TD3 : Extensions normales et séparables

09/10/2023

Exercice 1 : Sous-groupes multiplicatifs d'un corps

Soit U un sous-groupe multiplicatif fini d'un corps K. On veut montrer que G est cyclique.

1. Soit $(G,+)$ un groupe abélien de torsion, montrer que $G = \bigoplus_{p\in\mathcal{P}} G(p)$ où $G(p)$ est le sous-groupe des éléments de G dont l'ordre est une puissance de p.

2. En déduire qu'il suffit de montrer que $U(p)$ est cyclique.

3. Conclure.

Correction :

1. On considère le morphisme évident $\varphi : \bigoplus_p G(p) \to G$. Soit $x \in \ker\varphi$, alors pour tout q, $x_q = \sum_{p\neq q} -x_p$ (où la somme est finie, presque tous les x_p sont l'élément neutre de G). On en déduit que l'ordre de x_q divise le ppcm des ordre des x_p, mais par définition c'est une puissance de q. Finalement, l'ordre de x_q est 1 et $x_q = 0$, d'où l'injectivité.

Pour tout n, on note $A_n = \ker(m_n : x \mapsto nx)$. Alors on montre que si $n = pq$ avec $p \wedge q = 1$, alors $A_n = A_p + A_q$. En effet, $up + vq = 1$, donc tout $x \in G$ s'écrit $x = upx + vqx$ ce qui prouve le résultat, car G est de torsion.

2. Oui car les ordres sont premiers entre eux, par théorème chinois.

3. Soit a un élément de $U(p)$ d'ordre p^r maximal, de sorte que tout élément de $U(p)$ soit racine de $X^{p^r} - 1$, et donc $U(p)$ est d'ordre au plus p^r, or $\langle a\rangle$ est aussi d'ordre p^r, donc a génère $U(p)$.

Exercice 2 : Une infinité d'extensions intermédiaires

Soit p un nombre premier, on considère l'extension $\mathbb{F}_p(X,Y)/\mathbb{F}_p(X^p,Y^p)$.

1. Déterminer le degré de cette extension.

2. Trouver une infinité de corps intermédiaires pour cette extension.

3. Montrer que cette extension n'est ni séparable ni monogène.

Correction :

1. On montre que $[\mathbb{F}_p(X,Y) : \mathbb{F}_p(X^p,Y^p)] = p^2$. Par exemple X est racine de $T^p - X^p \in \mathbb{F}_p(X^p,Y^p)[T]$ et Y est racine de $T^p - Y^p \in \mathbb{F}_p(X,Y^p)[T]$ donc par multiplicativité des degrés, on obtient $[\mathbb{F}_p(X,Y) : \mathbb{F}_p(X^p,Y^p)] \leqslant p^2$ (on peut montrer que ces polynômes sont irréductibles, car on connait en fait toutes leurs racines, mais on propose une autre méthode), et la famille $(X^iY^j)_{0\leqslant i,j<p}$ est $\mathbb{F}_p(X^p,Y^p)$-libre. En effet, si on se donne une relation de liaison

$$\sum_{0\leqslant i,j<p} \frac{f_{i,j}(X^p,Y^p)}{g_{i,j}(X^p,Y^p)} X^iY^j = 0$$

Alors quitte à multiplier par les $g_{i,j}$ on obtient une relation de la forme

$$P(X,Y) = \sum_{0\leqslant i,j<p} \tilde{f}_{i,j}(X^p,Y^p)X^iY^j = 0$$

Or le coefficient en $(X^p)^a(Y^p)^b$ de $\tilde{f}_{i,j}$ est exactement le coefficient en $X^{ap+i}Y^{ap+j}$ de P qui est le polynôme nul, donc en fait tous les $\tilde{f}_{i,j}$ sont nuls, puis les $f_{i,j}$ aussi. D'où l'autre inégalité sur le degré (de même on peut montrer que la famille en question est génératrice)..

2. On peut prendre les $\mathbb{F}_p(X^p,Y^p)(X + X^{pk}Y)$ pour $k \geqslant 1$. Ces extensions sont de degré p sur $\mathbb{F}_p(X^p,Y^p)$ car $(X + X^{pk}Y)^p \in \mathbb{F}_p(X^p,Y^p)$, et $(X + X^{pk}Y) \notin \mathbb{F}_p(X^p,Y^p)$ (sinon on aurait deux polynômes

P, Q tels que $P(X^p, Y^p)(X + X^{pk}Y) = Q(X^p, Y^p)$ ce qui est absurde en regardant le coefficient (en tant qu'élément de $\mathbb{F}_p[X]$ en Y^{np+1}). Aussi, deux tels sous-corps ne sont pas égaux puisque si $i \neq j, X + X^{pi}Y$ et $X + X^{pj}Y$ engendrent $\mathbb{F}_p(X, Y)$ sur $\mathbb{F}_p(X^p, Y^p)$:

$$Y = (X^{pi} - X^{pj})^{-1}((X + X^{pi})Y) - (X + X^{pj}Y))$$

Exercice 3 : Théorème de l'élément primitf

1. Soit K une extension finie séparable de k de degré n. Soit $\overline{K}$ une cloture algébrique de K. On veut montrer que $K = k(x)$.

a. Conclure si k est fini.

On suppose maintenant que k est infini et on note $\mathrm{Hom}_k(K, \overline{K}) = \{\sigma_1, \dots, \sigma_n\}$.

b. Montrer qu'il existe $x \in K$ tel que pour $i \neq j, \sigma_i(x) \neq \sigma_j(x)$.

c. Conclure.

2. Soit L/K une extension finie. Montrer que L/K admet un nombre fini d'extensions interdmédiaires si et seulement si L/K est monogène.

Correction :

1.

a. Oui par l'exercice 1, on choisit x un générateur de $K^\times$ (K étant bien un corps fini car extension finie d'un corps k fini).

b. On remarque que c'est l'hypothèse de séparabilité qui permet d'écrire $\mathrm{Hom}_k(K, \overline{K}) = \{\sigma_1, \dots, \sigma_n\}$ avec $n = [K : k]$.

On pose, pour $i \neq j$, le k-espace vectoriel $E_{i,j} := \{x \in K, \sigma_i(x) = \sigma_j(x)\}$. Alors $\forall i \neq j$, $E_{i,j} \neq K$ sinon $\sigma_i = \sigma_j$. De plus, pour un corps infini, on sait qu'une réunion finie de sous-espaces vectoriels stricts ne peut pas être l'espace vectoriel tout entier. Prouvons ce fait :

Soit E un k-espace vectoriel, supposons $E = \bigcup_{i=1\dots m} V_i$ avec V_i propre. Quitte à le retirer, on peut suppose $V_1 \notin \bigcup_{i \geqslant 2} V_i$, et on peut alors trouver $x \in V_1 \backslash \bigcup_{i \geqslant 2} V_i$ et $y \in \bigcup_{i \geqslant 2} V_i \backslash V_1$. Pour tout $\lambda \in k$, $y + \lambda x \in E$ mais pas dans V_1 sinon $y \in V_1$. Il existe donc $i_\lambda \in \{2, \dots, m\}$ tel que $y + \lambda x \in V_{i_\lambda}$. Comme k est infini, on a $y + \lambda_1 x$et $y + \lambda_2 x$ qui sont dans le même V_i avec $\lambda_1 \neq \lambda_2$, donc $x \in V_i$, absurde.

On en déduit que $\bigcup_{i \neq j} E_{i,j} \neq K$ et cela permet de conclure.

c. Soit x comme dans la question précédente, alors $\mathrm{Hom}_k(k(x), \overline{k})$ contient au moins n éléments $\sigma_1, \dots, \sigma_n$ qui sont bien deux à deux distincts. En particulier, cela implique $n \leqslant [k(x) : k]_s \leqslant [k(x) : k]$ donc $k(x) = K$.

Exercice 4 : Extensions séparables et degré

1. Soit K un corps de caractérisque p, montrer que le Frobenius $\mathrm{Fr} : x \mapsto x^p$ est bien un morphisme de corps.

Soit $F \subset E$ une extension finie de corps de caractéristique $p > 0$.

2.

a. Montrer qu'un élément $x \in E$ est séparable si et seulement si on a $F(x) = F(x^p)$.

b. Montrer l'équivalence des assertions suivantes :

(i) Il existe une base $(x_1, \dots, x_n)$ de E sur F telle que $(x_1^p, \dots, x_n^p)$ est aussi une base de E sur F.

(ii) Pour toute base $(x_1, \dots, x_n)$ de E sur F, $(x_1^p, \dots, x_n^p)$ est aussi une base de E sur F.

c. Montrer que ces assertions sont vraies si et seulement si l'extension E/F est séparable.

Correction :

1. Cela vient du fait que p divise $\binom{p}{k} = \frac{p}{k}\binom{p-1}{k-1}$ pour $k = 1 \dots p-1$.

2.

a. Supposons x séparable sur F. Alors le polynôme $P(X) = X^p - x^p \in F(x^p)[X]$,n'est pas irréductible, sinon P serait le polynôme minimal de x, mais n'est pas séparable, ce qui est absurde par hypothèse sur x. Alors $P(X) = (X - x)^p$ se factorise sur $F(x^p)[X]$ en $f(X)g(Y)$, et on peut supposer $f(X) = (X - x)^k$ avec $k \in \{1, \dots, p-1\}$. Mais alors en regardant le coefficient de degré $k-1$ de f, on voit que $kx \in F(x^p)$, et comme $k \neq 0$, $x \in F(x^p)$. D'où $F(x^p) = F(x)$ (l'autre inclusion étant toujours vraie).

Réciproquement, si $F(x) = F(x^p)$, alors $x = Q(x^p)$ avec $Q \in F[X]$. Alors x est racine de $Q(X^p) - X$, qui est un polynôme séparable, et x est bien séparable sur F.

b. L'implication $\Leftarrow$ est évidente (car une base existe). Montrons donc $\Rightarrow$:

Soit $(x_i)_{i=1,\dots,n}$ une base telle que (x_i^p) est aussi une base. Soit $(y_i)_{i=1,\dots,n}$ une autre base. Soit $P \in \mathrm{GL}_n(F)$ telle que

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

Alors, en appliquant le Frobenius coefficient par coefficient, on obtient la relation matricielle :

$$\begin{pmatrix} y_1^p \\ \vdots \\ y_n^p \end{pmatrix} = \mathrm{Fr}(P) \begin{pmatrix} x_1^p \\ \vdots \\ x_n^p \end{pmatrix}$$

Or comme $\det(\mathrm{Fr}(P)) = \mathrm{Fr}(\det(P))$ par propriété de morphisme, on voit que $\mathrm{Fr}(P) \in \mathrm{GL}_n(F)$, ce qui conclut.

c. Supposons que les assertions sont vraies. Montrons que l'extension E/F est séparable. Soit $x \in E$. Notons $n = [F(x) : F]$, de sorte que $(x^i)_{i=0,\dots,n-1}$ soit une base de $F(x)/F$, et en choisissant (t_j) une base de $E/F(x)$ avec $t_1 = 1$, on sait d'après le cours que $(x^i t_j)$ est une base de E/F. Alors $((x^i)^p t_j^p)i, j$ est aussi une base par hypothèse, en particulier $((x^p)^i)_{i=0,\dots,n-1}$ est une famille F-libre de $F(x^p)$, donc $[F(x^p) : F] \geqslant n = [F(x) : F]$. Comme on a de plus $F(x) \supset F(x^p)$, on en dédduit l'égalité, puis le fait que x est séparable par question 2.a .

Réciproquement, si E/F est séparable, par théorème de l'élément primitif il existe x tel que $F(x) = E$, puis par séparablilité $F(x^p) = F(x) = E$. Alors la base $(1, x, \dots, x^{n-1})$ avec $n = [E : F]$ est une base qui vérifie l'assertion (i) de la question 2.b.

Exercice 5 :

Soit K un corps algébriquement clos. Montrer que K est infini.

Correction :

Si $|K| = n < \infty$, alors tout élément est racine de $X^n - X$, et donc le polynôme $X^n - X + 1$ n'a pas de racine.

Exercice 6 : Première preuve du Théorème de Steinitz

1. (Existence d'une clôture algébrique) On note $\mathcal{E}$ l'ensemble des polynômes irréductibles sur $K[X]$. Par le théorème de Zermelo (équivalent à Zorn), on choisit un bon ordre $\prec$ sur $\mathcal{E}$.

a. Montrer que le principe d'induction fonctionne, c'est à dire que si on a montré l'assertion "pour $P \in \mathcal{E}$, si pour tout $Q \prec P$, $\mathcal{P}(Q)$ est vraie, alors $\mathcal{P}(P)$ est vraie." alors $\mathcal{P}$ est vraie pour tout $P \in \mathcal{E}$.

b. Montrer qu'il existe une famille $j_P : K \to \Omega_P$ d'extensions algébriques où P est scindé, et de K-morphismes $j_P^Q : \Omega_Q \to \Omega_P$ pour $Q \prec P$, vérifiant $j_P = j_P^Q \circ j_Q$.

c. Montrer qu'il existe $j : K \to \Omega$ extension algébrique telle que tous les $P \in \mathcal{E}$ sont scindés sur Ω.

d. Conclure que Ω est une clôture algébrique de K.

2. (Unicité) Soit $K \to \Omega'$ une autre clôture algébrique de K.

a. Construire des K-morphismes $\alpha_P : \Omega_P \to \Omega'$ tels que $\alpha_P \circ j_P^Q = \alpha_Q$ pour $Q \prec P$.
b. En déduire qu'on a un K-morphisme injectif $\alpha : \Omega \to \Omega'$.
c. Conclure en montrant que α est surjectif.

Correction :

1.

a. Soit $A = \{P \in \mathcal{E}, \mathcal{P}(P) \text{ est fausse}\}$, et supposons par l'absurde que A est non vide. Alors A est une partie non vide de $\mathcal{E}$, qui par hypothèse est bien ordonné, donc A possède un élément minimal P pour $\prec$. Mais alors P vérifie l'hypothèse d'induction par minimalité, donc $\mathcal{P}$ est vraie, ce qui est absurde.

b. On montre par induction la propriété $\mathcal{P}(P)$: "Pour tout $Q \preceq P$, il existe une extension algébrique $j_Q : K \to \Omega_Q$ où Q est scindé, et des K-morphismes $j_P^Q : \Omega_Q \to \Omega_P$ pour $Q \prec P$, vérifiant $j_P = j_P^Q \circ j_Q$. De plus pour $R \prec Q \prec P, j_P^R = j_P^Q \circ j_Q^R$"

Supposons que $\mathcal{P}$ soit vrai pour tous les $Q \prec P$. Si P est minimal dans $\mathcal{E}$, un corps de décomposition de P convient. Sinon, on pose $K' = \bigcup_{Q \prec P} \Omega_Q$ qui est bien un corps, en le voyant comme une union croissante de corps viales inclusions $\Omega_Q \to \Omega_{Q'}$ pour $Q \prec Q'$. Pour être rigoureux, car on ne peut techniquement pas voir tous les Ω_P dans un même ensemble et considérer seulement une union, on pose

$$\Omega_{\prec P} := \bigsqcup_{Q \prec P} \Omega_Q / \sim$$

où pour $x \in \Omega_Q$, $y \in \Omega_{Q'}$, $x \sim y$ ssi il existe $Q, Q' \prec R$ tel que $j_R^Q(x) = j_R^{Q'}(y)$ (on peut remarquer que pour cette construction, on n'a besoin que l'ordre soit dirigé, ou ordonné filtrant, c'est à dire que pour tout Q, Q', il existe R plus grand pour l'ordre $\prec$ que Q et Q')

Alors K est bien un corps pour les opérations pour $x \in \Omega_Q$ et $y \in \Omega_{Q'}$ définies par $[x] + [y] := j_R^Q(x) + j_R^{Q'}(y)$ et $[x] \times [y] = j_R^Q(x) \times j_R^{Q'}(y)$ (en vérifiant que tout passe bien au quotient), et on a les inclusions évidentes $j_{\prec P}^Q : \Omega_Q \to \Omega_{\prec P}$ définies par la composition de $\Omega_Q \to \bigsqcup_{Q \prec P} \Omega_Q$ et de l'application canonique de passage au quotient. On remarque de plus que $\Omega_{\prec P}/K$ est algébrique : tout $x \in \Omega_{\prec P}$ est dans un Ω_Q, donc est algébrique car l'extension Ω_Q est algébrique par hypothèse d'induction. On appelle $\Omega_{\prec P}$ une *limite inductive* du diagramme $((\Omega_Q)_{Q \prec P}, , j_Q, j_{Q'}^Q)$.

Soit alors Ω_P le corps de décomposition de $P \in \Omega_{\prec P}[X]$, et on fixe $i : \Omega_{\prec P} \to \Omega_P$. On a clairement $j_P : K \to \Omega_P$ par composition de $K \to \Omega_{\prec P} \xrightarrow{i} \Omega_P$. Alors $\Omega_P/\Omega_{\prec P}$ est algébrique donc Ω_P/K est algébrique, de plus pour $Q \prec P$, on a les K-morphismes $\Omega_Q \xrightarrow{j_{K'}^Q} \Omega_{\prec P} \to \Omega_P$, que l'on nomme j_P^Q. On remarque enfin que pour $R \prec Q \prec P$, le diagramme suivant commute :

$$\begin{tikzcd}
\Omega_R \arrow[rr, "j_P^R"'] \arrow[dr, "j_Q^R"'] & & \Omega_P \\
& \Omega_Q \arrow[ur, "j_P^Q"'] &
\end{tikzcd}$$

car le diagramme

$$\begin{tikzcd}
\Omega_R \arrow[rr, "j_{\prec P}^R"'] \arrow[dr, "j_Q^R"'] & & \Omega_{\prec P} \\
& \Omega_Q \arrow[ur, "j_{\prec P}^Q"'] &
\end{tikzcd}$$

commute par définition de $\Omega_{\prec P}$ comme union croissante des Ω_Q, dans lesquels les recollements marchent bien. De même $j_P = j_P^Q \circ j_Q$.

c. On construit comme précédemment la limite inductive Ω du diagramme $((\Omega_P)_{P\in\mathcal{E}}, j_P, j_P^Q)$, et ce corps convient, en effet on a pour tout P des K-morphsimes $j^P : \Omega_P \to \Omega$ permettant de voir Ω comme une extension de Ω_P, sur lequel P est scindé.

d. même preuve que question 1 de l'exercice 9.

2. Remarque : ici les Ω_P sont fixés et obtenus par la question précédente.

a. On montre cela par induction : si on a des $\alpha_Q : \Omega_Q \to \Omega'$ pour tout $Q \prec P$, on peut définir $\alpha_{\prec P} : \Omega_{\prec} P \to \Omega'$ par propriété/définition de la limite inductive (on peut vérifier que ça marche avec la définition précise donnée, mais il faut y penser comme si c'était une vraie union croissante de corps). Comme Ω' est une clôture algébrique, on peut prolonger $\alpha_{\prec P}$ en $\alpha_P : \Omega_P \to \Omega'$ par un théorème du cours. La relation $\alpha_P \circ j_Q^P = \alpha_Q$ est vraie par définition de la limite inductive (les recollements se font selon j_Q^P).

b. même preuve que précédement, car Ω est la limite inductive des $(\Omega_P)_{P\in\mathcal{E}}$, et l'adjectif "injectif" est un pléonasme.

c. Si $x \in \Omega'$, par algébricité de Ω' alors x est racine d'un certain $P \in K[X]$, or $P = \prod_i (X - a_i)$ dans Ω. Alors $P = P^\alpha = \prod_i (X - \alpha(a_i))$ (la première égalité venant du fait que P est défini sur K) donc il existe un i tel que $\alpha(a_i) = x$, ce qui donne la surjectivité et conclut la preuve de l'unicité.

Exercice 7 : Extensions finie non normale ni séparable

Montrer que l'extension $\mathbb{F}_2(t^{1/6})/\mathbb{F}_2(t)$ n'est ni séparable ni normale.

Correction :

Exercice 8 : Un exemple

Soit $K = \mathbb{Q}(\sqrt[3]{2}, j)$ où $j = e^{2i\pi/3}$.

1. Déterminer $[K : \mathbb{Q}]$, et exprimer K comme corps de décomposition d'un polynôme bien choisi.

2. Déterminer tous les sous-corps de K ainsi que leur degré.

Correction :

1. Comme $[\mathbb{Q}(j) : \mathbb{Q}] = 2$ et $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3]$ on a $[K : \mathbb{Q}] = 6$. Si $P = X^3 - 2$ alors K contient un corps de décomposition de P. Comme les racines de P sont $\sqrt[3]{2}, j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$ un corps de décomposition de P contient toujours $\sqrt[3]{2}$ et $j = \frac{j\sqrt[3]{2}}{\sqrt[3]{2}}$ donc K est un corps de décomposition de P.

2. Un sous corps de K est de degré $1, 2, 3$ ou 6. Les cas 6 et 1, sont triviaux. On montre que si L est un sous corps de K de degré 3 alors $L = \mathbb{Q}(j^i\sqrt[3]{2})$ pour un $i = 0, 1, 2$ et que si L est de degré 2 alors $L = \mathbb{Q}(j)$.

On regarde les automorphismes de K, ils sont déterminés sur j et $\sqrt[3]{2}$ et donc il ne peut avoir qu'au plus 6. Il y en a exactement 6 et le groupe des automorphismes de K est isomorphe à S_3 le groupe de permutation de trois éléments, agissant sur $\{\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}\}$ le 3-cycle correspond à la multiplication par j et la transposition est engendrée par $j \mapsto j^2$.

Supposons tout d'abord que $[L : \mathbb{Q}] = 2$, alors on a $L = \mathbb{Q}(\alpha)$ avec $\alpha^2 \in \mathbb{Q}$. Et on a donc un automorphisme $c_\alpha : L \to L, \alpha \mapsto -\alpha$, de plus on a $K = L(\sqrt[3]{2})$. La composée $L \xrightarrow{c_\alpha} L \to K$ s'étend en un morphisme $K \to K$ (cela revient à choisir une racine cubique de 2 et on en a déjà choisi une dans la définition de K). On obtient donc un automorphisme de K, celui-ci est d'ordre 2. Pour conclure il suffit de montrer que L est invariant par le 3-cycle, supposons que ce n'est pas le cas. Notons $\tau : K \to K$ le 3-cycle, si $\tau(L) \neq L$ alors $\tau(L) = \mathbb{Q}[\tau(\alpha)]$ et comme précédemment on construit un automorphisme de K qui est déterminé par $\tau(\alpha) \mapsto -\tau(\alpha)$. On obtient alors trois automorphismes et on peut prescrire que chacun d'entre eux envoie $\sqrt[3]{2}$ sur lui même. Alors ces trois automorphismes sont égaux et donc c_α commute à l'action de τ ce qui est impossible dans S_3.

Supposons dans un deuxième cas que $[L : \mathbb{Q}] = 3$ alors $[K : L] = 2$ et on a un automorphisme L-linéaire de K d'ordre 2 et L s'identifie au points fixes de K sous cet automorphisme. Avec la connaissances du groupe des automorphismes et de leurs points fixes on gagne.

Exercice 9 : Deuxième preuve du Théorème de Steinitz

1. Soit $K \subset L$ une extension algébrique. On suppose que tout polynôme de $K[X]$ est scindé dans L. Montrer que L est une clôture algébrique de K.

2. On note $\mathcal{P}$ l'ensemble des polynômes unitaires de $K[X]$; à chaque polynôme $P \in \mathcal{P}$ on associe des indéterminées $\{X_{P,i}\}_{0 \leqslant i \leqslant deg(P)}$ et on considère la K-algèbre $A := K[X_{P,i}, P \in \mathcal{P}, 0 \leqslant i \leqslant deg(P)]$.

Pour $P \in \mathcal{P}$ de degré n, on note $a_{P,0}, \ldots, a_{P,n} \in A$ les coefficients du polynôme

$$P(T) - \prod_{i=1}^{n}(T - X_{P,i}) \in A[T].$$

On considère alors I l'idéal de A engendré par tous les $a_{P,i}$ lorsque P parcourt $\mathcal{P}$ et $0 \leqslant i \leqslant deg(P)$.

a. Montrer que I est un idéal propre de A.

b. Conclure.

Correction :

1. Si $P \in L[X]$ est un polynôme non nul irréductible, soit $L' = L[X]/P$ un corps de rupture de P, alors $x \in L'$ est algébrique sur L et si $a_1, \ldots, a_n$ sont les coefficients de P, x est algébrique sur $K(a_1, \ldots, a_n)$ donc en particulier x est algébrique sur K. Comme P est son polynôme minimal sur L, $P|Q$ où Q désigne le polynôme minimal de x sur K, mais par hypothèse Q est scindé donc P aussi. Comme P est irréductible, il est de dimension 1.

2.a. Supposons par l'absurde que I n'est pas un idéal propre, alors il existe une somme finie $\sum_i b_i a_{P_i,j_i} = 1$ pour les b_i sont des éléments de A. Il n'y a qu'un nombre fini de P_i qui interviennent, fixons une extensions L/K qui est un corps de décomposition de tous les P_i. Définissons maintenant un morphisme $A \to L$ donné par $X_{P,j} \mapsto 0$ si P n'est pas l'un des P_i et $x_{P_i,j}$ si $P = P_i$ et $x_{P_i,j}$ est la $j$ième racine de P_i dans L (pour un choix d'un ordre quelconque des racines). Le morphisme induit $A[T] \to L[T]$ envoie $P_i(T) - \prod_i (T - X_{P,i})$ sur le polynôme nul et donc a_{P_i,j_i} est envoyé sur 0. En regardant l'image de la somme $\sum_i b_i a_{P_i,j_i} = 1$ on obtient $0 = 1$ ce qui est absurde, ainsi I est bien un idéal propre.

2.b Comme I est un idéal propre, il est contenu dans un idéal maximal m, le quotient $L = A/m$ est une extension de K et on a des égalités $P(T) = \prod_i (T - x_{P,i})$ où $x_{P,i}$ désigne l'image de x_i et donc tout polynôme de $K[T]$ est scindé dans L. D'autre part cette extension est engendrée par les $x_{P,i}$ qui sont donc tous algébriques. Il suit que L/K est une extension algébrique et par 1. c'est une clôture algébrique de K.

Exercice 10 : Troisème preuve du théorème de Steinitz

Soit K un corps, on note $A = \{\omega_{f,i}, f \in K[X], i = 1, \ldots, \deg f\}$ où $\omega_{f,i}$ sont les zéros de f dans un corps de décomposition. Soit Ω un ensemble de cardinal strictement plus grand que A, qui contient K. On va regarder les extensions de K dont les éléments sont des éléments de Ω

1. Montrer que si L est une extension algébrique de K, alors il existe $L' \subset \Omega$ (l'inclusion est juste ensembliste) tel que $L' \simeq L$.

2. En considérant $S = \{E_j \subset \Omega\}$, où E_j est une extension algébrique de K dont les éléments sont dans Ω, muni de l'inclusion ensembliste, montrer que S possède un élément maximal.

3. Conclure.

Correction :

Voir par exemple 31.22 dans " A First Course in Abstract Algebra" de John B Fraleigh

Exercice 11 : Quatrième preuve du théorème de Steinitz

1. (Un lemme utile) Soit Ω un corps algébriquement clos, et K un sous corps. Montrer que $\overline{K}$ l'ensemble des éléments de Ω algébriques sur K est une clôture algébrique de K.

2. Pour $f \in K[X]\backslash K$, on considère une indéterminée X_f, et $A = \mathbb{K}[X_f]_{f \in K[X]\backslash K}$. On pose $I = (f(X_f))_{f \in K[X]\backslash K}$. Montrer que I est un idéal propre.

3. En déduire qu'il existe $\Omega_1 \supset K$ une extension de corps telle que tout polynôme de $K[X]$ possède une racine dans Ω_1.

4. Conclure

Correction :

Voir `https://www-fourier.ujf-grenoble.fr/~eherscov/MAT4111/ThmSteinitz.pdf`