TD n°5-Corrections.

1 Modules sur un anneau principal

Exercice 1. Combien y a-t-il de groupes abéliens de cardinal n=24 à isomorphisme près ? Même question pour n=48.

Solution. Notons a_n le nombre de classes d'isomorphismes de groupes abéliens de cardinal n. Si G est de cardinal 24, $G = G[2] \times G[3]$, avec $G[2]$ de cardinal 8 et $G[3]$ de cardinal 3, de plus $G \simeq G'$ si et seulement si $G[2] \simeq G'[2]$ et $G[3] \simeq G'[3]$, donc $a_{24} = a_3 a_8$. Tout groupe de cardinal 3 est monogène, donc isomorphe à $\mathbb{Z}/3\mathbb{Z}$, donc $a_3 = 1$. Les facteurs invariants d'un groupe abélien de cardinal 8 peuvent être $(2), (2), (2)$, ou $(2), (4)$ ou (8). Donc $a_{24} = a_8 = 3$.
De même $a_{48} = a_{16} a_3 = a_{16}$ et les facteurs invariants d'un groupe de cardinal 48 peuvent être $(2), (2), (2), (2)$ ou $(2), (2), (4)$ ou $(2), (8)$ ou $(4), (4)$ ou (16). Donc $a_{48} = 5$.

Exercice 2. Soient A un anneau principal et $a, b \in A$. Quels sont les facteurs invariants de $A/(a) \times A/(b)$?

Solution. Il suffit de trouver les facteurs invariants de la matrice diagonal 2×2 de coefficients diagonaux a et b. Le premier facteur invariant est donné par le pgcd des coefficients de la matrice : c'est $d = \text{pgcd}(a, b)$. Le produit des deux facteurs invariant est le déterminant de la matrice : c'est ab. Donc le deuxième facteur invariant est $ab/d = \text{ppcm}(a, b)$

Exercice 3. Soit A un anneau intègre et noetherien. Montrer que A est principal si et seulement si tous les A-modules de type fini sans torsion sont libres.

Solution. Le sens directe est un résultat du cours. Supposons récirpoquement que tous les A-modules de type fini sans torsion sont libres. Soit I un idéal de A. Comme A est noethérien, I est un A-module de type fini ; comme A est intègre, I est sans torsion. Par hypothèse, I est donc un module libre. Mais si $a, b \in I$, $b \times a - a \times b = 0$ donc (a, b) est une famille liée. Par conséquent, une base de I est de cardinal 0 (alors $I = 0$) ou 1 (alors I est un idéal principal comme voulu).

Exercice 4. Donner une base :

a) de $\mathbb{Z}^2$ adaptée à $N = \{(a, b) \in \mathbb{Z}^2 : 2|a + b\}$.

b) de $\mathbb{Z}^3$ adaptée au sous-module M engendrée par $(4, -2, 0), (2, -2, 2), (3, 0, -9)$.

Solution. a) N est un sous-module d'indice 2 de $\mathbb{Z}^2$: le morphisme $\mathbb{Z}^2 \to \mathbb{Z}$ qui à (a, b) associe $a + b$ se factorise en un isomorphisme $\mathbb{Z}^2/N \to \mathbb{Z}/2\mathbb{Z}$. Les facteurs invariants de N sont donc 1 et 2. Comme premier vecteur de notre base adapté, il faut (et il suffit de) choisir une droite D de $\mathbb{Q}^2$ telle que $D \cap \mathbb{Z}^2 = D \cap N$ et de prendre un générateur de $D \cap \mathbb{Z}^2$: on peut prendre $v_1 = (1, 1)$ par exemple. Le deuxième vecteur doit compléter v_1 en une base de $\mathbb{Z}^2$, on peut prendre $v_2 = (1, 0)$.

Exercice 5. Soit A un anneau principal, et $(a_1, a_2, a_3) \in A^3$ tels que $\text{pgcd}(a_1, a_2, a_3) = 1$. On cherche à décrire $E = \{(x_1, x_2, x_3) \in A^3, \sum_{i=1}^3 a_i x_i = 0\}$. Pour i, j, k distincts, on note $d_k = \text{pgcd}(a_i, a_j)$.

a) Montrer que E est un sous-A-module libre de A^3 de rang 2.

b) Montrer que si i, j, k sont distinct $d_i d_j | a_k$. Soit $b_k \in A$ tel que $a_k = d_i d_j b_k$.

c) Montrer que les b_i sont premiers deux à deux.

d) Soit $F = \{(y_1, y_2, y_3) \in A^3 : \sum_{i=1}^3 b_i y_i = 0\}$. Montrer que

$$\begin{array}{ccc} F & \to & E \\ (y_1, y_2, y_3) & \mapsto & (d_1 y_1, d_2 y_2, d_3 y_3) \end{array}$$

est un isomorphisme de A-modules.

e) Décrire une base de F.

f) Déterminer l'ensemble des solutions dans $\mathbb{Z}^3$ de $5x + 7y + 35z = 0$.

Solution. a) E est un sous-module d'un module libre de type fini, donc est libre car A est principal. Le rang de E est alors la dimension du K-espace vectoriel engendré E_K par E dans K^3 (où K est le corps des fractions de A). On a $E_K = \{(x_1, x_2, x_3) \in K^3, \sum_{i=1}^3 a_i x_i = 0\}$ qui est de codimension 1 (c'est le noyau d'une forme linéaire non nulle) donc de dimension 2.

b) $d_i | a_k$ et $d_j | a_k$. Or si d divise d_i et d_j, d diviserait a_i, a_j, a_k, ce qui est impossible par hypothèse. Donc d_i et d_j sont premiers entre eux, donc en utilisant le lemme de Gauss, $d_i d_j | a_k$.

c) si d divise b_i et b_j, d divise alors a_i et a_j, donc divise également d_k. Du coup d^2 divise a_i et a_j et donc également d_k. Du coup d^3 divise a_i et a_j... Par récurrence, on obtient que d doit être inversible, donc b_i et b_j sont premiers entre eux.

d) Si $(y_1, y_2, y_3)/inF$, $\sum a_i d_i y_i = \sum d_i d_j d_k b_i y_i = d_i d_j d_k \sum b_i y_i = 0$, donc on obtient bien une application linéaire de F vers E. L'injectivité est immédiate. Pour la surjectivité, soit $(x_1, x_2, x_3) \in E$. Alors $a_i x_i = -a_j x_j - a_k x_k$ est divisible par d_i. Comme a_i et d_i sont premiers entre eux, d_i divise x_i : on pose $y_i = x_i/d_i$. On verifie immédiatement que $(y_1, y_2, y_3) \in F$.

e) Soient $(u, v) \in A^2$ tels que $b_1 u + b_2 v = 1$. Alors $v_1 = (-b_3 u, -b_3 v, 1) \in F$. Si $y = (y_1, y_2, y_3) \in F$, $y - y3v_1 = (z_1, z_2, z_3) \in F$ vérifie $z_3 = 0$. Donc $b_1 z_1 + b_2 z_2 = 0$. Comme b_1, b_2 sont premiers entre eux, z_1 est multiple de b_2 : $z_1 = l b_2$ et donc $(z_1, z_2, z_3) = (l b_2, -l b_1, 0) = l v_2$ avec $v_2 = (b_2, -b_1, 0)$. Donc y est combinaison linéaire de v_1 et v_2. On vérifie facilement que v_1, v_2 forme une base de F (c'est une famille libre car échelonnée).

f) On trouve $b_1 = b_2 = b_3 = 1$, donc F admet pour base de solutions $(-1, 0, 1), (1, -1, 0)$. En utilisant l'isomorphisme de d), on obtient comme base de solutions $(-7, 0, 1), (7, -5, 0)$.

Exercice 6. a) Soit $f : \mathbb{Z}^n \to \mathbb{Z}^n$ un endomorphisme de groupe abélien. Montrer que $\mathbb{Z}^n / f(\mathbb{Z}^n)$ est fini si et seulement si $\det(f) \neq 0$, et qu'alors $\mathrm{Card}(\mathbb{Z}^n / f(\mathbb{Z}^n)) = |\det(f)|$.

b) Soit $x = a + ib \in \mathbb{Z}[i]$ avec $x \neq 0$. Montrer que $\mathrm{Card}(\mathbb{Z}[i]/(x)) = a^2 + b^2$.

Solution. a) $\mathbb{Z}^n / f(\mathbb{Z}^n)$ est de type fini. Soit $a_1 | \cdots | a_k$ et $(e_1, \cdots, e_k)$ tel que $(a_1 e_1, \cdots a_k e_k)$ forme une base de $f(M)$. Alors $\mathbb{Z}^n / f(\mathbb{Z}^n) \simeq \mathbb{Z}^{n-k} \oplus \bigoplus_i (\mathbb{Z}/a_i\mathbb{Z})$. Donc $\mathbb{Z}^n / f(M)$ est fini si et seulement si $k = n$, si et seulement si $f_{\mathbb{Q}} : \mathbb{Q}^n \to \mathbb{Q}^n$ est surjectif (car l'image de $f_{\mathbb{Q}}$ est le sous-$\mathbb{Q}$-espace vectoriel de $\mathbb{Q}^n$ engendré par $\mathbb{Z}^n / f(\mathbb{Z}^n)$, donc est de dimension k), si et seulement si $\det(f) = \det(f_{\mathbb{Q}}) \neq 0$.

Dans le cas où $f(M)$ est d'indice fini dans $\mathbb{Z}^n$, l'idéal de $\mathbb{Z}$ engendré par $\det(f)$ est le produit des idéaux invariants de $\mathbb{Z}^n / f(\mathbb{Z}^n)$, qui est donc engendré par $\prod_i a_i$. En prenant le générateur positif on obtient $|\det(f)| = \prod_i |a_i| = \mathrm{Card}(\mathbb{Z}^n / f(\mathbb{Z}^n))$.

b) On identifie $\mathbb{Z}[i]$ à $\mathbb{Z}^2$ en considérant la base $(1, i)$. Soit $f : \mathbb{Z}[i] \to \mathbb{Z}[i]$ qui à z associe xz. Alors (x) est l'image de $\mathbb{Z}^n$ et la matrice de f dans la base $(1, i)$ est

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix},$$

qui est bien de déterminant $a^2 + b^2$. On conclut en appliquant a).

2 Extensions finies de corps

Exercice 7. Montrer que pour tout corps K, il existe une infinité de polynômes unitaires irréductibles. En déduire que tout corps algébriquement clos est infini.

Solution. Si $P_1, \cdots P_n$ est une famille finie d'élément irréductible unitaire, alors $P_1 \cdots P_n + 1$ n'est divisible par aucun des P_i et n'est pas inversible : il existe donc un élément irréductible unitaire divisant $P_1 \cdots P_n + 1$ et donc distinct de tous les P_i.
Si K est algébriquement clos, les polynômes irréductibles unitaires sont les $X - a$ pour $a \in K$, et leur ensemble a donc le même cardinal que celui de K. Donc K est infini.

Exercice 8. Une extension finie de corps K/k est dite monogène s'il existe $x \in K$ tel que $K = k(x)$.

a) Montrer que toute extension de degré premier est monogène.

b) Soient K/k une extension et P un polynôme irréductible sur k. Montrer que si le degré de P est premier au degré de K/k, alors P est irréductible sur K.

c) Soient k un corps et x un élément algébrique sur k de degré impair. Montrer que $k(x^2) = k(x)$.

Solution. a) Soit $x \in K-k$. On a $k \subset k(x) \subset K$ donc $[k(x):k]|[K:k] = p$. Comme $k(x) \neq k$, $[k(x):k] \neq 1$, donc $[k(x):k] = p$ donc $k(x) = K$.

b) Soit R un facteur irréductible de P dans $K[X]$. Soit $L = K[X]/R$ le corps de rupture de R et notons x la classe de X. Alors $R(x) = 0$ donc $P(x) = 0$. Comme P est irréductible sur k, $k(x)$ est le corps de rupture de x sur k, donc $degP = [k(x):k]|[L:k] = [L:K][K:k]$. Comme $degP$ et $[K:k]$ sont premier entre eux, on obtient $degP|[L:K] = degR$ ce qui n'est possible que si R est associé à P.

c) On a $[k(x):k(x^2)] \leq 2$ car x est racine de $X^2 - x^2 \in k(x^2)[X]$. Or $[k(x):k(x^2)]|[k(x):k]$ qui est impair donc $[k(x):k(x^2)] \neq 2$. D'où l'égalité voulue.

Exercice 9. Déterminer le degré des extensions suivantes de $\mathbb{Q}$:

$$\mathbb{Q}(\sqrt{2}, \sqrt{18}, \sqrt{-7}), \qquad \mathbb{Q}(i, \sqrt[4]{2}), \qquad \mathbb{Q}(\sqrt{3}, \sqrt[3]{2}), \qquad \mathbb{Q}(\sqrt{2+\sqrt{2}}), \qquad \mathbb{Q}(i, \sqrt{2+\sqrt{2}}).$$

Solution. On a $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$ car $\sqrt{2}$ est racine de $X^2 - 2$ qui est irréductible (sinon on aurait $\sqrt{2} \in \mathbb{Q}$). Remarquons que $\sqrt{18} = 3\sqrt{2}$ est dans $\mathbb{Q}(\sqrt{2})$. Comme $\sqrt{-7})$ est racine de $X^2 + 7$, on a $[\mathbb{Q}(\sqrt{2}, \sqrt{18}, \sqrt{-7}) : \mathbb{Q}(\sqrt{2})] \leq 2$. Or, comme $\sqrt{-7} \notin \mathbb{R}$ et $[\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$, on a donc $\mathbb{Q}(\sqrt{2}, \sqrt{18}, \sqrt{-7}) \neq \mathbb{Q}(\sqrt{2})$. Donc $[\mathbb{Q}(\sqrt{2}, \sqrt{18}, \sqrt{-7}) : \mathbb{Q}(\sqrt{2})] = 2$ et $[\mathbb{Q}(\sqrt{2}, \sqrt{18}, \sqrt{-7}) : \mathbb{Q}] = 4$ par multiplicativité.

On a $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{Q}(i, \sqrt[4]{2})$.

On a $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$ comme précédemment.

On a $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})] \leq 2$ car $\sqrt[4]{2}$ est racine de $X^2 - \sqrt{2}$. Si $\sqrt[4]{2} \in \mathbb{Q}(\sqrt{2})$, on aurait $(a + b\sqrt{2})^2 = \sqrt{2}$ avec $a, b \in \mathbb{Q}$, on obtient, en décomposant dans la base $1, \sqrt{2}$, $a^2 + 2b^2 = 0$ et $2ab = 1$, on obtient $a^4 = -1/2$ dans $\mathbb{Q}$ ce qui n'est pas possible. Donc $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})] = 2$.

De même $[\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}(\sqrt[4]{2})] \leq 2$, car i est solution de $X^2 - 1$. Comme $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$ mais $i \notin \mathbb{R}$, $[\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}(\sqrt[4]{2})] \leq 2$.

Par multiplicativité, $[\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}] = 8$.

Le polynome $X^3 - 2$ est irréductible sur $\mathbb{Q}$ car sinon il aurait un facteur de degré 1, et donc aurait une racine dans $\mathbb{Q}$ ce qui n'est pas le cas. Donc $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. De même $X^2 - 3$ est irréductible sur $\mathbb{Q}$, donc sur $\mathbb{Q}(\sqrt[3]{2})$ d'après exo 9.b. Donc $[\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})] = 2$, et donc le degré cherché est 6 par multiplicativité

On a $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2+\sqrt{2}})$. L'important est de savoir si $2+\sqrt{2}$ est un carré dans $\mathbb{Q}(\sqrt{2})$. Or $N(2+\sqrt{2}) = 2$, qui n'est pas un carré dans $\mathbb{Q}$, donc $2 + \sqrt{2}$ est un carré dans $\mathbb{Q}(\sqrt{2})$. Donc $[\mathbb{Q}(\sqrt{2+\sqrt{2}}) : \mathbb{Q}(\sqrt{2})] = 2$, et $[\mathbb{Q}(\sqrt{2+\sqrt{2}}) : \mathbb{Q}] = 4$ par multiplicativité.

On a $\mathbb{Q}(\sqrt{2+\sqrt{2}}) \subset \mathbb{R}$ et $i \notin \mathbb{R}$, donc comme précédemment $[\mathbb{Q}(i, \sqrt{2+\sqrt{2}}) : \mathbb{Q}] = 2[\mathbb{Q}(\sqrt{2+\sqrt{2}}) : \mathbb{Q}] = 8$.

Exercice 10. Soit K une extension de k de degré 2.

a) On suppose que la caractéristique de k est différente de 2. Montrer qu'il existe $a \in k$ tel que K soit isomorphe à $k[X]/(X^2 - a)$. À quelle condition deux extensions de cette forme sont-elles isomorphes ? Décrire les automorphismes de K fixant k.

b) On suppose que k est de caractéristique 2. Montrer qu'il existe $a \in k$ tel que K soit isomorphe à $k[X]/(X^2 - a)$ ou à $KkX]/(X^2 - X - a)$. À quelle condition deux extensions de cette forme sont-elles isomorphes ? Décrire les automorphismes de K fixant k.

Solution. Soit $x \in K\backslash k$. La famille $1, x$ est libre sur k donc $x^2 = bx + c$. En caractéristique différente de 2, on obtient $(x + b/2)^2 = c + b^2/4$. En posant $a = c + b^2/4$ et en envoyant X sur $x + b/2$, on obtient un morphisme $k[X]/(X^2 - a) \to K$, qui est un isomorphisme car $1, x + b/2$ forment une base de K sur k. Si $b \in k$ est un carré dans $k[X]/(X^2 - a)$, alors $b = (c + d\sqrt{a})^2$, et donc $2cd = 0$ et $b = c^2 + ad^2$. Donc soit b soit b/a est un carré dans k. Or si b est un carré $k[X]/(X^2 - a)$ n'est pas un corps. Donc $k[X]/(X^2 - a)$ et $k[X]/(X^2 - b)$ sont isomorphes si et seulement si b/a est un carré.

Notons y une racine de a dans K. Si σ est un automorphisme de K fixant k. On a $\sigma(y)^2 = \sigma(y^2) = \sigma(a) = a$ donc $\sigma(y)$ est y ou $-y$. Comme y engendre K, on obtient au plus deux automorphismes possibles. On vérifie facilement que $\sigma(e + fy) = e - fy$ définit bien un automorphisme

Exercice 11. On dit qu'un nombre algébrique x est constructible à la règle et au compas si il existe une tour d'extensions de corps

$$k_0 = \mathbb{Q} \subset k_1 \subset \cdots \subset k_n$$

avec $[k_{i+1} : k_i] = 2$ et $x \in k_n$.

a) Montrer que $\sqrt[3]{2}$ n'est pas constructible à la règle et au compas.

b) Montrer que $\cos(\frac{\pi}{9})$ n'est pas constructible à la règle et au compas.

Solution. Supposons qu'il existe $k_1, \ldots, k_n$ comme dans l'énoncé avec $\sqrt[3]{2} \in k_n$. Alors $[k_n : \mathbb{Q}] = 2^n$ et $[\sqrt[3]{2} : \mathbb{Q}]$ divise 2^n donc doit être une puissance de 2. Or on a déjà dans l'exercice 11 que $[\sqrt[3]{2} : \mathbb{Q}] = 3$, donc $\sqrt[3]{2}$ n'est pas constructible à la règle et au compas.
On a $(e^{it}+e^{-it})^3 = e^{3it}+e^{-3it}+3(e^{it}+e^{-it})$. Donc $2\cos(\frac{\pi}{9})$ est racine de $P = X^3-3X-2cos(\mathfrak{Pi}/3) = X^3-3X-1$. On vérifie que $\mathbb{Q}$ est irréductible sur $\mathbb{Q}$ en vérifiant qu'il n'a pas de racine : une telle racine a serait un entier algébrique, donc un entier. Donc $1 = a^3 - 3a$ est divisible par a ce qui montre que $a = 1$ ou -1. On vérifie que 1 et -1 ne sont pas solutions.
Donc $[\mathbb{Q}(cos(\frac{\pi}{9})) : \mathbb{Q}]$ est divisible par 3, ce qui prouve la non constructibilité de $\cos(\frac{\pi}{9})$

Exercice 12. Soit L/K une extension de corps de degré 3 et soient $\alpha, \beta \in L$ tels que $L = K[\alpha] = K[\beta]$. Montrer qu'il existe $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(K)$ tel que $\beta = g \cdot \alpha = \frac{a\alpha+b}{c\alpha+d}$. Discuter l'unicité de g.

Solution. $E = \text{vect}(1, \alpha)$ est un sous-K-espace vectoriel de L dimension 2. L'application f de L dans L définie par $f : (x) = x\beta$ est K-linéaire (même L-linéaire en fait) et bijective. Donc $f(E)$ est un sous-K-espace vectoriel de dimension 2. Comme $\dim E + \dim f(E) > \dim_K L$, on en déduit qu'il existe $x \neq 0 \in E \cap f(E)$. D'où $a, b, c, d\mathbb{K}$ non tous nuls tels que $\beta(c\alpha + d) = a\alpha + b$ (mais a priori la matrice $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est seulement dans $M_2(K)$).
En intervertissant le rôle de α et β dans l'autre sens, on obtient $g' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ telle que $\alpha = (a'\beta+b')/(c'\beta+d')$.
On a donc $g'g \cdot \alpha = g \cdot \beta\alpha$, c'est-à-dire $(c''\alpha^2 + d''\alpha) = (a''\alpha + b'')$ et donc $g'g = a''\text{Id}$, avec $a'' \neq 0$, donc $g \in GL_2(K)$.
Supposons par l'absurde que $f(E) = E$. Alors $1 \in E$ et donc par récurrence $\beta^n \in E$, et donc $K[\beta] \subset E$ contrairement à l'hypothèse. Donc $E \cap f(E)$ est de dimension 1 sur K, ce qui montre l'unicité de a, b, c, d à multiplication par un scalaire commun près.

Exercice 13. Montrer que tout automorphisme de corps de $\mathbb{R}$ est l'identité (on pourra montrer qu'un tel automorphisme est nécessairement croissant).

Solution. Un tel automorphisme s conserve la propriété d'être un carré, donc la propriété d'être positif. Donc si $a \leq b$, $s(b) - s(a) = s(b - a) \leq 0$, donc s est croissant. De plus s est l'identité sur $\mathbb{Q}$ comme tout morphisme de corps. Soit $x \in \mathbb{R}$. Soit (a_n) (resp. (b_n)) une suite de rationnels tendants vers x par valeurs inférieures (par valeurs supérieurs). Alors, comme s est croissante, $a_n = s(a_n) \leq s(x) \leq s(b_n) = b_n$. En prenant la limite quand n tend vers l'infini, on obtient $s(x) = x$.