X, X)$ appelé identité,

d) pour chaque triplet d'objets X, Y, Z, d'une loi de composition des morphismes

$$\circ : \mathrm{Hom}(X, Y) \times \mathrm{Hom}(Y, Z) \to \mathrm{Hom}(X, Z).$$

On suppose de plus que la composition est associative, i.e., $f \circ (g \circ h) = (f \circ g) \circ h$ et que l'identité est une unité, i.e., $f \circ \mathrm{id} = f$ et $\mathrm{id} \circ f = f$.

Définition 2. Une propriété universelle [1] pour un objet Y de C est une description explicite (et compatible aux morphismes[2]) de $\mathrm{Hom}(X, Y)$ (ou $\mathrm{Hom}(Y, X)$) pour tout objet X de C.

Exemple 1. Voici quelques exemples que vous connaissez déjà bien.

a) (Ens) dont les objets sont les ensembles et les morphismes les applications.

b) (Grp) dont les objets sont les groupes et les morphismes les morphismes de groupes.

c) (Grab) dont les objets sont les groupes abéliens et les morphismes les morphismes de groupes.

d) (Anneaux) dont les objets sont les anneaux unitaires munis des morphismes d'anneaux.

e) (Top) dont les objets sont les espaces topologiques et les morphismes les applications continues.

Principe 1. *(Grothendieck)*

Ce qui compte, ce ne sont pas les objets mathématiques,
mais les relations qu'ils entretiennent
(i.e., les morphismes).

Exercice 1 : (Propriétés universelles) Quelle est la propriété universelle de

a) l'ensemble vide ?

b) l'ensemble à un point ?

c) $\mathbb{Z}$ comme groupe ?

d) $\mathbb{Z}$ comme anneau commutatif unitaire ?

e) $\mathbb{Q}$ comme anneau commutatif unitaire ?

f) l'anneau commutatif unitaire nul ?

Solution de l'exercice 1.

a) On a $\mathrm{Hom}_{(\mathrm{Ens})}(\emptyset, X) = \{\emptyset \subset X\}$ est réduit à un morphisme donné par l'inclusion canonique. C'est la propriété universelle à gauche de l'ensemble vide. On dit que c'est l'ensemble initial. On peut aussi écrire $\mathrm{Hom}_{(\mathrm{Ens})}(X, \emptyset) = \emptyset$ si X est non vide et $\mathrm{Hom}_{(\mathrm{Ens})}(\emptyset, \emptyset) = \{\emptyset \subset \emptyset\}$ est réduit à l'inclusion canonique. C'est l'autre propriété universelle de l'ensemble vide, mais comme elle est plus compliquée, elle est moins intéressante.

[1] Tout objet a exactement deux propriétés universelles, mais on n'écrira souvent uniquement la plus simple.

[2] Pour plus de précisions sur ces compatibilités, voir la page web [Wikipedia : lemme de Yoneda].

b) On a $\mathrm{Hom}_{(\mathrm{Ens})}(X, \{.\}) = \{.\}$ est réduit à un morphisme donné par la projection canonique $X \to \{.\}$. On dit que le point est l'ensemble final.

c) On a $\mathrm{Hom}_{(\mathrm{Grp})}(\mathbb{Z}, G) \cong \mathrm{Hom}_{(\mathrm{Ens})}(\{.\}, G) \cong G$, la bijection étant obtenue en envoyant un morphisme $f : \mathbb{Z} \to G$ sur l'élément $f(1)$, qui détermine complètement G. On dit que $\mathbb{Z}$ est le groupe libre sur l'ensemble $\{.\}$ à un élément.

d) On a $\mathrm{Hom}_{(\mathrm{Anneaux})}(\mathbb{Z}, A) = \{i_A : \mathbb{Z} \to A\} \cong \mathrm{Hom}_{(\mathrm{Ens})}(\emptyset, A)$ pour A commutatif et $i_A : \mathbb{Z} \to A$ l'application canonique donnée par $i(n) = n.1_A$. On dit que $\mathbb{Z}$ est l'anneau commutatif unitaire initial.

e) L'anneau $\mathbb{Q}$ est le corps de fractions de $\mathbb{Z}$. On a donc $\mathrm{Hom}_{(\mathrm{Anneaux})}(\mathbb{Q}, A) = \{f : \mathbb{Z} \to A | f(n) \in A^\times \forall n \in \mathbb{Z} - \{0\}\}$ est égal à $\emptyset$ si il existe un entier non nul non inversible dans A et à $\mathrm{Hom}_{(\mathrm{Anneaux})}(\mathbb{Z}, A) = \{i_A\}$ sinon.

f) On a $\mathrm{Hom}_{(\mathrm{Anneaux})}(A, 0) = \{0_A : A \to 0\}$ est réduit à un morphisme donné par $0_A(a) = 0$. En effet, on a nécessairement $1 = 0$ dans l'anneau nul et $0_A(a) = 0_A(a.1) = 0_A(a).0 = 0$ pour tout $a \in A$. On dit que l'anneau nul est l'anneau commutatif unitaire final.

Exercice 2 : (Objets libres) Soit C une catégorie dont les objets sont décrits par des ensembles munis de structures supplémentaires (par exemple, (Ens), (Grp), (Grab), (Anneaux) ou (Top)). Soit X un ensemble. Un objet libre de C sur X est un objet $L(X)$ de C tel que pour tout objet Z, on ait une bijection naturelle

$$\mathrm{Hom}(L(X), Z) \cong \mathrm{Hom}_{\mathrm{Ens}}(X, Z).$$

Soit X un ensemble donné. Décrire explicitement

a) le groupe libre sur X,

b) le groupe abélien libre sur X,

c) le $\mathbb{R}$-module libre sur X,

d) l'anneau commutatif unitaire libre sur X,

e) la $\mathbb{C}$-algèbre commutative unitaire libre sur X,

f) la $\mathbb{C}$-algèbre associative unitaire libre sur X.

Solution de l'exercice 2.

a) Le groupe libre sur X est donné par les mots dont les lettres sont dans l'ensemble $X \coprod X^{-1}$ formés d'éléments de X et d'éléments notés x^{-1} pour $x \in X$, et muni de la loi donnée par la concaténation des mots. On vérifie que $\mathrm{Hom}_{(\mathrm{Grp})}(L(X), G) = \mathrm{Hom}_{(\mathrm{Ens})}(X, G)$, c'est à dire que pour définir un morphisme du groupe libre sur X dans le groupe G, il suffit de définir l'image des générateurs. En effet, si $f : X \to G$ est une application, on peut donner l'image d'un mot en les lettre dans $X \coprod X^{-1}$ en prenant le mot en les images $f(x)$ et $(f(x))^{-1}$ des éléments de X et de leur inverse.

b) Le groupe abélien $L(X) = \mathbb{Z}^{(X)}$ libre sur X est donné par les applications $a : X \to \mathbb{Z}$ à support fini (nulles en dehors d'un ensemble fini). On peut aussi les voir comme des sommes $\sum_{x \in X} a_x\{x\}$ avec $a_x \in \mathbb{Z}$ presque tous nuls. On voit aussi que pour définir un morphisme $L(X) \to M$ vers un groupe abélien M, il suffit de définir l'image de ses éléments, d'où la bijection $\mathrm{Hom}_{(\mathrm{Grab})}(L(X), M) \cong \mathrm{Hom}_{(\mathrm{Ens})}(X, M)$ pour tout groupe abélien M.

c) Même chose qu'avant : $L(X) = \mathbb{R}^{(X)}$ est donné par les applications $f : X \to \mathbb{R}$ à support fini. C'est le $\mathbb{R}$-espace vectoriel de base X.

d) L'anneau commutatif unitaire libre sur X est l'anneau $\mathbb{Z}[X]$ des polynômes ayant leurs variables dans l'ensemble X. On peut commencer par définir le monoide libre $\mathbb{N}^{(X)}$ sur X qui est donné par les monômes sur X, i.e., les mots en des éléments de X avec la condition de commutation de toutes les lettres, i.e., par des produits finis $x_1^{n_1} \dots x_n^{m_n}$. On définit ensuite l'anneau commutatif unitaire libre sur X comme le $\mathbb{Z}$-module libre sur $\mathbb{N}^{(X)}$, i.e. l'ensemble des applications $a : \mathbb{N}^{(X)} \to \mathbb{Z}$ à

support fini (qui représentent les coefficients du polynôme $P(X) = \sum_{i \in \mathbb{N}^{(X)}} a_i x^i$), muni de son addition canonique et de la multiplication polynômiale. Si X est un ensemble fini, on retrouve les polynômes en un nombre fini de variables. On vérifie en combinant la propriété universelle du monoide libre et celle du module libre que c'est bien l'anneau commutatif unitaire libre sur X, i.e. , qu'on a une bijection

$$\mathrm{Hom}_{(\textsc{Anneaux})}(\mathbb{Z}[X] \to A) \cong \mathrm{Hom}_{(\textsc{Ens})}(X, A)$$

pour tout anneau commutatif unitaire A. On remarque au passage que l'algèbre symétrique sur le $\mathbb{Z}$-module libre $\mathbb{Z}^{(X)}$ sur X vérifie aussi cette propriété universelle, ce qui montre que l'algèbre symétrique du $\mathbb{Z}$-module libre $\mathbb{Z}^{(X)}$ est aussi l'algèbre commutative unitaire libre sur l

e) Comme avant, on définit la $\mathbb{C}$-algèbre commutative unitaire libre sur X comme le $\mathbb{C}$-module libre sur les monômes $\mathbb{N}^{(X)}$. Ce sont simplement les polynômes à variables dans l'ensemble X et à coefficients complexes.

f) Par définition de l'algèbre tensorielle, on sait que si $M(X) = \mathbb{C}^{(X)}$ est le $\mathbb{C}$-module libre sur X et que A est une $\mathbb{C}$-algèbre associative unitaire, on a un isomorphisme naturel

$$\mathrm{Hom}_{\mathbb{C}-Alg}(T_{\mathbb{C}}(M(X)), A) \cong \mathrm{Hom}_{\mathbb{C}-mod}(M(X), A)$$

et par la propriété universelle du module libre, on a

$$\mathrm{Hom}_{\mathbb{C}-mod}(M(X), A) \cong \mathrm{Hom}_{(\textsc{Ens})}(X, A)$$

donc l'algèbre tensorielle sur le $\mathbb{C}$-module libre sur X est la $\mathbb{C}$-algèbre associative libre sur l'ensemble X.

Exercice 3 : (Produits et sommes) Le produit (resp. la somme) de deux objets X et Y est est un objet $X \times Y$ (resp. $X \coprod Y$, parfois noté $X \oplus Y$) tel que pour tout objet Z, soit donné une bijection naturelle en Z (compatible aux morphismes $f : Z_1 \to Z_2$)

$$\mathrm{Hom}(Z, X \times Y) \cong \mathrm{Hom}(Z, X) \times \mathrm{Hom}(Z, Y)$$
$$(\text{resp. } \mathrm{Hom}(X \coprod Y, Z) \cong \mathrm{Hom}(X, Z) \times \mathrm{Hom}(Y, Z)).$$

Décrire explicitement

a) les sommes et produits de deux ensembles,

b) les sommes et produits de deux groupes abéliens, puis celles de deux groupes,

c) les sommes et produits de deux anneaux commutatifs unitaires.

Solution de l'exercice 3.

a) On va donner juste la somme, le produit étant déjà bien connu. On définit $X \coprod Y$ comme l'union disjointe de X et Y, c'est à dire un ensemble composé exclusivement des éléments de X et de ceux de Y. On a deux inclusions naturelles $i_X : X \to X \coprod Y$ et $i_Y : Y \to X \coprod Y$ et si $f \in \mathrm{Hom}_{(\textsc{Ens})}(X \coprod Y, Z)$ est une application définie sur l'union disjointe, le couple $(f \circ i_X, f \circ i_Y)$ détermine f de manière unique. Ceci donne une application injective

$$\mathrm{Hom}(X \coprod Y, Z) \to \mathrm{Hom}(X, Z) \times \mathrm{Hom}(Y, Z).$$

Si (h, k) sont dans le terme de droite, on peut définir une application $f : X \coprod Y \to Z$ par $f(x) = h(x)$ si $x \in X$ et $f(y) = k(y)$ si $y \in Y$. Ceci montre la surjectivite de l'application entre ensembles de morphismes, et donc sa bijectivité. On a ainsi montré que l'union disjointe de deux ensembles vérifie la propriété universelle de la somme de deux ensembles.

b) Pour X et Y deux groupes abéliens, leur somme est définie comme un quotient du groupe abélien libre $\mathbb{Z}^{(X \coprod Y)}$ sur la somme des ensembles sous-jacents. On définit ce quotient en imposant que les applications canoniques $i_X : X \to \mathbb{Z}^{(X \coprod Y)}$ et $i_Y : Y \to \mathbb{Z}^{(X \coprod Y)}$ soient des morphismes de groupes, i.e., $\{x\} + \{x'\} = \{x + x'\}$ pour (x, x') dans X^2 ou Y^2 et $0_X = 0_Y = 0$. La combinaison de la propriété universelle de la somme de deux ensembles, de celle du groupe abélien libre et de celle du quotient nous montre qu'on a une bijection

$$\mathrm{Hom}_{(\mathrm{GRAB})}(X \coprod\!\!\!\!\coprod Y, Z) \cong \mathrm{Hom}_{(\mathrm{GRAB})}(X, Z) \times \mathrm{Hom}_{(\mathrm{GRAB})}(Y, Z).$$

Le groupe abélien $X \coprod Y$ obtenu est aussi noté $X \oplus Y$ et appelé la somme directe des deux groupes abéliens. Pour les groupes, on procède de manière similaire, mais il faut utiliser le groupe libre (non abélien, i.e., les mots, sur l'union disjointe $X \coprod Y$ des ensembles sous-jacents aux groupes considérés). Le groupe obtenu $X \coprod Y$ est appelé le produit libre des deux groupes X et Y et souvent noté $X * Y$. On note que ce n'est pas un produit mais une somme du point de vue des propriétés universelles, mais les traditions linguistiques ont la peau dure.

Exercice 4 : (Produits fibrés et sommes amalgamées) Le produit fibré (resp. la somme amalgamée) de deux morphismes $f : X \to S$ et $g : Y \to S$ (resp. $f : S \to X$ et $f : S \to Y$) est est un objet $X \times_S Y$ (resp. $X \coprod_S Y$, parfois noté $X \oplus_S Y$) tel que pour tout objet Z, soit donné une bijection naturelle en Z (compatible aux morphismes $f : Z_1 \to Z_2$)

$$\begin{array}{rcl} \mathrm{Hom}(Z, X \times_S Y) & \cong & \{(h,k) \in \mathrm{Hom}(Z,X) \times \mathrm{Hom}(Z,Y) | f \circ h = g \circ k\} \\ (\text{resp. } \mathrm{Hom}(X \coprod_S Y, Z) & \cong & \{(h,k) \in \mathrm{Hom}(X,Z) \times \mathrm{Hom}(Y,Z) | h \circ f = k \circ g\}). \end{array}$$

a) Répondre succintement aux mêmes questions que l'exercice précédent pour les produits et sommes amalgamées.

b) Soit $a < b < c < d$ trois nombres réels. Décrire explicitement les ensembles

$$]a, c[\times_{]a,d[}]b, d[\qquad \text{et} \qquad]a, c[\coprod\!\!\!\!\coprod_{]b,c[}]b, d[.$$

c) Décrire explicitement le groupe abélien

$$\mathbb{Z} \times_{\mathbb{Z}} \mathbb{Z}$$

où $f, g : \mathbb{Z} \to \mathbb{Z}$ sont données par $f : n \mapsto 2n$ et $g : n \mapsto 3n$.

Solution de l'exercice 4.

a) Laissé au lecteur. C'est similaire aux produits et sommes.

b) Le produit fibré donne l'intersection et la somme amalgamée donne la réunion (recollement) des deux intervalles considérés.

c) C'est $6\mathbb{Z}$, muni des deux projections $6\mathbb{Z} \xrightarrow{.3} \mathbb{Z}$ et $6\mathbb{Z} \xrightarrow{.3} \mathbb{Z}$. En effet, si $h : M \to \mathbb{Z} \times_{\mathbb{Z}} \mathbb{Z}$ est un morphisme de groupes abéliens tel que $h \circ f = g \circ f$ alors $f(x) = (n_x, m_x)$ avec $3 | n_x$ et $2 | m_x$ et $n_x = m_x \in 6\mathbb{Z}$. Ceci montre que

$$\mathrm{Hom}_{(\mathrm{GRAB})}(M, Z \times_{\mathbb{Z}} \mathbb{Z}) \cong \mathrm{Hom}_{(\mathrm{GRAB})}(M, 6\mathbb{Z})$$

donc $6\mathbb{Z} \cong \mathbb{Z} \times_{\mathbb{Z}} \mathbb{Z}$.

Exercice 5 : (Limites projectives) Soit $(I, \leq)$ un ensemble partiellement ordonné. Un système projectif d'objets indexé par I est une famille

$$A_\bullet = ((A_i)_{i \in I}, (f_{i,j})_{i \leq j})$$

d'objets et pour chaque $i \leq j$ de morphismes $f_{i,j} : A_j \to A_i$ tels que $f_{i,i} = \mathrm{id}_{A_i}$ et $f_{i,k} = f_{i,j} \circ f_{j,k}$ (une telle donnée est aussi appelée un foncteur de $A_\bullet : I \to C$ dans la catégorie considérée C). Une limite projective pour $A_\bullet$ est un objet $\varprojlim_I A_\bullet$ tel que pour tout objet Z, on ait une bijection naturelle

$$\mathrm{Hom}(Z, \varprojlim_I A_\bullet) \cong \varprojlim_I \mathrm{Hom}(A_i, Z)$$

où $\varprojlim_I \mathrm{Hom}(A_i, Z) \subset \prod_i \mathrm{Hom}(A_i, Z)$ désigne les familles de morphismes h_i telles que $f_{i,j} \circ h_j = h_i$. On définit les limites inductives $\varinjlim A_\bullet$ de manières similaires en inversant les but et sources des morphismes.

a) Montrer que les produits et produits fibrés sont des cas particuliers de cette définition.

b) Décrire l'anneau $\varprojlim_n \mathbb{C}[X]/(X^n)$.

c) Décrire l'anneau $\mathbb{Z}_p := \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$.

Solution de l'exercice 5.

a) Soient $f : X \to S$ et $g : Y \to S$ deux morphismes dont on veut prendre le produit fibré. Soit I l'ensemble à trois éléments $\{X, Y, S\}$ avec pour seule inégalités non triviales $X \leq S$ et $Y \leq S$. Le couple donné par $X \to S$ et $Y \to S$ est donc un système projectif indexé par l'ensemble partiellement ordonné I. La condition imposée à la limite projective L est que si Z est un objet, la donnée d'un morphisme $Z \to L$ est équivalente à celle d'une famille de trois morphismes $(i : Z \to X, j : Z \to Y, k : Z \to S)$ qui vérifient les conditions $f \circ i = g \circ j = k$, ce qui est exactement la propriété universelle du produit fibré (car k est déterminé par i ou j).

b) C'est l'anneau des séries formelles $\mathbb{C}[[X]]$. On a pour tout n une application de réduction modulo X^n $\mathbb{C}[[X]] \to \mathbb{C}[X]/(X^n)$ et une série formelle S est représentée dans le produit $\prod_n \mathbb{C}[X]/(X^n)$ par la famille $(S \mod X^n)_n$ de toutes ses réductions. On voit qu'une telle série vérifie bien les conditions de compatibilité avec les morphismes du système projectifs puisque ces morphismes sont des réductions et que les réductions sont toutes celles d'une série donnée. On montre que ceci donne tous les éléments de la limite projective par utilisation de la division euclidienne. On remarque que le polynôme $1 - X$ n'est pas inversible dans $\mathbb{C}[X]$ mais il le devient dans $\mathbb{C}[[X]]$ car la série $\sum_{i \geq 0} X^i$ est un élément de la limite projective qui donne un inverse pour $1 - X$.

c) On peut voir les éléments de la limite projective, notée $\mathbb{Z}_p$ comme des familles infinies d'entiers $(m_n)_n$ indexées par les entiers telles que $m_{n+1} \mod p^n = m_n$. Par division euclidienne successive, une telle famille de nombres peut être décrite par une série $s = \sum_{i \geq 0} a_i p^i$ avec $a_i \in \{0, \ldots, p-1\}$. On remarque que le nombre $\frac{1}{1-p}$ n'est pas un entier, i.e., pas dans $\mathbb{Z}$, mais c'est un entier p-adique, il est dans $\mathbb{Z}_p$, car on peut l'écrire $\sum_{i \geq 0} p^i$ et cette série converge clairement dans $\mathbb{Z}_p$ par définition de la limite projective.

Exercice 6 : Soit A un anneau commutatif unitaire, $S \subset A$ un ensemble multiplicatif (stable par multiplication et contenant 1_A). La localisation $A[S^{-1}]$ de A par rapport à S est défini par la propriété universelle

$$\mathrm{Hom}_{(\textsc{Anneaux})}(A[S^{-1}], B) = \{f \in \mathrm{Hom}_{(\textsc{Anneaux})}(A, B) | \forall s \in S,\, f(s) \in B^\times\},$$

où $B^\times$ est l'ensemble des éléments inversibles dans un anneau B.

a) Décrire $\mathbb{Z}[1/2] := \mathbb{Z}[\{2^{\mathbb{Z}}\}^{-1}]$.

b) Le morphisme $\mathbb{Z} \to \mathbb{Z}[1/2]$ est-il fini (i.e. $\mathbb{Z}[1/2]$ est t'il un $\mathbb{Z}$-module de type fini, i.e. engendré par un nombre fini d'éléments) ? De type fini (i.e. $\mathbb{Z}[1/2]$ peut-il être décrit comme un quotient d'un anneau de polynômes sur $\mathbb{Z}$ en un nombre fini de variables) ?

c) Construire un morphisme $\mathbb{Z}[1/2] \to \mathbb{Z}_3$ où $\mathbb{Z}_3$ sont les entiers 3-adiques définis dans l'exercice précédent.

d) Existe-t'il un morphisme $\mathbb{Z}[1/3] \to \mathbb{Z}_3$?

Solution de l'exercice 6.

a) Tout élément de $\mathbb{Z}[1/2]$ s'écrit sous la forme $n.2^m$ avec $n \in \mathbb{Z}$ non divisible par 2 et $m \in \mathbb{Z}$.

b) Le morphisme $\mathbb{Z} \to \mathbb{Z}[1/2]$ n'est pas fini. En effet, supposons qu'on dispose d'un système générateur fini F, i.e. d'un morphisme surjectif de $\mathbb{Z}$-modules $\mathbb{Z}^{(F)} \to \mathbb{Z}[1/2]$. Alors, il existe m_0 tel que tout $f \in F$ a pour dénominateur une puissance de 2 inférieure strictement à m_0. Ceci montre que l'application $\mathbb{Z}^{(F)} \to \mathbb{Z}$ n'est pas surjective car $\frac{1}{2^{m_0}}$ n'est pas dans son image. C'est une contradiction donc $\mathbb{Z}[1/2]$ n'est pas finie sur $\mathbb{Z}$. Par contre, on a un morphisme naturel $\mathbb{Z}[X] \to \mathbb{Z}[1/2]$ donné par $X \mapsto 1/2$ et ce morphisme est surjectif donc $\mathbb{Z} \to \mathbb{Z}[1/2]$ est de type fini.

c) On remarque que le nombre 3-adique donnée par les polynômes $S_n = -\sum_{i=0}^{n} 3^i$ (qui sont bien dans la limite projective $\mathbb{Z}_3$ de l'exercice précédent puisque $S_{n+1} = S_n \mod 3^{n+1}$) est un inverse du nombre $3-1=2$. En effet, on a $(1-3)S_n = 1-3^{n+1} = 1 \mod 3^{n+1}$. Par la propriété universelle de la localisation, on obtient un morphisme naturel $\mathbb{Z}[1/2] \to \mathbb{Z}_3$.

d) D'après la propriété universelle de la localisation, la donnée d'un morphisme $\mathbb{Z}[1/3] \to \mathbb{Z}_3$ est équivalente à celle d'un morphisme $\mathbb{Z} \to \mathbb{Z}_3$ tel que l'image de 3 soit inversible. Par la propriété universelle de $\mathbb{Z}$, il n'existe qu'un morphisme $\mathbb{Z} \to \mathbb{Z}_3$ donc il suffit de vérifier que l'image de 3 dans $\mathbb{Z}_3$ n'est pas inversible pour montrer qu'il n'existe pas de morphisme $\mathbb{Z}[1/3] \to \mathbb{Z}_3$. Comme le passage aux éléments inversibles est compatible aux morphismes d'anneaux, on devrait avoir un morphisme $\mathbb{Z}_3^\times \to (\mathbb{Z}/3\mathbb{Z})^\times$ or l'image de 3 dans $\mathbb{Z}/3\mathbb{Z}$ est nulle donc n'est pas inversible, ce qui donnerait une contradiction si 3 était inversible dans $\mathbb{Z}_3$, d'où la conclusion.

Exercice 7 : L'idéal $I = (X_1, \dots, X_n, \dots)$ engendré par toutes les variables de l'anneau de polynôme $A = \mathbb{Z}[\mathbb{N}] := \mathbb{Z}[(X_i)_{i\in\mathbb{N}}]$ est il de type fini ? L'anneau A est-il noetherien ? *Solution de l'exercice* 7. Si l'idéal considéré n'est pas de type fini, l'anneau A ne peut être noetherien. Supposons donné un système F fini de générateurs pour le A-module $I = (X_1, \dots, X_n, \dots)$. Rappelons qu'on a par définition explicite de l'anneau $\mathbb{Z}[(X_i)_{i\in\mathbb{N}}]$ un isomorphisme de $\mathbb{Z}$-modules

$$\mathbb{Z}^{\{(\mathbb{N}^{(X_i)_{i\in\mathbb{N}}})\}} \to \mathbb{Z}[(X_i)_{i\in\mathbb{N}}]$$

qui peut-être résumé en disant que tout polynôme $P \in A$ peut s'écrire sous la forme

$$P = \sum_{\underline{i}\in\mathbb{N}^{\{(X_i)_{i\in\mathbb{N}}\}}} a_{\underline{i}} \underline{X^i}$$

avec $\underline{X^i} := \prod_{n_i\in\underline{i}} X_i^{n_i}$. Maintenant, on se donne un système F fini de générateurs et on suppose que leur écriture ne fait intervenir que des variables parmi $X_0, \dots, X_M$. On peut alors supposer pour simplifier que $F = \mathbb{N}^{(\{X_0,\dots,X_M\})}$ est l'ensemble de tous les monômes en les variables considérées (c'est le monoïde libre sur l'ensemble des variables). Le système F est générateur si et seulement si l'application canonique $A^{(F)} \to I$ est un morphisme surjectif de A-modules. On devrait donc pouvoir écrire

$$X_{M+1} = \sum_{j=0}^{M} P_j X_i$$

avec $P_j \in A$. Si on décompose les P_j dans la $\mathbb{Z}$-base de $\mathbb{Z}[(X_i)_{i\in\mathbb{N}}]$ donnée par les monômes, on obtient

$$X_{M+1} = \sum_{j=0}^{M} \sum_{\underline{i}_j\in I_j\subset\mathbb{N}^{\{(X_i)_{i\in\mathbb{N}}\}}} a_{\underline{i}_j} \underline{X^{i_j}} X_j$$

avec $a_{\underline{i}_j} \in \mathbb{Z}$. On considère alors dans l'expression de droite les monômes qui contiennent la variable X_{M+1} et on les passe de l'autre coté de l'égalité pour obtenir

$$X_{M+1}(1 - \sum_{\underline{i}_j \in I_j, X_{M+1} | \underline{X}^{\underline{i}_j}} a_{\underline{i}_j} \frac{\underline{X}^{\underline{i}_j}}{X_{M+1}} X_j) = \sum_{\underline{i}_j \in I_j, X_{M+1} \nmid \underline{X}^{\underline{i}_j}} a_{\underline{i}_j} \underline{X}^{\underline{i}_j} X_j.$$

Si le polynôme de droite est non nul, X_{M+1} le divise, mais il n'apparaît par définition pas dans son écriture et on obtient une contradiction. Si le polynôme de droite est nul, celui de gauche aussi donc

$$\sum_{\underline{i}_j \in I_j, X_{M+1} | \underline{X}^{\underline{i}_j}} a_{\underline{i}_j} \frac{\underline{X}^{\underline{i}_j}}{X_{M+1}} X_j) = 1,$$

ce qui est impossible car les monômes sont des multiples de X_j donc de degré strictement supérieur à 0. On conclut que $X_{M+1} \notin I$ donc F n'est pas un système générateur et c'est une contradiction. Donc I n'admet pas de système générateur fini et A n'est pas noethérien.

Exercice 8 : (**Algèbre de Clifford)** Soit A un anneau commutatif unitaire, M un A-module et $q \in \text{Bilsym}(M, M; A)$ une forme A-bilinéaire symétrique sur $M \times M$ à valeurs dans A. L'algèbre de Clifford $\text{Cliff}(M, q)$ de (M, q) est la A-algèbre associative unitaire qui vérifie la propriété universelle

$$\text{Hom}_{A-alg}(\text{Cliff}(M, q), B) \cong \{j \in \text{Hom}_{A-Mod}(M, B) | j(v).j(w) + j(w).j(v) = q(v, w).1_B\}$$

pour toute A-algèbre associative B.

a) Définir l'algèbre de Clifford explicitement en utilisant l'algèbre associative libre (i.e. l'algèbre tensorielle).

b) Montrer que l'automorphisme $v \mapsto -v$ de (M, q) induit un automorphisme $\alpha : \text{Cliff}(M, q) \to \text{Cliff}(M, q)$ et une décomposition $\text{Cliff}(M, q) = \text{Cliff}^0(M, q) \oplus \text{Cliff}^1(M, q)$.

c) On note $\text{GSpin}(M, q)$ le groupe des inversibles de l'algèbre $Q(M, q)$ tels que $xv\alpha(x)^{-1} \in M$ pour tout $m \in M$. Définir un morphisme naturel

$$\text{GSpin}(M, q) \to O(M, q)$$

vers le groupe orthogonal de (M, q).

d) On suppose maintenant que $M = A^n$ est libre et q non dégénérée. On définit le groupe $\text{Spin}(M, q)$ comme le noyau du déterminant $\det : \text{GSpin}(M, q) \to O(M, q) \to A^\times = \text{GL}_1(\wedge^n M)$. On note $V = \text{Cliff}(M, q)$. Montrer que l'action naturelle de $\text{Spin}(M, q)$ sur V commute à l'automorphisme α de V. En déduire que la décomposition $V = V_0 \oplus V_1$ est munie d'une action du groupe $\text{Spin}(M, q)$. Une composante irréductible de cette représentation est appelée représentation de Spin demi-entier.

e) (difficile) Soit $(M, q) = (\mathbb{R}^{3,1}, q)$ l'espace de Minkowski sur $\mathbb{R}$ donné par la forme quadratique $q(t, x, y, z) = -c^2t^2 + x^2 + y^2 + z^2$ sur $M = \mathbb{R}^4$. On note $\text{Cliff}_{3,1}(\mathbb{R})$ l'algèbre de Clifford de M. Construire un isomorphisme entre le groupe spinoriel [3] correspondant $\text{Spin}_{3,1}(\mathbb{R})$ et le groupe réel $\text{SL}_2(\mathbb{C})$. Décrire l'action correspondante de $\text{SL}_2(\mathbb{C})$ sur $\mathbb{R}^{3,1}$.

Solution de l'exercice 8. Voir [Wikipedia : Clifford algebra].

[3] On remarque qu'en physique, un type de particule élémentaire libre relativiste est décrite par une représentation de $\text{Spin}_{3,1}(\mathbb{R})$. Par exemple, le photon correspond à l'action de ce groupe sur $\mathbb{R}^{3,1}$ et l'électron correspond à la représentation de spin demi-entier.

Algèbre et théorie de Galois - TD6

Exercice 1 : Soit f un polynôme séparable sur un corps K de caractéristique différente de 2 et $\Delta(f)$ son discriminant. Soit L un corps de décomposition de f sur K et $\rho : \mathrm{Gal}(L/K) \to S_{x_1,\dots,x_n}$ l'action du groupe de Galois sur les racines $x_1, \dots, x_n$ de f. Montrer que

$$\rho(\mathrm{Gal}(L/K)) \subset A_n \Leftrightarrow \Delta(f) \text{ est un carré dans } K.$$

Exercice 2 : (Groupes de galois en degré 3) Soit f un polynôme cubique séparable irréductible sur un corps K de caractéristique différente de 2 et L un corps de décomposition de f sur K. Montrer que le groupe de Galois de L/K est

a) isomorphe à $\mathbb{Z}/3\mathbb{Z}$ si $\Delta(f)$ est un carré dans K,

b) isomorphe à S_3 sinon.

Exercice 3 : (Racines p-ièmes de 2) Soit ζ_p une racine primitive p-ième de l'unité et $f = x^p - 2$.

a) Calculer le corps de décomposition L de f sur $\mathbb{Q}$.

b) Décrire explicitement le groupe de Galois G de $L/\mathbb{Q}$.

c) Donner une description du groupe G comme un groupe de matrices.

Exercice 4 : (L'extension universelle) Soit $B = \mathbb{Z}[x_1, \dots, x_n]$ et $A = \mathbb{Z}[\sigma_1, \dots, \sigma_n]$ l'anneau des polynômes en des variables abstraites $\sigma_1, \dots, \sigma_n$. On considère l'inclusion naturelle $A \subset B$ qui envoie les σ_i sur les polynômes symétriques en les x_i (coefficients de $P_{univ} := \prod_{i=1}^n (X - x_i) \in A[X]$).

a) Montrer que si L est le corps de décomposition d'un polynôme P sur un corps K et que $y_1, \dots, y_n$ sont les racines (ordonnées) de P dans L, il existe un unique diagramme commutatif

$$\begin{array}{ccc} A & \longrightarrow & B \\ {\scriptstyle a_P}\downarrow & & \downarrow{\scriptstyle b_P} \\ K & \longrightarrow & L \end{array}$$

tel que $a_P(\sigma_i) = \sigma_i(y_1)$ et $b_P(x_i) = y_i$. Calculer alors $b_P(P_{univ})$.

b) Décrire le groupe $\mathrm{Aut}_{A-alg}(B)$ des automorphismes de la A-algèbre B.

c) Définir un morphisme (appelé morphisme de spécialisation universelle) $\mathrm{Gal}(L/K) \to \mathrm{Aut}_{A-alg}(B)$. Montrer que ce morphisme est injectif.

d) En considérant par exemple le polynôme $f = x^5 - 2$, montrer le morphisme de spécialisation universelle n'est pas un isomorphisme.

Exercice 5 : (Théorie de Galois inverse) Soit G un groupe fini d'ordre n. Montrer que G est le groupe de Galois de $L = \mathbb{Q}(x_1, \dots, x_n)$ sur une sous-extension de L/K où $K = \mathbb{Q}(\sigma_1, \dots, \sigma_n)$.

Exercice 6 : Décrire complètement la correspondance de Galois pour l'extension $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.

Exercice 7 : Décrire la structure du groupe de Galois de $X^5 - 3$ sur $\mathbb{Q}$ par générateurs et relations.

Exercice 8 : (Groupes de galois en degré 4) Soit f un polynôme quadratique unitaire sur un corps K de caractéristique différente de 2, L un corps de décomposition de f et $G = \mathrm{Gal}(L/K)$. Soient $\Delta(f)(x)$ le discriminant de f et si $P_f = x_1x_2 + x_3x_4$ est le polynôme de Ferrari, on note $\theta_f(x) = \theta(P_f)(x) := \prod(x - P_{f,i})$ la résolvante de Ferrari où les $P_{f,i}$ sont tous les translatés distincts de P_f par S_n.

a) Montrer que si $\theta_f(x)$ est irréductible sur K, alors G est
   i) S_4 si $\Delta(f) \notin K^2$,
   ii) A_4 si $\Delta(f) \in K^2$.

b) Monter que $\Delta(\theta_f(x)) = \Delta(f)$.

c) Montrer que si θ_f a une racine dans K, on a une inclusion

$$G \subset D_4 := \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \cong \langle (1324), (12) \rangle \subset S_4.$$

d) Montrer que les sous-groupes de $D_4 = \langle (1324), (12) \rangle$ d'ordre 4 sont donnés par les quatre groupes

$$\langle (12), (34) \rangle,\ \langle (12)(34), (13)(24) \rangle,\ \langle (1324) \rangle,\ \langle (1324), (12) \rangle$$

et que tous sauf le premier sont transitifs.

e) Montrer que si $\theta_f(x)$ se décompose complètement sur K alors G est $\mathbb{Z}/2 \times \mathbb{Z}/2$.

f) Montrer que si $\theta_f(x)$ a une racine unique $\beta \in K$, alors G est isomorphe soit à $D_4 := \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ soit à $\mathbb{Z}/4\mathbb{Z}$.

Algèbre et théorie de Galois - TD7

Exercice 1 : (Entiers quadratiques) Si $K/\mathbb{Q}$ est une extension finie, on note O_K son anneau d'entiers.

a) Montrer que toute extension quadratique $K/\mathbb{Q}$ peut s'écrire $K = \mathbb{Q}(\sqrt{d})$ avec $d \neq 0, 1$ et d sans facteur carré.

b) Soit $K = \mathbb{Q}(\sqrt{d})$. Montrer que

i) $O_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ si $d \cong 4 \mod 4$,

ii) $O_K = \mathbb{Z}[\sqrt{d}]$ sinon.

c) Quels sont les morphismes de K dans $\mathbb{C}$? En déduire l'expression de la norme et la trace de $z = x + y\sqrt{d} \in K$. Montrer que $z \in O_K$ si et seulement si sa norme et sa trace sont dans O.

d) Déterminer le groupe des inversibles $O_K^\times$ de O_K (appelé groupe des unités) lorsque d est négatif.

e) Monter que le groupe des unités de $\mathbb{Z}[\sqrt{2}]$ est infini (c'est ce qui rend les corps quadratiques réels plus difficiles à étudier).

f) Trouver tous les rationnels x tels que $\cos(2\pi x)$ soit rationnel.

Exercice 2 : Déterminer si les éléments suivants $x \in \mathbb{C}$ sont des entiers algébriques dans leur corps de définition $\mathbb{Q}(x)$:

a) $\frac{\sqrt{3}+\sqrt{5}}{2}$,

b) $\frac{\sqrt{3}+\sqrt{7}}{2}$,

c) $\frac{\sqrt{5}+\sqrt{7}}{2}$,

d) $\frac{1+i\sqrt{3}+i\sqrt{7}-\sqrt{21}}{4}$.

Exercice 3 : (Racines quinzièmes de l'unité) On pose $\zeta = e^{\frac{2i\pi}{15}}$, $\eta = e^{\frac{2i\pi}{5}}$, $j = e^{\frac{2i\pi}{3}}$. On rappelle que $\cos\frac{2\pi}{5} = \frac{-1+\sqrt{5}}{2}$.

a) Quel est le degré de $\mathbb{Q}(\zeta)/\mathbb{Q}$? Calculer son polynôme minimal et donner la décomposition en facteurs irréductibles dans $\mathbb{Q}[X]$ de $X^15 - 1$. On note $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ et on note σ_k l'élément du groupe G tel que $\sigma_k(\zeta) = \zeta^k$.

b) Quelles sont les valeurs possibles pour k ?

c) Décrire G et calculer les ordres de ses éléments.

d) Montrer que $\mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\eta)$ et que $\mathbb{Q}(\zeta)$ est une extension de degré 2 de $\mathbb{Q}(\cos\frac{2\pi}{15})$.

e) Montrer que les extensions $\mathbb{Q}(j)$, $\mathbb{Q}(\eta)$, $\mathbb{Q}(\sqrt{5})$ et $\mathbb{Q}(j, \sqrt{5})$ sont contenues dans $\mathbb{Q}(\zeta)$ et déterminer le sous-groupe de G qui les fixe.

f) Déterminer les corps des invariants de $\langle\sigma_{14}\rangle$ et $\langle\sigma_2\rangle$.

g) Donner explicitement la correspondance de Galois entre les deux treillis de la situation.

h) Calculer une expression algébrique de $\cos\frac{2\pi}{15}$ en utilisant le groupe

$$\mathrm{Gal}(\mathbb{Q}(\cos\frac{2\pi}{15})/\mathbb{Q}(\sqrt{5})).$$

i) Dire si le polygone régulier à 15 cotés de rayon 1 est constructible à la règle et au compas.

Exercice 4 : (Groupes de Galois cyclotomiques) Soient n un entier naturel $f_n(X) = X^n - 1$. On note $L/\mathbb{Q}$ le corps de décomposition de f_n.

a) Calculer le groupe de Galois G de $L/\mathbb{Q}$.

b) Montrer que si $H \subset G$ est un sous-groupe, on a un morphisme naturel $H(p) \to G(p)$ entre les composantes p-primaires (éléments annulés par une puissance de p) pour tout p premier.

c) En déduire une méthode pour simplifier la classification des sous-groupes de G.

d) Classifier les idéaux de l'anneau $\mathbb{Z}/p^k\mathbb{Z}$ et en déduire une suite naturel de quotients de $(\mathbb{Z}/p^k\mathbb{Z})^\times$.

e) Pour p premier et k naturel, montrer les congruences

$$(1+p)^{p^k} \equiv 1 + p^{k+1} \mod (p^{k+2})$$

et

$$5^{2^k} \equiv 1 + 2^{k+2} \mod (2^{k+3}).$$

f) Montrer qu'on a une suite exacte

$$0 \to 1 + (p) \to (\mathbb{Z}/p^k\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times \to 1$$

si p est premier impair avec $1 + (p) \cong \mathbb{Z}/p^{k-1}\mathbb{Z}$ et que si $k > 2$, on a une suite exacte

$$1 \to 1 + (4) \to (\mathbb{Z}/2^k\mathbb{Z})^\times \to (\mathbb{Z}/4\mathbb{Z})^\times \to 0$$

avec $1 + (4) \cong \mathbb{Z}/2^{k-1}\mathbb{Z}$.

g) En déduire une description explicite du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ et des sous-groupes de $(\mathbb{Z}/p^k\mathbb{Z})^\times$.

h) Déterminer tous les sous-groupes de G pour $n = 3^2.7$.

i) Même question pour $n = 3^2.5^2$.

Algèbre et théorie de Galois - TD8

Exercice 1 :

a) Les $\mathbb{Z}$-modules $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Q}$ sont-ils libres ?

b) Sont-ils de type fini ?

c) Monter qu'il n'y a pas de morphismes d'anneaux de $\mathbb{C}$ dans $\mathbb{R}$, de $\mathbb{R}$ dans $\mathbb{Q}$, de $\mathbb{Q}$ dans $\mathbb{Z}$, de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}$, de $\mathbb{Z}[\sqrt{2}]$ dans $\mathbb{Z}[\sqrt{3}]$.

d) Montrer que $\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/d\mathbb{Z}$ avec $d = \mathrm{pgcd}(m, n)$.

e) Calculer $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$.

f) Calculer $\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}$.

g) Calculer $G \otimes_{\mathbb{Z}} \mathbb{Q}$ avec G un groupe abélien dont tous les éléments sont d'ordre fini.

Exercice 2 : Soit A un anneau (commutatif unitaire). Soient M, N, V des A-modules. On note $M^\vee = \mathrm{Hom}(M, \mathbb{Q})$ le dual de M.

a) Construire une bijection canonique $\mathrm{Hom}(M \otimes N, V) \cong \mathrm{Hom}(M, \mathrm{Hom}(N, V))$.

b) Construire un morphisme $M^\vee \otimes N \to \mathrm{Hom}(M, N)$ et montrer que c'est un isomorphisme si M et N sont libres de rang fini.

c) Construire un isomorphisme $(M \oplus N) \otimes V \to (M \otimes V) \oplus (N \otimes V)$.

d) En déduire que si $0 \to M \to N \to K \to 0$ est une suite exacte scindée et $A \to B$ est une A-algèbre, la suite obtenue par application de $. \otimes_A B$ est aussi exacte scindée.

e) Le morphisme de $\mathbb{Z}/2\mathbb{Z}$-modules obtenu par tensorisation du morphisme injectif de $\mathbb{Z}$-module $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ par $\mathbb{Z}/2\mathbb{Z}$ est il injectif ? Même question pour $2\mathbb{Z} \to \mathbb{Z}$ et $\mathbb{Z} \to \mathbb{Q}$?

f) En déduire que si $0 \to M \to N \to K \to 0$ est une suite exacte quelconque, on obtient en général uniquement une suite exacte

$$M \otimes_A B \to N \otimes_A B \to K \otimes_A B \to 0$$

mais le produit tensoriel ne préserve pas en général l'exactitude à gauche (i.e. l'injectivité).

Exercice 3 : Soit A un anneau commutatif unitaire.

a) Soit M un A-module et I un idéal de A. Montrer que

$$M/IM \cong M \otimes_A A/I.$$

b) Soit $A \to B$ un morphisme d'anneau (i.e. une A-algèbre). Montrer que $A[X] \otimes_A B \cong B[X]$.

c) Calculer $\mathbb{Z}[\sqrt{2}] \otimes_{\mathbb{Z}} \mathbb{Z}[\sqrt{2}]$ et $\mathbb{Z}[i] \otimes_{\mathbb{Z}} \mathbb{Z}[i]$.

d) Calculer $\mathbb{Q}[\sqrt{2}] \otimes_{\mathbb{Q}} \mathbb{Q}[i]$.

e) Calculer $\mathbb{Q}[\sqrt[3]{3}] \otimes \mathbb{Q}[j]$.

f) Calculer $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$.

Exercice 4 : Soit A un anneaux commutatif unitaire et M un A-module.

a) Définir un morphisme

$$T_A^*(M^\vee \otimes M) \to \mathrm{End}_A(M)$$

de l'algèbre tensorielle sur A dans l'algèbre des endomorphismes du A-module M.

b) Montrer que si M est libre de rang fini, le morphisme ci-dessus est surjectif.

c) Soit X un ensemble. Montrer que la A-algèbre associative libre sur X est donnée par l'algèbre tensorielle $T_A^*(A^{(X)})$ sur le A-module libre sur X.

d) En déduire une présentation de l'algèbre associative des matrices $M_n(A)$ par générateurs et relations.