TD11 : Extensions de corps, Nullstellensatz

Diego Izquierdo

Les exercices 1, 2, 6, 8 sont à préparer avant la séance de TD. Nous traiterons les exercices dans l'ordre suivant : 1, 2, 6, 8, 15, question 1 de 19, 20, 18.

Exercice 1 : Partiel 2012
Soit K un corps. Soit L une extension algébrique de K contenue dans $K(X)$. Montrer que $L = K$.

Exercice 2 : Polynômes minimaux
Soient K un corps et L une extension finie de K. Soient x, y deux éléments de L, et P_x, P_y leurs polynômes minimaux respectifs sur K. Montrer que P_x est irréductible sur $K(y)$ si et seulement si P_y est irréductible sur $K(x)$.

> **Indications :** Supposons que P_x est irréductible sur $K(y)$. On a alors $[K(x,y) : K(y)] = \deg(P_x)$. Donc $[K(x,y) : K] = [K(x,y) : K(y)][K(y) : K] = \deg(P_x)\deg(P_y)$. Comme $[K(x,y) : K] = [K(x,y) : K(x)][K(x) : K] = [K(x,y) : K(x)]\deg(P_x)$, on en déduit que $\deg(P_y) = [K(x,y) : K(x)]$. Cela montre que P_y est irréductible sur $K(x)$. En renversant les rôles de x et y, on obtient l'implication réciproque.

Exercice 3 : Partiel 2012
Soit L/K une extension de corps algébrique de corps. Soit $P \in L[X]$. Montrer qu'il existe $Q \in K[X]$ divisible par P dans $L[X]$.

> **Indications :** Voir le corrigé du partiel 2012.

Exercice 4 : Irréductibilité de polynômes et extension de scalaires
Soient K un corps et P un polynôme irréductible de degré n sur K. Soit L une extension finie de K de degré premier à n. Montrer que P est irréductible sur L.

> **Indications :** Soit M un corps de décomposition de P sur L. Soit x une racine de P dans M. On a $\deg(P) = [K(x) : K]$. De plus, $[K(x) : K]$ et $[L : K]$ divisent $[L(x) : K]$. Comme $[L(x) : K]$ et $[L : K]$ sont premiers entre eux, on en déduit que $[K(x) : K][L : K]$ divise $[L(x) : K]$. Or $[L(x) : K] = [L(x) : L][L : K] \leq [K(x) : K][L : K]$. Donc $[L(x) : K] = [K(x) : K][L : K]$, et $[L(x) : L] = [K(x) : K] = \deg(P)$. On en déduit que P est irréductible.

Exercice 5 : Un contre-exemple
Soient $K = \mathbb{Q}(T)$ et ses deux sous-corps $K_1 = \mathbb{Q}(T^2)$ et $K_2 = \mathbb{Q}(T^2 - T)$.

Montrer que K est algébrique sur K_1 et K_2, mais pas sur $K_1 \cap K_2$.

> **Indications :** Comme T est racine des polynômes $X^2 - T^2 \in K_1(X)$ et $X^2 - X - T^2 + T \in K_2(X)$, le corps K est algébrique sur K_1 et K_2. Montrons que $K_1 \cap K_2 = \mathbb{Q}$. Soient $F_1 \in \mathbb{Q}(T)$ et $F_2 \in \mathbb{Q}(T)$ telles que $F_1(T^2 - T) = F_2(T^2)$. Soit $F = F_2(T^2)$. Comme $F_1(T - T^2)$ est invariante par $T \mapsto 1 - T$ et $F_2(T^2)$ est invariante par $T \mapsto -T$, F est invariante par $T \mapsto T + 1$. Mais alors, les zéros et les pôles de F dans $\overline{\mathbb{Q}}$ sont invariants par $t \mapsto t + 1$. Comme F ne peut avoir qu'un nombre fini de zéros et de pôles, on en déduit que F n'a pas zéros ni de pôles. Par conséquent, $F \in \mathbb{Q}$ et $K_1 \cap K_2 = \mathbb{Q}$.

Exercice 6 : Extensions de degré 2

Soient K un corps et L/K une extension de degré 2. On suppose la caractéristique de K différente de 2.

1. Montrer qu'il existe $x \in L \setminus K$ tel que l'on ait $L = K(x)$ et $x^2 \in K$.
2. Montrer alors l'égalité $L^{\times 2} \cap K^\times = K^{\times 2} \sqcup x^2 K^{\times 2}$.
3. Soient $y, z \in K^\times$. Montrer que $K(\sqrt{y})$ et $K(\sqrt{z})$ sont isomorphes en tant que K-algèbres si et seulement si zy^{-1} est un carré dans K.

Exercice 7 : Extensions de degré 2 en caractéristique 2

Soient K un corps et L/K une extension de degré 2. On suppose que la caractéristique de K est égale à 2.

1. Supposons que L n'est pas de la forme $K(x)$ avec $x^2 \in K$. Montrer qu'il existe $z \in L$ tel que l'on ait $L = K(z)$ et $z^2 - z \in K$.

   > **Indications :** Un élément y de $L \setminus K$ engendre L et vérifie une équation du type $y^2 - ay - b = 0$ avec $a, b \in K$. Parce que L n'est pas de la forme $K(\sqrt{x})$, on a $a \neq 0$ et on peut donc prendre $z = a^{-1}y$.

2. En déduire une classification des extensions de degré 2 de K à isomorphisme de K-algèbres près.

   > **Indications :** Les éléments a de L vérifiant $a^2 - a \in K$ sont $K \cup (z + K)$. De ce fait, deux extensions $K[X]/(X^2 - X - x)$ et $K[X]/(X^2 - X - y)$ sont isomorphes en tant que K-algèbres si et seulement si $x - y$ est dans l'image de l'automorphisme $\mathbb{F}_2$-linéaire $a \mapsto a^2 - a$ de K. De plus, pour $x \in K^\times$, $K[X]/(X^2 - X - x)$ n'est isomorphe à aucun $K[X]/(X^2 - y)$ puisque les seuls éléments de carré dans K de $K[X]/(X^2 - X - x)$ sont les éléments de K.

Exercice 8 : Extensions engendrées par deux racines carrées

Soient K un corps de caractéristique différente de 2. Soient $x, y \in K^\times$.

1. Montrer que l'extension $K(\sqrt{x}, \sqrt{y})$ de K est de degré 4 si et seulement si on a $x, y, xy \in K^\times \setminus K^{\times 2}$.
2. Dans ce cas, montrer que les seuls corps intermédiaires entre K et $K(\sqrt{x}, \sqrt{y})$ sont K, $K(\sqrt{x})$, $K(\sqrt{y})$, $K(\sqrt{xy})$ et $K(\sqrt{x}, \sqrt{y})$.

Exercice 9 : Partiel 2014

Soit K un corps de caractéristique différente de 2. Soient $a, b \in K^\times$, avec $b \notin K^{\times 2}$. Soient $K_1 = K(\sqrt{b})$ et $L = K(\alpha)$ avec $\alpha^2 = a + \sqrt{b}$. On rappelle (exercice 6) que $K^\times \cap K_1^{\times 2} = K^{\times 2} \sqcup bK^{\times 2}$.

1. Montrer que $L = K_1$ si, et seulement si, il existe $d \in K^\times$ tel que $a^2 - b = d^2$ et $2(a + d) \in K^{\times 2}$.
2. Montrer qu'il existe $\beta \in L^\times$ tel que $\beta^2 = a - \sqrt{b}$ si, et seulement si, $a^2 - b \in K^{\times 2} \sqcup bK^{\times 2}$.
3. Calculer $K^\times \cap L^{\times 2}$.
4. Montrer qu'il existe $c \in K^\times$ tel que $L = K(\sqrt{b}, \sqrt{c})$ si, et seulement si, $a^2 - b \in K^{\times 2}$.

Exercice 10 : Sommes de carrés

Soit $\alpha \in \mathbb{C}$ tel que $\alpha^2 = 1 + \rho\sqrt[3]{2}$.

1. Montrer que le corps $\mathbb{Q}(\alpha)$ est une extension de degré 6 de $\mathbb{Q}$.
2. Dans $\mathbb{Q}(\alpha)$, le nombre -1 est-il une somme de carrés ?

Exercice 11 : Fractions rationnelles telles que $F(x) = F\left(\frac{1}{x}\right)$

Soit K un corps. Soit $L = \{F \in K(x) \mid F(x) = F\left(\frac{1}{x}\right)\}$. Montrer que $K(y) \to L, F(y) \mapsto F(x + \frac{1}{x})$ est un K-isomorphisme de corps. C'est ce résultat qui explique par exemple pourquoi, pour résoudre les équations de la forme $\sum_{k=0}^{6} a_k x^k = 0$ avec $a_k = a_{6-k}$ pour chaque k, il suffit de savoir résoudre les équations de degré 3.

> **Indications :** On voit immédiatement que $K(x + \frac{1}{x}) \subseteq L$. De plus, comme x est racine du polynôme $t^2 - (x + \frac{1}{x})t + 1 \in K(x + \frac{1}{x})[t]$, l'extension $K(x)/K(x + \frac{1}{x})$ est de degré au plus 2. Comme $L \neq K(x)$, on en déduit que $L = K(x + \frac{1}{x})$. Reste à voir que $x + \frac{1}{x}$ est transcendant sur K, ce qui découle immédiatement de l'exercice 1.

Exercice 12 : Fractions rationnelles fixées par le groupe alterné

Soit K un corps de caractéristique différente de 2. Montrer que, pour $n \geq 2$, le sous-corps de $K(x_1, ..., x_n)$ fixé par $\mathcal{A}_n$ est : $K(x_1, ..., x_n)^{\mathcal{A}_n} = \{f + g\Delta | f, g \in K(x_1, ..., x_n)^{\mathcal{S}_n}\}$, où $\Delta = \prod_{i<j}(x_i - x_j)$.

> **Indications :** Pour $\sigma \in \mathcal{S}_n$, $f \in K(x_1, ..., x_n)^{\mathcal{S}_n}$ et $g \in K(x_1, ..., x_n)^{\mathcal{S}_n}$, on a $\sigma \cdot (f + \Delta g) = f + \epsilon(\sigma)\Delta g$, et donc $f + g\Delta \in K(x_1, ..., x_n)^{\mathcal{A}_n}$. Réciproquement, soit $h \in K(x_1, ..., x_n)^{\mathcal{A}_n}$. Soit $\tau \in \mathcal{S}_n$ une transposition. Posons $f = \frac{h + \tau \cdot h}{2}$ et $g = \frac{h - \tau \cdot h}{2\Delta}$. On a alors $h = f + g\Delta$ et on vérifie immédiatement que f et g sont dans $K(x_1, ..., x_n)^{\mathcal{S}_n}$.

Exercice 13 : Fractions rationnelles fixées par un groupe cyclique

1. Soit $n > 0$ un entier. Soit G un sous-groupe cyclique de $GL_n(\mathbb{C})$. On fait agir naturellement G sur $\mathbb{C}(x_1, ..., x_n)$. Montrer que l'extension

$\mathbb{C}(x_1,...,x_n)^G/\mathbb{C}$ est transcendante pure de degré de transcendance n.

Indications : Soit M un générateur de G. Soit m l'ordre de G.
L'action de M sur $\mathbb{C}(x_1,...,x_n)$ est définie de la manière suivante : si $F(x_1,...,x_n) \in \mathbb{C}(x_1,...,x_n)$, alors $M \star F(x_1,...,x_n) = F(y_1,...,y_n)$ où :

$$\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = M \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

On note ζ une racine primitive m-ième de l'unité. Comme G est cyclique, il existe $P \in GL_n(\mathbb{C})$ et des entiers $a_1,...,a_n$ tels que $PMP^{-1} = Diag(\zeta^{a_1},...,\zeta^{a_n})$. On pose :

$$\begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} = P \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Comme P est inversible, on a $K(x_1,...,x_n) = K(z_1,...,z_n)$ et on définit un isomorphisme de corps $K(x_1,...,x_n) \to K(z_1,...,z_n)$ en envoyant x_i sur z_i. On remarque que :

$$\begin{pmatrix} M \star z_1 \\ \vdots \\ M \star z_n \end{pmatrix} = PM \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = Diag(\zeta^{a_1},...,\zeta^{a_n})P \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \zeta^{a_1} z_1 \\ \vdots \\ \zeta^{a_n} z_n \end{pmatrix}.$$

Soit maintenant $A = \mathbb{C}[z_1,...,z_n,z_1^{-1},...,z_n^{-1}] \subseteq \mathbb{C}(z_1,...,z_n)$. Pour $b = (b_1,...,b_n) \in \mathbb{Z}^n$, on note $z^b = z_1^{b_1}...z_n^{b_n}$. Soit $P = \sum_{b\in\mathbb{Z}^n} \lambda_b z^b \in A$. On a alors :

$$M \star P = \sum_{b\in\mathbb{Z}^n} \lambda_b \zeta^{a_1 b_1 + ... a_n b_n} z^b.$$

Par conséquent, P est fixé par M si, et seulement si, $\lambda_b = 0$ dès que m ne divise pas $a_1b_1 + ... + a_nb_n$. Autrement dit,

$$A^G = \mathbb{C}[(z^b)_{b\in B}]$$

où B est noyau de $\mathbb{Z}^n \to \mathbb{Z}/m\mathbb{Z}, (b_1,...,b_n) \mapsto a_1b_1 + ... + a_nb_n$. On remarque alors que B est un groupe abélien libre de rang n. On se donne donc une base $b^{(1)},...,b^{(n)}$ de B. Comme la famille $b^{(1)},...,b^{(n)}$ engendre B, on a :

$$A^G = \mathbb{C}[z^{b^{(1)}},...,z^{b^{(n)}},z^{-b^{(1)}},...,z^{-b^{(1)}}].$$

Comme la famille $b^{(1)},...,b^{(n)}$ est libre, on définit un isomorphisme d'anneaux $A \to A^G$ en envoyant z_i sur $z^{b^{(i)}}$ et z_i^{-1} sur $z^{-b^{(i)}}$. Ce dernier s'étend en un isomorphisme entre $\mathbb{C}(z_1,...,z_n)$ et $Frac(A^G)$. Or, si P et Q sont des éléments non nuls de A et $P/Q \in \mathbb{C}(z_1,...,z_n)^G$, alors en écrivant :

$$\frac{P}{Q} = \frac{P\prod_{i=1}^{m-1}(M^i \star Q)}{\prod_{i=0}^{m-1}(M^i \star Q)},$$

on voit que $P/Q \in Frac(A^G)$. Par conséquent, $Frac(A^G) = \mathbb{C}(x_1, ..., x_n)^G$ et $\mathbb{C}(x_1, ..., x_n)^G$ est isomorphe à $\mathbb{C}(z_1, ..., z_n)$.

2. Exhiber un isomorphisme explicite entre les corps $\{F \in \mathbb{C}(x_1, ..., x_n) \mid F(x_1, x_2, ..., x_n) = F(x_2, x_3, ..., x_n, x_1)\}$ et $\mathbb{C}(y_1, ..., y_n)$.

Indications : Soit G le sous-groupe de $GL_n(\mathbb{C})$ en engendré par la matrice $M = (m_{ij})$ telle que $m_{ij} = 1$ si $i \equiv j + 1 \mod n$, $m_{ij} = 0$ sinon. On cherche $\mathbb{C}(x_1, ..., x_n)^G$.
Soit ζ une racine primitive n-ième de l'unité. Pour $0 \leq k \leq m - 1$, posons :

$$y_k = \sum_{i=1}^{m} \zeta^{ik} x_k.$$

On vérifie immédiatement que :

$$M \star y_k = \zeta^{-k} y_k.$$

En tenant compte de la question 1, on s'intéresse au noyau de

$$\mathbb{Z}^n \to \mathbb{Z}/n\mathbb{Z}, (b_0, ..., b_{n-1}) \mapsto b_1 + 2b_2 + 3b_3 + ... + n - 1b_{n-1}.$$

Si $(e_0, ..., e_{n-1})$ est la base canonique de $\mathbb{Z}^n$, une base de ce noyau est donnée par e_0, ne_1, et les $e_k - ke_1$ pour $k \geq 2$. Cela montre que l'on a un isomorphisme entre $\mathbb{C}(z_0, ..., z_{n-1})$ et $\mathbb{C}(x_1, ..., x_n)^G$ envoyant z_0 sur y_0, z_1 sur y_1^n et z_k sur $y_k y_1^{-k}$ pour $k \geq 2$.

Exercice 14 : Quelques calculs explicites

1. Déterminer le polynôme minimal de $\sqrt{2} + \sqrt{3}$ sur $\mathbb{Q}$.

2. Déterminer le polynôme minimal de $1 + \sqrt[3]{2} + 3\sqrt[3]{4}$ sur $\mathbb{Q}$.

Indications : Le polynôme $X^3 - 2 \in \mathbb{Q}[X]$ est irréductible d'après le critère d'Eisenstein. Donc l'extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ est de degré 3. Une base est donnée par $(1, \sqrt[3]{2}, \sqrt[3]{4})$. Dans cette base, la matrice de la multiplication par $1 + \sqrt[3]{2} + 3\sqrt[3]{4}$ est :

$$\begin{pmatrix} 1 & 6 & 2 \\ 1 & 1 & 1 \\ 3 & 1 & 1 \end{pmatrix}.$$

Son polynôme caractéristique est $-X^3 + 3x^2 + 10X + 8$. Comme $1 + \sqrt[3]{2} + 3\sqrt[3]{4}$ n'est pas dans $\mathbb{Q}$, son polynôme minimal est de degré 3 : c'est $X^3 - 3X^2 - 10X - 8$.

3. Calculer $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ où $\alpha = 10^{1/5} + 7^{1/3}$.

Indications : Par le critère d'Eisentein, les polynômes $X^5 - 10$ et $X^3 - 7$ de $\mathbb{Q}[X]$ sont irréductibles donc $[\mathbb{Q}(10^{1/5}) : \mathbb{Q}] = 5$ et $[\mathbb{Q}(7^{1/3}) : \mathbb{Q}] = 3$. Comme 3 et 5 sont premiers entre eux, cela montre que $[\mathbb{Q}(10^{1/5}, 7^{1/3}) : \mathbb{Q}] = 15$. On en déduit que $[\mathbb{Q}(\alpha) : \mathbb{Q}]|15$.
Soit maintenant $P \in \mathbb{Q}[X]$ le polynôme minimal de α sur $\mathbb{Q}$. Soit $Q = (X - 7^{1/3})^5 - 10 \in \mathbb{Q}(7^{1/3})[X]$. On remarque que $Q(\alpha) = 0$. Comme $\mathbb{Q}(\alpha, 7^{1/3}) = \mathbb{Q}(10^{1/5}, 7^{1/3})$, le polynôme minimal de α sur $\mathbb{Q}(7^{1/3})$ est de degré 5. C'est donc le polynôme Q. On en déduit que Q divise P. Comme $Q \notin \mathbb{Q}[X]$, le degré de P est au moins 6. Par conséquent, $[\mathbb{Q}(\alpha) : \mathbb{Q}] \geq 6$. Comme $[\mathbb{Q}(\alpha) : \mathbb{Q}]|15$, on a $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 15$.

Exercice 15 : Une question de polynômes
Soient P, Q et R des polynômes dans $\mathbb{C}[X_1, ..., X_n]$, avec P irréductible. On suppose que, pour tout $x \in \mathbb{C}^n$, si $P(x) = 0$ et $Q(x) \neq 0$, alors $R(x) = 0$. Montrer que $P|Q$ ou $P|R$.

Exercice 16 : Produit tensoriel d'algèbres réduites
Soit k un corps algébriquement clos. Soient A et B deux k-algèbres de type fini. Montrer que, si A et B sont réduites (resp. intègres), alors $A \otimes_k B$ est réduite (resp. intègre).

Exercice 17 : Points dans une variété projective
Soient k un corps algébriquement clos et $n \in \mathbb{N}$. Soit $\mathbb{P}^n(k)$ l'ensemble des droites de k^{n+1}. C'est l'espace projectif de dimension n sur k. Pour $x = (x_0, ..., x_n) \in k^{n+1} \setminus \{0\}$, on note $[x_0 : ... : x_n] \in \mathbb{P}^n(k)$ la droite engendrée par x. On se donne un idéal homogène I de $A = k[X_0, ..., X_n]$, c'est-à-dire un idéal engendré par des polynômes homogènes. On note :

$$V(I) = \{[x_0 : ... : x_n] \in \mathbb{P}^n(k) | \forall f \in I \text{ homogène}, f(x_0, ..., x_n) = 0\}.$$

Montrer que $V(I) = \emptyset$ si, et seulement si, pour $0 \leq i \leq n$, il existe $d \in \mathbb{N}$ tel que $X_i^d \in I$.

Indications : Supposons que $V(I) = \emptyset$. Soit :

$$J = \{f(1, X_1, ..., X_n) | f \in A\}.$$

C'est un idéal de $B = k[X_1, ..., X_n]$. Il définit un sous-ensemble algébrique $V(J)$ de k^n. De plus , $V(J) = \emptyset$ car $V(I) = \emptyset$. Le Nullstellensatz montre alors que $1 \in J$. Par conséquent, il existe d tel que $X_0^d \in I$. On peut bien sûr montrer le même résultat pour les autres variables.

Exercice 18 : Examen 2012
Soit A une $\mathbb{Z}$-algèbre de type fini.

1. Soit $\mathfrak{m}$ un idéal maximal de A. Dans toute la suite, on note $\mathbb{Z} \cap \mathfrak{m}$ l'image inverse de $\mathfrak{m}$ par l'application canonique $\mathbb{Z} \to A$. Montrer que l'anneau quotient $\mathbb{Z}/(\mathbb{Z} \cap \mathfrak{m})$ est soit $\mathbb{Z}$, soit un corps fini.
2. Montrer que le corps $A/\mathfrak{m}$ est une extension finie du corps des fractions de $\mathbb{Z}/(\mathbb{Z} \cap \mathfrak{m})$.
3. Si $\mathbb{Z} \cap \mathfrak{m} = 0$, montrer qu'on arrive à une contradiction. En déduire que le corps $A/\mathfrak{m}$ est fini.
4. Soit $f \in A$ un élément non nilpotent et soit $\mathfrak{n}$ un idéal maximal de l'anneau de fractions (non nul) A_f . Montrer que le corps $A_f/\mathfrak{n}$ est fini.
5. En déduire que $A/(A \cap \mathfrak{n})$ est un corps fini.
6. Montrer que l'intersection de tous les idéaux maximaux de A est $\sqrt{(0)}$.
7. En déduire que toute $\mathbb{Z}$-algèbre de type fini est un anneau de Jacobson.

Exercice 19 : Vers la théorie des modèles

1. Soient $f_1, ..., f_n \in \mathbb{Q}[X_1, ..., X_m]$. Montrer que le système d'équations $f_1(x) = ... = f_n(x) = 0$ a des solutions dans $\mathbb{C}^m$ si, et seulement si, il a des solutions dans $\overline{\mathbb{Q}}^m$.
2. Soient $x_1, ..., x_m \in \overline{\mathbb{Q}}$ et $A = \mathbb{Z}[x_1, ..., x_m]$.
   (a) Montrer qu'il existe $N \in \mathbb{N}^*$ tel que Nx_i est un entier algébrique pour chaque i.

   > **Indications :** Soit P_i un polynôme (non nul) annulateur de x_i à coefficients entiers. Soient d_i le degré et a_i le coefficient dominant de P_i. On vérifie alors que $Q_i = a_i^{d_i} P_i(X/a_i)$ est un polynôme annulateur de $a_i x_i$ et que Q_i est unitaire à coefficients dans $\mathbb{Z}$. On en déduit que $a_i x_i$ est un entier algébrique. Il suffit alors de choisir $N = a_1 ... a_m$.

   (b) Montrer que $A[1/N]$ est un $\mathbb{Z}[1/N]$-module de type fini.

   > **Indications :** Comme $Nx_1, ..., Nx_m$ sont des entiers algébriques, $\mathbb{Z}[Nx_1, ..., Nx_m]$ est un $\mathbb{Z}$-module de type fini. Notons $z_1, ..., z_k$ une famille génératrice. On voit alors aisément que $A[1/N]$ est un $\mathbb{Z}[1/N]$-module engendré par $z_1, ..., z_k$.

   (c) En déduire que, pour p premier ne divisant pas N, le quotient $A[1/N]/pA[1/N]$ n'est pas nul.

   > **Indications :** Comme $\mathbb{Z}[1/N]$ est un anneau principal et $A[1/N]$ est un $\mathbb{Z}[1/N]$-module de type fini sans torsion, il existe $r > 0$ tel que $A[1/N] \cong \mathbb{Z}[1/N]^r$ comme $\mathbb{Z}[1/N]$-module. Du coup, $A[1/N]/pA[1/N] \cong (\mathbb{Z}/p\mathbb{Z})^r \neq 0$.

3. Soient $f_1, ..., f_n \in \mathbb{Z}[X_1, ..., X_m]$. Montrer que le système d'équations $f_1(x) = ... = f_n(x) = 0$ a des solutions dans $\mathbb{C}^m$ si, et seulement si, il a des solutions dans $\overline{\mathbb{F}}_p$ pour presque tout premier p. On pourra utiliser les questions 1 et 2, ainsi que la question 3 de l'exercice 18.

Indications : Supposons que le système ait des solutions dans $\mathbb{C}$. Alors il a des solutions dans $\overline{\mathbb{Q}}$ par la question 1. Il existe donc une extension finie L de $\mathbb{Q}$ sur laquelle le système possède une solution $x = (x_1, ..., x_m)$. On adopte alors les notations de la question 2. Pour p ne divisant pas N, le quotient $A[1/N]/pA[1/N]$ n'est pas nul : l'anneau $A[1/N]$ possède donc un idéal maximal $\mathfrak{m}$ contenant p. Par réduction modulo $\mathfrak{m}$, le système d'équations a alors une solution dans $A[1/N]/\mathfrak{m}$, qui est un corps fini de caractéristique p. Par conséquent, le système a des solutions dans $\overline{\mathbb{F}_p}$ pour tout p ne divisant pas N.
Réciproquement supposons que le système n'ait pas de solutions dans $\mathbb{C}$. Alors il n'a pas de solutions dans $\overline{\mathbb{Q}}$. Donc par le Nullstellensatz, il existe $g_1, ..., g_n$ des polynômes à coefficients dans $\mathbb{Q}$ tels que $g_1 f_1 + ... + g_n f_n = 1$. Soit $M > 0$ un entier tel que Mg_i est à coefficients dans $\mathbb{Z}$ pour tout i. Si p est un nombre premier ne divisant pas M, alors en réduisant modulo p l'équation $(Mg_1)f_1 + ... + (Mg_n)f_n = M$ on voit que le système d'équations $f_1 = ... = f_n = 0$ n'a pas de solutions dans $\overline{\mathbb{F}_p}$. Cela achève la preuve.

Exercice 20 : Fractions symétriques

Soit K un corps. Soient $\sigma_1, ..., \sigma_n$ les polynômes symétriques élémentaires de $K[X_1, ..., X_n]$. Soient $E = K(X_1, ..., X_n)$ et $F = K(\sigma_1, ..., \sigma_n)$.

1. Montrer que E est une extension finie de F.
2. En déduire que $(\sigma_1, ..., \sigma_n)$ est une base de transcendance de E. En particulier, l'extension F/K est transcendante pure.
3. On fait agir $\mathcal{S}_n$ sur E par permutation des variables. Soit $F' = E^{\mathcal{S}_n}$ le sous-corps de E fixé par $\mathcal{S}_n$. On admet que $[E : F'] = |\mathcal{S}_n|$ (c'est le lemme d'Artin qui sera vu plus tard dans le cours). Montrer que $F = F'$.

Exercice 21 : Extensions de corps de type fini

Soit $M/L/K$ une tour d'extensions de corps.

1. Soit $\alpha \in M$ (resp. $t \in M$) algébrique sur K (resp. transcendant sur K). Montrer que $[K(\alpha) : K] = [K(\alpha, t) : K(t)]$.
2. Supposons que M/K est une extension de corps de type fini et que L/K est algébrique. Montrer que $[L : K] < +\infty$.
3. Montrer que si M/K est de type fini, L/K est de type fini.