Algèbre – Devoir à la maison II

Problème 1 — Équations de Mordell. Pour $k \in \mathbf{Z}$, on notera $E_k : y^2 = x^3 + k$. Mordell a établi en 1920 que pour tout entier k, l'équation E_k possède un nombre fini de solutions $(x, y) \in \mathbf{Z}^2$. L'objet de ce problème est d'étudier quelques valeurs particulières de k.

1. On suppose dans cette question que $k = -5$ et on suppose qu'on dispose d'une solution $(x, y) \in \mathbf{Z}^2$ de E_{-5}.
   (a) Montrer que l'on peut supposer y pair et $x \equiv 1 \mod 4$.
   (b) En écrivant $y^2 + 4 = x^3 - 1 = (x-1)(x^2+x+1)$, aboutir à une contradiction et en déduire que E_{-5} n'a pas de solution entière. *On pourra utiliser librement le fait que -1 est un carré modulo p si, et seulement si, $p \not\equiv 3 \mod 4$.*
2. On suppose dans cette question que $k = -2$. On note $\mathbf{Z}[i\sqrt{2}]$ le sous-anneau de $\mathbf{C}$ engendré par $i\sqrt{2}$.
   (a) Justifier qu'il existe un polynôme à coefficients entier P tel que $\mathbf{Z}[i\sqrt{2}] \cong \mathbf{Z}[X]/(P)$. Établir que $\mathbf{Z}[i\sqrt{2}]$ est un anneau euclidien pour le stathme donné par $N(z) = z\overline{z}$ pour $z \in \mathbf{Z}[i\sqrt{2}]$.
   (b) Soit à présent $(x, y) \in \mathbf{Z}^2$ une solution de E_{-2}. Justifier que l'on peut supposer x et y impairs.
   (c) Montrer que $y + i\sqrt{2}$ et $y - i\sqrt{2}$ sont premiers entre eux dans $\mathbf{Z}[i\sqrt{2}]$. *On pourra penser à utiliser N.*
   (d) Démontrer que $y + i\sqrt{2}$ et $y - i\sqrt{2}$ sont des cubes dans $\mathbf{Z}[i\sqrt{2}]$.
   (e) Déterminer toutes les solutions de E_{-2}.
   (f) Pouvait-on appliquer cette méthode pour étudier les solutions de E_{-5} ?

Solution.

1. On suppose dans cette question que $k = -5$ et on suppose qu'on dispose d'une solution $(x, y) \in \mathbf{Z}^2$ de E_{-5}.
   (a) On a $y^2 \equiv x^3 - 1 \pmod 4$. En dressant la table modulo 4, on constate que $y^2 \equiv 0, 1 \pmod 4$ tandis que $x^3 - 1 \equiv 0, 2, 3 \pmod 4$. On doit donc avoir $4 \mid y^2$ soit y pair et $x^3 \equiv 1 \pmod 4$. Cela impose $x \equiv 1 \pmod 4$ puisque $3^3 \equiv 3 \pmod 4$.
   (b) On a $y^2 + 4 = x^3 - 1 = (x-1)(x^2+x+1)$ avec $x^2 + x + 1 \equiv 3 \pmod 4$ donc en particulier impair. Par ailleurs, $x^2 + x + 1$ est de discriminant strictement positif donc reste strictement positif et $\geqslant 3$ pour x entier non nul. Il s'ensuit que $x^2 + x + 1$ doit avoir un facteur premier p congrus à 3 modulo 4. Modulo p, il vient $y^2 + 4 \equiv 0 \pmod p$ ce qui implique que -1 est un carré modulo p, ce qui est absurde. On a donc pas de solution !
2. On suppose dans cette question que $k = -2$. On note $\mathbf{Z}[i\sqrt{2}]$ le sous-anneau de $\mathbf{C}$ engendré par $i\sqrt{2}$.
   (a) On pose $P = X^2 + 2$. Montrons que $\mathbf{Z}[i\sqrt{2}] \cong \mathbf{Z}[X]/(P)$. Le morphisme d'évaluation $\varphi : P \in \mathbf{Z}[X] \to P(i\sqrt{2}) \in \mathbf{Z}[i\sqrt{2}]$ est surjectif car par définition du sous-anneau engendré, on a
   $$\mathbf{Z}[i\sqrt{2}] = \left\{ P(i\sqrt{2}) \,:\, P \in \mathbf{Z}[X] \right\}.$$
   On a alors que $(P) \subseteq \mathrm{Ker}(\varphi)$. Réciproquement, si $P \in \mathrm{Ker}(\varphi)$, comme P est unitaire (attention que $\mathbf{Z}[X]$ n'est PAS euclidien), il vient Q à coefficients entier et $a, b \in \mathbf{Z}$ tels que $P = (X^2+2)Q + aX + b$. On a ainsi
   $$0 = ai\sqrt{2} + b \quad \text{soit} \quad a = b = 0 \quad \text{et} \quad P = (X^2+2)Q.$$
   On conclut alors que $(P) = \mathrm{Ker}(\varphi)$ et par théorème d'isomorphisme. On montre que $\mathbf{Z}[i\sqrt{2}]$ est un anneau euclidien pour le stathme donné par $N(z) = z\overline{z}$ pour $z \in \mathbf{Z}[i\sqrt{2}]$ exactement comme dans le TD dans le cas de $\mathbf{Z}[i]$ car la norme est donnée par $a^2 + 2b^2$ et $\frac{1}{4} + \frac{2}{4} = \frac{3}{4} < 1$.
   (b) Soit $(x, y) \in \mathbf{Z}^2$ une solution de E_{-2}. Si x est pair, alors $y^2 \equiv -2 \pmod 8$ mais on vérifie que -2 n'est pas un carré modulo 8. Ainsi, x est pair et nécessairement y aussi puisque $y^2 = x^3 - 2$.
   (c) Noter que l'anneau est euclidien donc factoriel et toutes ces notions sont donc bien définies. Soit d un facteur commun. Alors d divise leur différence, soit $d \mid 2i\sqrt{2}$. On a donc $N(\delta) \mid 8$. Mais, par ailleurs, $N(\delta) \mid N(y + i\sqrt{2}) = y^2 + 2$ qui est impair puisque y est pair. Il s'ensuit que $N(\delta) = 1$ et donc δ est inversible, d'où le résultat !
   (d) On a que
   $$x^3 = y^2 + 2 = (y + i\sqrt{2})(y - i\sqrt{2}).$$
   On en déduit que $y + i\sqrt{2}$ et $y - i\sqrt{2}$ sont (à un inversible près) des cubes dans $\mathbf{Z}[i\sqrt{2}]$ car cet anneau est factoriel et qu'ils sont premiers entre eux. On vérifie que les inversibles qui sont les éléments de norme 1 sont ± 1 et sont eux-mêmes des cubes pour conclure !
   (e) On a donc l'existence de deux entiers r et s tels que
   $$y + i\sqrt{2} = (s + i\sqrt{2}t)^3 \quad \text{soit} \quad y = s^3 - 6st^2 \quad \text{et} \quad 1 = t(3s^2 - 2t^2).$$
   On déduit de la seconde équation que $t = \pm 1$. Si $t = 1$, la seconde équation devient $1 = 3s^2 - 2$ qui implique $s = \pm 1$. Il s'ensuit que $y = \pm 5$ et donc $x^3 = 27$ soit $x = 3$. Lorsque $t = -1$, la seconde équation fournit $1 = 2 - 3s^2$ soit $3s^2 = 1$ qui n'a pas de solution entière. On a donc obtenu que l'ensemble des solutions a deux éléments : $(3, \pm 5)$.

(f) Non car l'anneau $\mathbf{Z}[i\sqrt{5}]$ n'est pas factoriel car $9 = 3 \times 3 = (2 - i\sqrt{5})(2 + i\sqrt{5})$. Or, on a une norme sur $\mathbf{Z}[i\sqrt{5}]$ donnée par $N(a + i\sqrt{5}) = a^2 + 5b^2$ et on montre comme en TD qu'un élément est inversible si, et seulement s'il est de norme 1. Par ailleurs N est multiplicative. On obtient alors du fait qu'il n'existe pas d'élément de norme 3 que $3, 2 \pm i\sqrt{5}$ sont irréductibles. On a pas unicité dans la décomposition en produit d'irréductibles et l'anneau n'est donc pas factoriel.

Problème 2 — Une autre approche du groupe de Galois. Soit k un corps. Dans tout le problème, on se donne un polynôme $P \in k[T]$ unitaire, irréductible, séparable, de degré $n \geqslant 1$.
Soit L un corps de décomposition de P sur k. On note $x_1, \dots, x_n$ les racines de P dans L. Par définition, une *relation algébrique* entre les racines de P est un polynôme $R \in k[X_1, \dots, X_n]$ tel que $R(x_1, \dots, x_n) = 0$. On note I_P l'ensemble de ces relations algébriques entre les racines de P.

1. Montrer que I_P est un idéal de $k[X_1, \dots, X_n]$ et montrer l'existence d'un isomorphisme de k-algèbres entre $k[X_1, \dots, X_n]/I_P$ et L. Justifier que la connaissance de I_P détermine le polynôme P (et donc ses racines).

On définit G_P comme l'ensemble des permutations $\sigma \in \mathfrak{S}_n$ telles que[1]

$$\forall R \in I_P, \quad \sigma \cdot R \in I_P.$$

2. Montrer en utilisant l'isomorphisme de k-algèbre de la question **1.** que tout $\sigma \in G_P$ fournit un automorphisme de L laissant k invariant.

3. Établir que G_P est un sous-groupe de $\mathfrak{S}_n$ isomorphe à $\mathrm{Gal}(L/k)$.

On cherche maintenant des générateurs de l'idéal I_P. On pose $k_0 = k$ et $k_i = k(x_1, \dots, x_i)$ pour tout $i \in \{1, \dots, n\}$. On note $\mu_i(T) \in k_{i-1}[T]$ le polynôme minimal de x_i sur k_{i-1} et on pose $d_i = \deg(\mu_i)$.

4. Montrer que pour tout $i \in \{1, \dots, n\}$, il existe un unique polynôme $R_i \in k[X_1, \dots, X_i]$ vérifiant les propriétés suivantes :

(i) Le polynôme R_i est unitaire de degré d_i en X_i ;

(ii) Pour tout $1 \leqslant j \leqslant i-1$, on a $\deg_{X_j}(R_i) \leqslant d_j - 1$;

(iii) On a $R_i(x_1, \dots, x_{i-1}, T) = \mu_i(T)$.

5. Montrer que pour tout $i \in \{1, \dots, n\}$, on a un isomorphisme de k-algèbres entre $k[X_1, \dots, X_i]/(R_1, \dots, R_i)$ et k_i. En déduire que $I_P = (R_1, \dots, R_n)$.

6. Calculer les groupe de Galois et les générateurs explicites de la question **4.** de l'idéal I_P dans les cas suivants :

(i) $k = \mathbf{F}_2$ et $P = X^3 + X + 1$;

(ii) $k = \mathbf{Q}$ et $P = X^3 - 2$;

(iii) $k = \mathbf{Q}$ et $P = X^4 - 2X^2 + 2$.

Indication : Pour le cas ***(i)****, on pourra établir que si α est racine de P, alors α^2 et $\alpha + \alpha^2$ aussi.*

On cherche maintenant à établir une formule explicite générale pour les polynômes R_i. On pose $G = \mathrm{Gal}(L/k) = \{\sigma_1, \dots, \sigma_N\}$. Pour tout $y \in L$, on définit le vecteur

$$Gy = (\sigma_1(y), \dots, \sigma_N(y)) \in L^N.$$

7. Soient $y_1, \dots, y_r \in L$. Montrer que les conditions suivantes sont équivalentes :

(a) La famille $(y_1, \dots, y_r)$ est k-libre dans L ;

(b) La famille $(Gy_1, \dots, Gy_r)$ est L-libre dans L^N.

Indication : Pour l'implication non triviale, on pourra considérer une relation de dépendance minimale et évaluer en $\sigma \in G$ pour tout $\sigma \in G$ pour en déduire que les coefficients de cette relation de dépendance sont en réalité dans k.

Dans la suite, on fixe un entier $i \in \{1, \dots, n\}$.

8. Montrer que R_i est l'unique polynôme de $L[X_1, \dots, X_i]$ qui vérifie **4.(i), 4.(ii)** et qui s'annule en $(\sigma(x_1), \dots, \sigma(x_i))$ pour tout $\sigma \in G$.

L'extension L/k_i est galoisienne et on note $G_i = \mathrm{Gal}(L/k_i)$ son groupe de Galois, qui est un sous-groupe de G.

9. Montrer que pour $\sigma \in G$ et $1 \leqslant j \leqslant i$, l'élément $\sigma(x_j)$ ne dépend que de la classe de σ dans l'ensemble quotient G/G_i.

Pour tout $\sigma \in G$, on définit l'ensemble

$$C_{\sigma,i} = \left\{\tau(x_i) \ : \ \tau \in G, \ \tau_{|k_{i-1}} = \sigma_{|k_{i-1}}\right\} \smallsetminus \{\sigma(x_i)\}.$$

10. Montrer que $C_{\sigma,i}$ ne dépend que de la classe de σ dans l'ensemble quotient G/G_i et préciser le cardinal de $C_{\sigma,i}$.

11. Montrer la formule d'interpolation suivante

$$R_i = X_i^{d_i} - \sum_{[\sigma] \in G/G_i} \sigma(x_i)^{d_i} \left(\prod_{y_1 \in C_{\sigma,1}} \frac{X_1 - y_1}{\sigma(x_1) - y_1}\right) \cdots \left(\prod_{y_i \in C_{\sigma,i}} \frac{X_i - y_i}{\sigma(x_i) - y_i}\right)$$

et comparer avec vos résultats en question **6.**

1. On rappelle que $\sigma \cdot R(X_1, \dots, X_n) = R(X_{\sigma(1)}, \dots, X_{\sigma(n)})$.

Remarque.– Noter que cette définition du groupe de Galois est beaucoup plus proche de la définition originelle de Galois que l'on peut trouver ci-dessous, extrait de son *Mémoire sur les conditions de résolubilité des équations par radicaux*, texte manuscrit de 1830, publié en 1846 au *Journal de mathématiques pures et appliquées* après sa redécouverte par Liouville en 1843, près de dix ans après la mort de Galois.

PROPOSITION I.

Théorème. « Soit une équation donnée, dont $a, b, c, \ldots$ sont les » m racines. Il y aura toujours un groupe de permutations des lettres » $a, b, c, \ldots$ qui jouira de la propriété suivante :
» 1°. Que toute fonction des racines, invariable [*] par les substi- » tutions de ce groupe, soit rationnellement connue ;
» 2°. Réciproquement, que toute fonction des racines, déterminable » rationnellement, soit invariable par les substitutions. »

Solution.

1. Il est clair que I_P est stable par somme et par multiplication par tout élément de $K[X_1, \ldots, X_n]$ et forme donc un idéal. Par ailleurs, on a un morphisme de K-algèbre fournit par l'évaluation en $(x_1, \ldots, x_n)$

$$\varphi : \left\{ \begin{array}{ccc} K[X_1, \ldots, X_n] & \longrightarrow & L \\ R & \longrightarrow & R(x_1, \ldots, x_n). \end{array} \right.$$

Ce morphisme est surjectif car L est engendré par $x_1, \ldots, x_n$ et son noyau est précisément[2] I_P de sorte que le premier théorème d'isomorphisme fournit le résultat ! En particulier, I_P est un idéal maximal[3] !

Les relations racines-coefficients assurent que[4]

$$(x_1, \ldots, x_n) \text{ racines de } P \iff \forall 1 \leqslant k \leqslant n, \quad a_{n-k} = (-1)^k a_n \sum_{\substack{J=\{i_1,\ldots,i_k\} \subseteq \{1,\ldots,n\} \\ \#J=k}} x_{i_1} x_{i_2} \cdots x_{i_k}.$$

On obtient ainsi des éléments de I_P dont les coefficients constants fournissent les coefficients $a_0, \ldots, a_{n-1}$ et on obtient donc P et ses racines (à partir uniquement de n relations). Noter que ces relations ne différencient pas les racines puisqu'elles sont parfaitement symétriques en les $x_1, \ldots, x_n$. Ce sont à travers les autres relations algébriques que chaque racine exprime ses spécificités.
Une autre façon de voir les choses est de voir que l'isomorphisme de K-algèbres entre $K[X_1, \ldots, X_n]/I_P$ et L donne lieu à un isomorphisme de K-algèbres entre $(K[X_1, \ldots, X_n]/I_P)[T]$ et $L[T]$ dont on voit qu'il envoie le polynôme $\prod_{i=1}^{n} (T - \overline{X_i})$ sur P. En d'autres termes, la classe de X_i correspond à x_i à travers l'isomorphisme entre $K[X_1, \ldots, X_n]/I_P$ et L.

2. Par définition, $\sigma \in G_P$ laisse I_P invariant. On a donc que σ induit un morphisme de corps sur $K[X_1, \ldots, X_n]/I_P$ via[5]

$$\tilde{\sigma} : \left\{ \begin{array}{ccc} K[X_1, \ldots, X_n]/I_P & \longrightarrow & K[X_1, \ldots, X_n]/I_P \\ \pi(R) & \longmapsto & \pi(\sigma \cdot R). \end{array} \right.$$

Cette application est bien définie car si $\pi(R) = \pi(S)$, alors $R = S + Q$ avec $Q \in I_P$ et $\sigma \cdot R = \sigma \cdot S + \sigma \cdot Q$ avec par définition $\sigma \cdot Q \in I_P$ de sorte que $\pi(\sigma \cdot R) = \pi(\sigma \cdot S)$. On a alors clairement un morphisme surjectif[6] qui, via l'isomorphisme $\tilde{\varphi}$ entre $K[X_1, \ldots, X_n]/I_P$ et L fournit un morphisme surjectif du corps L via

$$\hat{\sigma} : \left\{ \begin{array}{ccc} L & \longrightarrow & L \\ x & \longmapsto & \tilde{\varphi}\left(\tilde{\sigma}\left(\tilde{\varphi}^{-1}(x)\right)\right). \end{array} \right.$$

Reste à voir que ce morphisme fixe K. Soit alors $x \in K$, on a que $\tilde{\varphi}_{|K} = \mathrm{Id}_K$ de sorte que $\hat{\sigma}(x) = \tilde{\varphi}(\tilde{\sigma}(x)) = \tilde{\varphi}(x) = x$ car x est ici vu comme polynôme constant de $K[X_1, \ldots, X_n]$ et donc $\sigma \cdot x = x$. On a ainsi le résultat ! En particulier, il est intéressant (puisque ces éléments engendrent L) de voir comment $\hat{\sigma}$ agit sur x_i pour $i \in \{1, \ldots, n\}$. On a que $\tilde{\varphi}^{-1}(x_i) = \pi(X_i)$ et par conséquent

$$\hat{\sigma}(x_i) = \tilde{\varphi}(\tilde{\sigma}(\pi(X_i)) = \tilde{\varphi}(X_{\sigma(i)}) = x_{\sigma(i)}.$$

3. On commence par vérifie que G_P est un sous-groupe. On a pour tout $\sigma, \sigma' \in G_P$ et $R \in I_P$, $(\sigma \circ \sigma') \cdot R = \sigma \cdot (\sigma' \cdot R)$ et donc $(\sigma \circ \sigma') \cdot R \in I_P$ et $\sigma \circ \sigma' \in G_P$. Pour la satbilité par passage à l'inverse, si $\sigma \in G_P$, on note r son ordre dans $\mathfrak{S}_n$. Si $r = 1$, alors

2. Ce qui permet de retrouver qu'il s'agit d'un idéal !
3. Noter que si K est algébriquement clos, on obtient $I_P = \langle X_1 - x_1, \ldots, X_n - x_n \rangle$ et on retrouve la forme des idéaux maximaux vus en TD.
4. Si $P = X^n + \sum_{k=0}^{n-1} a_k X^k$.
5. On posera $\pi : K[X_1, \ldots, X_n] \to K[X_1, \ldots, X_n]/I_P$ la surjection canonique.
6. En effet, $\pi(\sigma^{-1} \cdot R)$ est un antécédent de $\pi(R)$.

immédiatement $\sigma^{-1}\cdot R = R \in I_P$ et sinon on a par le premier point que $\sigma^{r-1}\cdot R = \in I_P$ mais $\sigma^{r-1} = \sigma^{-1}$ de sorte que $\sigma^{-1} \in I_P$ et finalement G_P est bien un sous-groupe de $\mathfrak{S}_n$.
On a par la question précédente, une application bien définie[7]

$$\theta : \left\{ \begin{array}{ccc} G_P & \longrightarrow & \mathrm{Gal}(L/K) \\ \sigma & \longmapsto & \hat{\sigma}. \end{array} \right.$$

On vérifie qu'il s'agit bien d'un morphisme de groupes en utilisant le fait que $\sigma \cdot R$ est une action du groupe $\mathfrak{S}_n$ sur $K[X_1,\dots,X_n]$. Reste à voir qu'il est bijectif. On considère pour commencer $\sigma \in \mathrm{Ker}(\theta)$. On a donc $x_{\sigma(i)} = x_i$ pour tout $i \in \{1,\dots,n\}$. Comme les racines de P sont deux à deux distinctes (car P est séparable), cela implique $\sigma(i) = i$ pour tout $i \in \{1,\dots,n\}$ et donc $\sigma = \mathrm{Id}$.
Reste alors à établir la surjectivité. On se donne un élément $f \in \mathrm{Gal}(L/K)$. On a alors (comme en cours) que f induit une permutation $\sigma \in \mathfrak{S}_n$ car pour tout $i \in \{1,\dots,n\}$, $P(f(x_i)) = 0$ donc $f(x_i) = x_{\sigma(i)}$. On a alors clairement que $\sigma \in G_P$ car si R est dans I_P, alors

$$\sigma \cdot R(x_1,\dots,x_n) = R(f(x_1),\dots,f(x_n)) = f(R(x_1,\dots,x_n)) = 0.$$

car f est un morphisme de corps si bien que $\sigma \cdot R \in I_P$. On vérifie enfin que σ est un antécédent de f car $\hat{\sigma}$ envoie x_i sur $x_{\sigma(i)} = f(x_i)$ donc $\hat{\sigma}$ et f sont deux mrophismes de corps qui coïncident sur x_i et comme les x_i engendrent L, tout élément de L est polynôme à coefficients dans K en les x_i de sorte que $\hat{\sigma} = f$ et on a le résultat!

4. On constate que $R_1 = \mu_1$ convient et que c'est l'unique polynôme qui convient par **(iii)**. Supposons construits $R_1,\dots,R_i$ et expliquons comment construire R_{i+1} et pourquoi il est unique. On a par définition que

$$\mu_{i+1}(T) = T^{d_{i+1}} + \sum_{k=0}^{d_{i+1}-1} a_k T^k$$

avec $a_k \in K_i = K(x_1,\dots,x_i)$. En particulier, pour tout k, $a_k = Q_k(x_1,\dots,x_i)$ avec $Q_k \in K[X_1,\dots,X_i]$. On peut effectuer la division euclidienne successive[8] de chaque Q_k par $\mu_1(X_1), \mu_2(X_2),\dots,\mu_i(X_i)$ et obtenir

$$Q_k(x_1,\dots,x_i) = \sum_{s=1} \hat{\imath} Q_s(x_1,\dots,x_i)\mu_i(x_i) + R_k(x_1,\dots,x_i) = R_k(x_1,\dots,x_i)$$

avec R_k de degré inférieur à $d_j - 1$ pour tout $1 \leqslant j \leqslant i$. On pose alors

$$R_{i+1}(X_1,\cdots,X_{i+1}) = X_{i+1}^{d_{i+1}} + \sum_{k=0}^{d_{i+1}-1} R_k(X_1,\dots,X_i)X_{i+1}^k$$

et R_{i+1} convient! Reste à justifier l'unicité. Or le point **(iii)** implique que si l'on a deux tels polynômes R_i et R_i' de la forme

$$R_{i+1}(X_1,\dots,X_{i+1}) = X_{i+1}^{d_{i+1}} + \sum_{k=0}^{d_{i+1}-1} R_k(X_1,\dots,X_i)X_{i+1}^k \quad \text{et} \quad R'_{i+1}(X_1,\dots,X_{i+1}) = X_{i+1}^{d_{i+1}} + \sum_{k=0}^{d_{i+1}-1} R'_k(X_1,\dots,X_i)X_{i+1}^k$$

alors on a $R_k(x_1,\dots,x_i) = R'_k(x_1,\dots,x_i)$ pour tout k. Or, l'extension K_i de K est de degré $d_1 d_2 \cdots d_i$ (par multiplicativité des degrés) et on constate aisément que la famille $x_1^{d_1-k_1} x_2^{d_2-k_2} \cdots x_i^{d_i-k_i}$ pour $1 \leqslant k_j \leqslant d_j$ est une K-base de K_i (par exemple parce qu'elle est génératrice et possède le bon cardinal! On en déduit donc par liberté que $R_k = R'_k$ pour tout k et par suite que $R_{i+1} = R'_{i+1}$ et on a bien l'unicité!

5. On établit le résultat par récurrence sur i avec l'hypothèse supplémentaire que la classe de X_i est envoyée sur x_i. C'est clair pour $i = 1$ par définition du polynôme minimal et du corps de rupture. Supposons le résultat établi au rang $i-1$. On a alors (comme vu en TD)

$$K[X_1,\dots,X_i]/(R_1,\dots,R_i) \cong (K[X_1,\dots,X_{i-1}]/(R_1,\dots,R_{i-1}))\,[X_i]/(\overline{R}_i).$$

En effet, pour tout polynôme $R \in K[X_1,\dots,X_i] = K[X_1,\dots,X_{i-1}][X_i]$, comme $R_1,\dots,R_{i-1}$ ne vont intervenir que les indéterminées $X_1,\dots,X_{i-1}$, on a un morphisme de réduction des coefficients modulo $(R_1,\dots,R_{i-1})$. Ce morphisme est surjectif et de noyau $(R_1,\dots,R_{i-1})$ si bien que[9]

$$K[X_1,\dots,X_i]/(R_1,\dots,R_{i-1}) \cong (K[X_1,\dots,X_{i-1}]/(R_1,\dots,R_{i-1}))\,[X_i].$$

Il s'ensuit que, par hypothèse de récurrence,

$$K[X_1,\dots,X_i]/(R_1,\dots,R_i) \cong K_{i-1}[X_i](\overline{R}_i) = K_{i-1}[X_i](R_i(x_1,\dots,x_{i-1},X_i)) = K_{i-1}[X_i]/(\mu_i) \cong K_{i-1}(x_i) = K_i.$$

7. Noter que puisque P est séparable et L le corps de décomposition de P, l'extension L de K est bien galoisienne!
8. Car de coefficient dominant inversible.
9. Penser au cas de $\mathbf{Z}[X]/(2) \cong (\mathbf{Z}/2\mathbf{Z})\,[X]$.

On a donc que $(R_1, \dots, R_n)$ est un idéal maximal clairement contenu dans I_P avec $I_P \neq K[X_1, \dots, X_n]$ de sorte que $I_P = (R_1, \dots, R_n)$. Noter qu'on pouvait aussi considérer le morphisme d'évaluation

$$f : \begin{cases} K[X_1, \dots, X_i] & \longrightarrow & K_i \\ R & \longrightarrow & P(x_1, \dots, x_i) \end{cases}$$

qui est surjectif par définition de K_i. On a alors clairement que $(R_1, \dots, R_i) \subseteq \mathrm{Ker}(f)$ et on peut établir l'inclusion réciproque par récurrence. C'est clair pour $i = 1$ et supposons le résultat au rang $i-1$. Soit $R \in \mathrm{Ker}(f)$. On a alors $R(x_1, \dots, x_i) = 0$ donc $R(x_1, \dots, x_{i-1}, X_i)$ est un multiple de $\mu_i(X_i)$ dans $K_{i-1}[X_i]$. On a donc $R(x_1, \dots, x_{i-1}, X_i) = \mu_i(X_i)\underline{S}(x_1, \dots, x_{i-1}, X_i)$ avec $S \in K[X_1, \dots, X_i]$. Or, par hypothèse de récurrence, $K[X_1, \dots, X_{i-1}]/(R_1, \dots, R_{i-1}) \to K_{i-1}$ donné par $\overline{Q} \mapsto Q(x_1, \dots, x_{i-1})$ est un isomorphisme de sorte qu'on obtient un isomorphisme entre $K[X_1, \dots, X_{i-1}]/(R_1, \dots, R_{i-1})[X_i] \cong K[X_1, \dots, X_i]/(R_1, \dots, R_{i-1})$ et $K_{i-1}[X_i]$. Or, $R(x_1, \dots, x_{i-1}, X_i) - \mu_i(X_i)S(x_1, \dots, x_{i-1}, X_i) = R(x_1, \dots, x_{i-1}, X_i) - R_i(x_1, \dots, x_{i-1}, X_i)S(x_1, \dots, x_{i-1}, X_i)$ est dans le noyau de cet isomorphisme et donc $R - SR_i \in (R_1, \dots, R_{i-1})$ ce qui termine la preuve.

6. **(i)** On remarque que si α est racine de P (dans un corps de rupture), alors

$$P(\alpha^2) = P(\alpha)^2 = 0 \quad \text{et} \quad P(\alpha + \alpha^2) = \alpha^3 + \alpha^4 + \alpha^5 + \alpha^6 + \alpha + \alpha^2 + 1 = P(\alpha) + \alpha^2(1 + \alpha^2 + \alpha^3 + \alpha^4) = \alpha^2 P(\alpha) = 0$$

en développant et car on est e caractéristique 2 et car $\alpha^4 = \alpha^2 + \alpha$. Un corps de rupture est donc le corps de décomposition et on $L = \mathbf{F}_2(\alpha) \cong \mathbf{F}_{2^3}$ qui est de degré 3 car P est irréductible de degré 3 (car par exemple de degré 3 sans racine sur $\mathbf{F}_2$). Une telle extension est normale (en tant que corps de décomposition) et séparable car P l'est (car toutes ses racines sont distinctes [10]), on a donc une extension galoisienne. Noter que $\alpha + \alpha^2 = \alpha^4$ et $\alpha^8 = (\alpha^4)^2 = \alpha$. Le groupe de Galois est alors d'ordre 3 donc isomorphe à $\mathbf{Z}/3\mathbf{Z}$ et on peut voir qu'il est engendré par l'automorphisme qui envoie α sur α^2. En fait, on peut montrer qu'on a toujours

$$\mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p) \cong \mathbf{Z}/n\mathbf{Z}$$

engendré par le Frobenius $F : x \mapsto x^p$. En effet, les F^k avec $k \in \{0, \dots, n-1\}$ sont deux à deux disctincts et élémenst du groupe de Galois!

Passons à la détermination des polynômes $R_1, R2, R_3$. Dans ce cas, on a toujours $R_1 = P$ puisque P est le polynôme minimal de $x_1 = \alpha$ sur K. On cherche alors le polynôme minimal de $x_2 = \alpha^2$ sur $K(\alpha) = L$. Il s'agit de $T - \alpha^2$ et on constate alors que $R_2(X_1, X_2) = X_2 - X_1^2$ convient. Enfin, pour $x_3 = \alpha + \alpha^2$, on a $\mu_3(T) = T - \alpha - \alpha^2$ et $R_3(X_1, X_2, X_3) = X_3 - X_1 - X_1^2$ convient [11]. Par unicité, on a $I_P = (X_1^3 + X_1 + 1, X_2 - X_1^2, X_3 - X_1 - X_1^2)$. Noter qu'il est alors clair que

$$K[X_1, X_2, X_3]/(R_1, R_2, R_3) \cong K[X_1]/(P) \cong L$$

et on pourrait retrouver que le groupe de Galois est isomorphe à $\mathbf{Z}/3\mathbf{Z}$ engendré par le trois cycle (123).

(ii) C'est du cours que $L = K(\sqrt[3]{2}, j)$ et que l'extension L est galoisienne et $\mathrm{Gal}(L/K) \cong \mathfrak{S}_3$. On a à nouveau que pour $x_1 = \sqrt[3]{2}$, $R_1(X_1) = P(X_1)$. Puis, pour $x_2 = jx_1$, on cherche le polynôme minimal de x_2 sur $K(\sqrt[3]{2})$. Il s'agit évidemment de $(X - j\sqrt[3]{2})(X - \overline{j}\sqrt[3]{2}) = X^2 + \sqrt[3]{2}X + (\sqrt[3]{2})^2$. Il s'ensuit que $R_2(X_1, X_2) = X_2^2 + X_1X_2 + X_1^2$ convient (et est donc le seul par unicité). Enfin, le polynôme minimal de $x_3 = j^2\sqrt[3]{2} = -(1+j)\sqrt[3]{2}$ sur $K(x_1, x_2) = L$ est $T - j^2\sqrt[3]{2}$ de sorte que $R_3(X_1, X_2, X_3) = X_3 + X_2 + X_1$. Par complète symétrie, on pourrait retrouver le groupe de Galois $\mathfrak{S}_3$ en utilisant la définition du devoir!

(iii) On peut vérifier (par exemple par Eisenstain) que P est irréductible sur $\mathbf{Q}$ et donc L (son corps de décomposition sur K) est une extension galoisienne car on est en caractéristique 0. On peut déterminer ici les racines de P (qui est bicarré), à savoir

$$x_1 = \sqrt[4]{2}e^{i\frac{\pi}{8}}, \quad x_2 = -\sqrt[4]{2}e^{i\frac{\pi}{8}}, \quad x_3 = \sqrt[4]{2}e^{-i\frac{\pi}{8}}, \quad x_4 = -\sqrt[4]{2}e^{-i\frac{\pi}{8}}.$$

On constate que $x_1/x_2 = 1 + i$ donc $K(i)$ est une sous-extension galoisienne de L. Comme en TD, on dispose d'un élément d'ordre 2, à savoir la conjugaison complexe τ et d'un sous-groupe distingué $\mathrm{Gal}(L/K(i))$. Or L est d'ordre 8. En effet, on a $L = K(x_1, x_3) = K(x_1, \zeta_8)$ aved $\zeta_8 = e^{i\frac{\pi}{4}}$ une racine primitive 8-ème de l'unité de sorte que $x_3 = x_1\zeta_8$. et

$$[L : K] = [L : K(\zeta_8)][K(\zeta_8) : K) = 4[L : K(\zeta_8)].$$

Or, ζ_8 est annulé par $\Phi_8 = X^4 + 1$ irréductible sur K (noter qu'il s'agit du huitième polynôme cyclotomique). On a alors que $K(\zeta_8) = K(i, \sqrt{2})$ car ce sont deux extensions de même degré et $K(\zeta_8) \subseteq K(i, \sqrt{2})$ (on pouvait aussi raisonner par double inclusion). On a alors que $[L : K(\zeta_8)] > 1$ car sinon $L = K(\zeta_8) = K(i, \sqrt{2})$ mais alors $1 + i$ n'est pas un carré dans L qui serait de base $1, i, \sqrt{2}, i\sqrt{2}$ car alors

$$1 + i = (a + bi + c\sqrt{2} + di\sqrt{2})^2 = (a + c\sqrt{2})^2 - (b + d\sqrt{2})^2 + 2i\left(b + d\sqrt{2}\right)\left(a + c\sqrt{2}\right).$$

10. Car si $\alpha = \alpha^2$, alors $\alpha \in \{0, 1\}$ et si $\alpha^k = \alpha + \alpha^2$ pour $k \in \{0, 1\}$, alors $\alpha = 0$ ce qui est exclu. On pouvait aussi utiliser que sur un corps fini, comme on est parfait (l'automorphisme de Frobenius est un automorphisme car injectif en tant que morphisme de corps et bijectif par cardinalité), on est automatiquement séparable. Mais attention que cela n'est pas toujours le cas en caractéristique > 0.

11. Noter que $X_3 - X_1 - X_2$ ne convient pas car il ne respecte pas la condition sur le degré en X_2!

Cela implique $a^2+2c^2-b^2-2d^2=1$, $ac=bd$, $2(ba+2cd)=1$ et $ad=-bc$. On a donc $adc=bd^2$ puis $-bc^2=bd^2$ soit $b(c^2+d^2)=0$. On a donc un premier cas avec $b=0$ et donc soit $a=0$ auquel cas $cd=1/4$ et $c^2-d^2=1/2$ soit $1-16d^4=8d^2$ qui n'a pas de racine rationnelle. On a alors $b=0$ et $c=d=0$ et une contradiction avec $2(ab+2cd)=1$. On a donc nécessairement $b\neq 0$ et donc $c=d=0$ et $ba=1/2$ et $a^2-b^2=1$ soit $1-4b^4=4b^2$ qui n'a pas de racine rationnelle! Ainsi, le polynôme $X^2-(1+i)=X^2-1-\zeta_8^2$ est irréductible (car sans racine et de degré 2) sur $K(\zeta_8)$ et annule x_1 de sorte que $[L:K(\zeta_8)]=2$ et $[L:K]=8$. Comme on contient au moins deux extensions de degré 4, à savoir $K(\zeta_8)$ et $K(x_1)$ (qui sont bien disjointe car sinon $L=K(\zeta_8)=K(x_1)$ et on a une contradiction en terme de degré, cela correspond à des sous-groupes d'ordre 2 de $\mathrm{Gal}(L/K)$. Si l'on démontre que ce groupe n'est pas abélien, la classification des groupes d'ordre 8 fournira que $\mathrm{Gal}(L/k)\cong \mathbf{D}_4$. En fait, le seul sous-groupe de $\mathfrak{S}_4$ transitif est non abélien et isomorphe à $\mathbf{D}_4$!
On constate que $x_1x_3=\sqrt{2}$ si bien que $L=K(x_1,\sqrt{2})$ de degré 8. En effet, on a

$$[L:K]=[L:K(\sqrt{2})][K(\sqrt{2}):K]=2[L:K(\sqrt{2})].$$

Maintenant, on constate que $L=K(\sqrt{2})(x_1)$ et P annule x_1 et est irréductible[12] sur $K(\sqrt{2})$. On en déduit qu'il s'agit de son polynôme minimal sur $K(\sqrt{2})$ et par conséquent $[L:K(\sqrt{2})]=4$ et $[L:K]=8$ et une K-base de L est

$$\{1,\sqrt{2},x_1,\sqrt{2}x_1,x_1^2,\sqrt{2}x_1^2,x_1^3,\sqrt{2}x_1^3\}.$$

Tout élément de L s'écrit donc de manière unique comme une combinaison K-linéaire de ces éléments et donc un K-automorphisme de L est déterminé par son image de $\sqrt{2}$ (parmi $\pm\sqrt{2}$) et de x_1 (parmi les x_1,x_2,x_3,x_4). On a donc l'expression de nos huit éléments de $\mathrm{Gal}(L/K)$

$$\begin{array}{ccc}
\sigma & \sqrt{2} & x_1\\
\sigma_1=\mathrm{Id} & \sqrt{2} & x_1\\
\sigma_2 & \sqrt{2} & x_2\\
\sigma_3 & \sqrt{2} & x_3\\
\sigma_4 & \sqrt{2} & x_4\\
\sigma_5 & -\sqrt{2} & x_1\\
\sigma_6 & -\sqrt{2} & x_2\\
\sigma_7 & -\sqrt{2} & x_3\\
\sigma_8 & -\sqrt{2} & x_4
\end{array}$$

On peut alors vérifier que le groupe n'est pas abélien, que $\langle\sigma_7\rangle$ est d'ordre 4 distingué et d'intersection triviale avec $\langle\sigma_2\rangle$ d'ordre 2 de sorte qu'on retrouve le groupe diédral. Attention toutefois qu'ici contrairement au TD, si on considère $H=\mathrm{Gal}(L/K(\sqrt{2}))=\{\sigma_1,\sigma_2,\sigma_3,\sigma_4\}$, on a alors que $H\cong(\mathbf{Z}/2\mathbf{Z})^2$ et $N=\{\sigma_1,\sigma_5\}$, $\mathrm{Gal}(L/K)\cong H\rtimes N\cong(\mathbf{Z}/2\mathbf{Z})^2\rtimes\mathbf{Z}/2\mathbf{Z}$ qui est bien isomorphe au groupe diédral! On pouvait aussi faire appel au DM II de l'an dernier disponible sur Ecampus!
Passons alors à la détermination des R_i. Comme d'habitude, on a $R_1(X_1)=P(X_1)$ puis on a $K_1=K(x_1)$. On a alors $x_2=-x_1\in K_1$ de sorte que son polynôme minimal sur K_1 est $T-x_1$ et donc $R_2(X_1,X_2)=X_2+X_1$. Enfin, $K_2=K_1$ et $x_3=\sqrt{2}x_1^{-1}$ de sorte que $T^2-2x_1^{-2}$ annule x_3 à coefficients dans K_2. Mais

$$-x_1^4+2x_1^2=2\quad\text{soit}\quad 2x_1^{-2}=-x_1^2+2$$

et ainsi $T^2-2+x_1^2$ et $R_3(X_1,X_2,X_3)=X_3^2+X_1^2-2$. Enfin, $K_4=K_3=L$ et donc $R_4(X_1,X_2,X_3,X_4)=X_4+X_3$.

7. Il est clair que **(b)** implique **(a)** puisque si on se donne $\lambda_1,\dots,\lambda_r\in K$ tels que $\lambda_1y_1+\cdots+\lambda_ry_r=0$, alors pour tout $j\in\{1,\dots,N\}$, on a (puisque les coefficients sont dans K), $\lambda_1\sigma_j(y_1)+\cdots+\lambda_r\sigma_j(y_r)=0$ et par conséquent

$$\begin{pmatrix}\lambda_1\sigma_1(y_1)+\cdots+\lambda_r\sigma_1(y_r)\\ \lambda_1\sigma_2(y_1)+\cdots+\lambda_r\sigma_2(y_r)\\ \vdots\\ \lambda_1\sigma_N(y_1)+\cdots+\lambda_r\sigma_N(y_r)\end{pmatrix}=\begin{pmatrix}0\\0\\\vdots\\0\end{pmatrix}\quad\text{soit}\quad \lambda_1Gy_1+\cdots+\lambda_rGy_r=0$$

12. Il n'a pas de racines sur ce corps réels alors que toutes ses racines sont dans $\mathbf{C}\setminus\mathbf{R}$. Reste donc à voir qu'il ne se scinde pas comme produit de deux irréductibles de degré 2. Cela signifierait qu'il existe i et j tels que $(X-x_i)(X-x_j)$ est dans $K(\sqrt{2})$. On peut vérifier que

$$x_1x_2,\quad x_3x_4,\quad x_1+x_4,\quad x_2+x_3\in\mathbf{C}\setminus\mathbf{R}$$

et $x_1+x_3=-(x_2+x_4)=2\sqrt[4]{2}\cos\left(\frac{\pi}{8}\right)$ En effet, si

$$\sqrt[4]{2}\cos\left(\frac{\pi}{8}\right)=a+b\sqrt{2}\quad\text{alors}\quad\sqrt{2}\cos\left(\frac{\pi}{8}\right)^2=\frac{\sqrt{2}}{2}\left(1+\cos\left(\frac{\pi}{4}\right)\right)=a^2+2b^2+2ab\sqrt{2}$$

soit

$$\frac{\sqrt{2}}{2}+\frac{1}{2}=a^2+2b^2+2ab\sqrt{2}\quad\text{soit}\quad\begin{cases}a^2+2b^2=\frac{1}{2}\\ 4ab=1.\end{cases}$$

On aurait donc que b serait une solution rationnelle de $1+32b^4-8b^2=0$ mais on peut vérifier (comme en TD) que cette équation n'a aucune solution rationnelle!

avec les $\lambda_1, \dots, \lambda_r \in K \subseteq L$ donc $\lambda_1 = \cdots = \lambda_r = 0$.
Passons donc à la réciproque. Supposons **(a)** et supposons qu'il existe $\lambda_{i_1}, \dots, \lambda_{i_s} \in L$ tous non nuls tels que $\lambda_{i_1} G y_{i_1} + \cdots + \lambda_{i_s} G y_{i_s} = 0$ avec s minimal (où nécessairement $s \geqslant 2$ sinon un des y_i est nul et la famille n'est pas K-libre). On a alors en prenant l'image par $\sigma \in G$ que $\sigma(\lambda_{i_1})\sigma \circ \sigma_i(y_{i_1}) + \cdots + \sigma(\lambda_{i_s})\sigma \circ \sigma_i(y_{i_s}) = 0$ pour tout $i \in \{1, \dots, N\}$. Comme $\mu \mapsto \sigma \circ \mu$ est une bijection de G, on a $\sigma(\lambda_{i_1}) G y_{i_1} + \cdots + \sigma(\lambda_{i_s}) G y_{i_s} = 0$. On voit que s'il existe $\sigma \in G$ et i_j tel que $\sigma(\lambda_{i_j}) \neq \lambda_{i_j}$, alors on obtiendrait par soustraction une relation de dépendance de taille $s-1$ contredisant la minimalité de s. Ainsi, pour tout $\sigma \in G$ i_j, on a $\sigma(\lambda_{i_j}) = \lambda_{i_j}$ et $\lambda_{i_j} \in K$. On a donc par la première ligne de $\lambda_{i_1} G y_{i_1} + \cdots + \lambda_{i_s} G y_{i_s} = 0$ que $\lambda_{i_1} y_{i_1} + \cdots + \lambda_{i_s} y_{i_s} = 0$ et par **(a)**, on a $\lambda_{i_1} = \cdots = \lambda_{i_s} = 0$, ce qui est absurde ! On a donc bien obtenu **(b)** et l'équivalence !

8. Il est clair que R_i est dans $L[X_1, \dots, X_n]$ vérifiant **4.(i)** et **4.(ii)**. Par ailleurs, pour $\sigma \in G$, on a

$$R_i(\sigma(x_1), \dots, \sigma(x_i)) = \sigma(R(x_1, \dots, x_i)) = \sigma(\mu_i(x_i)) = 0$$

car σ est un morphisme de corps et R_i à coefficients dans K. Reste à voir qu'un polynôme S_i satisfaisant les conditions de la question satisfait aussi **4.(iii)** et est dans $K[X_1, \dots, X_i]$ et on aura $S_i = R_i$ par unicité dans la question **4.** On rappelle que les $x_1^{d_1-k_1} x_2^{d_2-k_2} \cdots x_i^{d_i-k_i}$ pour $1 \leqslant k_j \leqslant d_j$ forment une K-base de K_i (donc une famille K-libre). On a alors que $R_i - S_i$ peut se réécrire (les coefficients en $X_i^{d_i}$ s'annulant) comme combinaison linéaire de monômes du type $X_1^{d_1-k_1} X_2^{d_2-k_2} \cdots X_i^{d_i-k_i}$ pour $1 \leqslant k_j \leqslant d_j$. L'hypothèse que $R_i - S_i$ s'annule en tout les $(\sigma(x_1), \dots, \sigma(x_i))$ pour $\sigma \in G$ implique que l'on a une combinaison linéaire (à coefficients dans L puisque S_i est à coefficients dans L) annulant $G x_1^{d_1-k_1} x_2^{d_2-k_2} \cdots x_i^{d_i-k_i}$ pour $1 \leqslant k_j \leqslant d_j$. Par la question précédente, cette famille est libre et donc les coefficients de S_i et R_i sont les mêmes et $R_i = S_i$!

9. Soient σ et τ deux éléments de G tels que $\sigma G_i = \tau G_i$. On a donc $\mu \in G_i$ tel que $\sigma = \tau\mu$ et par définition, μ fixe K_i donc x_j ce qui implique bien que $\sigma(x_j) = \tau(\mu(x_j)) = \tau(x_j)$ et on a le résultat !

10. La première partie de la question provient de la question précédente et du fait que deux éléments dans la même classe ont la même restriction à K_{i-1}. Plus généralement

$$\left\{\tau(x_i) \ : \ \tau \in G, \ \tau_{|K_{i-1}} = \sigma_{|K_{i-1}}\right\}$$

ne dépend que de la classe de σ dans G/G_i. Montrons dans un premier temps que $\left\{\tau \ : \ \tau \in G, \ \tau_{|K_{i-1}} = \sigma_{|K_{i-1}}\right\} = \sigma G_{i-1}$. L'inclusion de droite à gauche est claire et pour l'inclusion réciproque, il est clair que $\sigma^{-1}\tau$ agit comme l'identité sur K_{i-1} donc est dans G_{i-1}. Par ailleurs, pour $\tau, \tau' \in \sigma G_{i-1}$, on a $\tau(x_i) = \tau'(x_i)$ si, et seulement si, $\tau_{|K_i} = \tau'_{|K_i}$ de sorte que $\tau G_i = \tau' G_i$. Il est alors clair que l'application

$$f : \begin{cases} \left\{\tau \ : \ \tau \in G, \ \tau_{|K_{i-1}} = \sigma_{|K_{i-1}}\right\} & \longrightarrow & \left\{\tau(x_i) \ : \ \tau \in G, \ \tau_{|K_{i-1}} = \sigma_{|K_{i-1}}\right\} \\ \tau & \longmapsto & \tau(x_i) \end{cases}$$

est surjective et chaque $f^{-1}(\tau(x_i))$ est de cardinal $\#G_i$. Il s'ensuit que par le lemme des bergers [13]

$$\#\left\{\tau(x_i) \ : \ \tau \in G, \ \tau_{|K_{i-1}} = \sigma_{|K_{i-1}}\right\} = \frac{\#G_{i-1}}{\#G_i}.$$

On a alors vu que $[K_i : K_{i-1}] = d_i$ de sorte que

$$\frac{\#G_{i-1}}{\#G_i} = \frac{[L : K_{i-1}]}{[K : K_i]} = [K_i : K_{i-1}] = d_i.$$

Finalement, $\#C_{\sigma,i} = d_i - 1$.

11. Vérifions que R_i satisfait les conditions de la question **8.** On a bien affaire à un polynôme de $L[X_1, \dots, X_i]$. Il est de degré (au vu du calcul du cardinal de $C_{\sigma,i}$) d_i et unitaire en X_i et de degré inférieur à $d_j - 1$ pour tout $1 \leqslant j \leqslant i-1$. Il reste donc à voir que ce polynôme s'annule en tout les $(\sigma(x_1), \dots, \sigma(x_i))$ pour tout $\sigma \in G$. Soit alors $\tau \in G$. On doit alors montrer que

$$\tau(x_i)^{d_i} - \sum_{[\tau] \in G/G_i} \tau(x_i)^{d_i} \left(\prod_{y_1 \in C_{\sigma,1}} \frac{\tau(x_1) - y_1}{\sigma(x_1) - y_1}\right) \cdots \left(\prod_{y_i \in C_{\sigma,i}} \frac{\tau(x_i) - y_i}{\sigma(x_i) - y_i}\right) = 0.$$

On constate que si $[\sigma] = [\tau]$, alors le terme obtenu est $\tau(x_i)^{d_i}$ tandis que si $[\sigma] \neq [\tau]$, alors il existe $j \in \{1, \dots, i\}$ tel que $\sigma(x_j) \neq \tau(x_j)$ car sinon $\sigma_{|K_i} = \tau_{|K_i}$ (car K_i est engendré par $x_1, \dots, x_i$) et $[\sigma] = [\tau]$. Il s'ensuit que

$$\left(\prod_{y_1 \in C_{\sigma,1}} \frac{\tau(x_1) - y_1}{\sigma(x_1) - y_1}\right) \cdots \left(\prod_{y_i \in C_{\sigma,i}} \frac{\tau(x_i) - y_i}{\sigma(x_i) - y_i}\right) = 0$$

13. Noter que $G_i \leqslant G_{i-1}$ de sorte qu'on obtient bien un entier !

et finalement

$$\tau(x_i)^{d_i} - \sum_{[\tau]\in G/G_i} \tau(x_i)^{d_i} \left(\prod_{y_1\in C_{\sigma,1}} \frac{\tau(x_1)-y_1}{\sigma(x_1)-y_1}\right)\cdots\left(\prod_{y_i\in C_{\sigma,i}} \frac{\tau(x_i)-y_i}{\sigma(x_i)-y_i}\right) = \tau(x_i)^{d_i} - \tau(x_i)^{d_i} = 0.$$

On a donc le résultat!

Reprenons alors un par un la question **6.** On a vu que le groupe de Galois est cyclique d'ordre 3 engendré par le Frobenius. On constate que R_1 est toujours unitaire de degré d_1 à coefficients dans K et annulant $x_1,\dots,x_n$ donc $R_1(X_1) = P$. On a en fait ici $L = K_1 = K_2 = K_3$ et $G_1 = G_2 = G_3 = \{\mathrm{Id}\}$. On retrouve ainsi laborieusement

$$R_1(X_1) = X_1^3 - \alpha^3\frac{(X_1-\alpha^2)(X_1-\alpha-\alpha^2)}{(\alpha-\alpha^2)\alpha^2} - \alpha^6\frac{(X_1-\alpha)(X_1-\alpha-\alpha^2)}{(\alpha^2-\alpha)\alpha} - (\alpha+\alpha^2)^3\frac{(X_1-\alpha)(X_1-\alpha^2)}{\alpha^3} = P_1(X_1)$$

soit en dévloppant et en utilisant $\alpha^3 = \alpha+1$ soit en utilisant ce qui précède. On a ensuite $d_2 = d_3 = 1$ et $C_{\sigma,i}$ est vide pour $i\in\{2,3\}$ et

$$\begin{aligned} R_2(X_1,X_2) &= X_2 - \alpha^2\frac{(X_1-\alpha^2)(X_1-\alpha-\alpha^2)}{(\alpha+\alpha^2)\alpha^2} - (\alpha+\alpha^2)\frac{(X_1-\alpha)(X_1-\alpha-\alpha^2)}{\alpha(\alpha+\alpha^2)} - \alpha\frac{(X_1-\alpha^2)(X_1-\alpha)}{\alpha^3} \\ &= X_2 - \left(\frac{1}{\alpha(1+\alpha)} + \frac{1}{\alpha} + \frac{1}{\alpha^2}\right)X_1^2 + \left(\frac{1}{1+\alpha} + \alpha + \alpha^2\right)X_1 - \left(\alpha^2+\alpha(1+\alpha)+\alpha\right) \\ &= X_2 - X_1^2 \end{aligned}$$

ce qui correspond bien au précédent résultat (ouf)! De même,

$$\begin{aligned} R_3(X_1,X_2,X_3) &= X_3 - (\alpha+\alpha^2)\frac{(X_1-\alpha^2)(X_1-\alpha-\alpha^2)}{(\alpha+\alpha^2)\alpha^2} - \alpha\frac{(X_1-\alpha)(X_1-\alpha-\alpha^2)}{\alpha(\alpha+\alpha^2)} - \alpha^2\frac{(X_1-\alpha^2)(X_1-\alpha)}{\alpha^3} \\ &= X_3 - \left(\frac{1}{\alpha(1+\alpha)} + \frac{1}{\alpha} + \frac{1}{\alpha^2}\right)X_1^2 + \left(\frac{1}{\alpha} + \frac{1}{\alpha^2} + \alpha + 1\right)X_1 - \left(\alpha^2+\alpha(1+\alpha)+\alpha\right) \\ &= X_2 - X_1^2 - X_1. \end{aligned}$$

On constate que les calculs pour les cas suivants deviennent vite affreux et donc cette formule d'interpolation ne semblent pas très maniables en pratique à la main mais qui est utile d'un point de vue informatique! Je vous renvoie à cet article dont le sujet est tiré de l'article de recherche (disponible sur Ecampus) *Explicit constructions in splitting fields of polynomials* de Mathias Lederer, 2003.