THÉORIE DE GALOIS I - CORRIGÉ

Exercice 1 — 1. Par définition même, $S(f)$ est un élément du corps fini K.

Considérons tout d'abord le cas d'une variable ($n = 1$).
- On a $S(1) = q = 0$.
- Le groupe multiplicatif $K^\times$ étant cyclique, il existe $\zeta \in K^\times$ tel que

$$S(T^\nu) = \sum_{x\in K} x^\nu = \sum_{x\in K^\times} x^\nu = \sum_{0\le i\le q-2} \zeta^{\nu i}$$

pour tout entier naturel $\nu \geq 1$; on a donc

$$S(T^\nu) = \begin{cases} \frac{1-\zeta^{\nu(q-1)}}{1-\zeta^\nu} = 0 & \text{si } q-1 \nmid \nu \\ q-1 = -1 & \text{si } q-1 | \nu. \end{cases}$$

Le cas général s'en déduit immédiatement :

$$\begin{aligned} S(T_1^{\nu_1}\dots T_n^{\nu_n}) = \sum_{\mathbf{x}\in K^n} x_1^{\nu_1}\dots x_n^{\nu_n} = \left(\sum_{x_1\in K} x_1^{\nu_1}\right)\dots\left(\sum_{x_n\in K} x_n^{\nu_n}\right) &= S(T^{\nu_1})\dots S(T^{\nu_n}) \\ &= \begin{cases} (-1)^n & \text{si } \nu_i > 0 \text{ et } q-1|\nu_i \text{ pour tout } i \\ 0 & \text{sinon.} \end{cases} \end{aligned}$$

2. Quel que soit $\mathbf{x} \in K^n$,

$$f(\mathbf{x}) = \begin{cases} 0 & \text{si } \mathbf{x} \notin V \\ 1 & \text{si } \mathbf{x} \in V \end{cases}$$

et donc $S(f) = \mathrm{Card}(V)$.

D'autre part, l'hypothèse sur les degrés des polynômes f_i fournit l'inégalité

$$\deg(f) \le \sum_{1\le i\le m} (q-1)\deg(f_i) < (q-1)n$$

et donc, si l'on écrit f sous la forme $\sum_{\nu\in\mathbb{N}^n} a_\nu T^\nu$, $a_\nu = 0$ pour tout multi-indice ν tel que, pour tout i, $\nu_i > 0$ et $q-1|\nu_i$; vu la première question, ceci implique $S(f) = 0$. Nous obtenons ainsi la congruence $\mathrm{Card}(V) \equiv 0 \pmod{p}$.

Si les polynômes f_i sont sans termes constants, $\mathbf{0}$ est un zéro commun et V est donc non vide. On a alors $\mathrm{Card}(V) \geq 2$ en vertu de ce qui précède, ce qui établit l'existence d'un point $\mathbf{x}$ de $K^n - \{\mathbf{0}\}$ dans V. En particulier : si $f_1,\dots,f_m$ sont des polynômes *homogènes* non constants tels que $\deg(f_1)+\dots+\deg(f_m) < n$, ils possèdent un zéro commun non trivial dans K^n (ou de manière équivalente, le sous-ensemble de l'espace projectif $\mathbb{P}^n(K)$ défini par l'annulation simultanée des f_i est *non vide*).

Exercice 2 — 1. Les polynômes cyclotomiques $\Phi_d \in \mathbb{Z}[T]$ sont irréductibles [(1)] et

$$T^n - 1 = \prod_{d|n} \Phi_d$$

pour tout entier naturel $n \geq 1$. Dans tout ce qui suit, nous travaillons avec les réductions modulo p des polynômes cyclotomiques et allons étudier leur réductibilité sur les extensions finies de $\mathbb{F}_p$.

Étant donné un entier $n \geq 2$ premier à p, le polynôme $T^n - 1$ de $\mathbb{F}_p[T]$ est séparable sur $\mathbb{F}_p$ puisqu'il est premier à son polynôme dérivé $nT^{n-1} \neq 0$ dans $\mathbb{F}^p[T]$; il possède donc n racines distinctes dans une clôture algébrique de $\mathbb{F}_p$ et les polynômes cyclotomiques Φ_d et $\Phi_{d'}$ associés à des diviseurs *distincts* d et d' de N sont par conséquent premiers entre eux dans $\mathbb{F}_p[T]$.

[(1)] Voir l'exercice 2 de la fiche *Théorie de Galois II*

Vu l'identité $T^{p^r n} - 1 = (T^n - 1)^{p^r}$ dans $\mathbb{F}_p[T]$, les polynômes $\Phi_{p^i d}$ et Φ_d ont les mêmes racines dans une clôture algébrique de $\mathbb{F}_p$ pour tout d divisant n et tous deux sont par conséquent premiers aux polynômes $\Phi_{p^j d'}$ lorsque d' est un diviseur de n distinct de d. Vu cette observation, l'identité

$$\left(\prod_{d|n} \Phi_d\right)^{p^r} = \prod_{\delta | p^r n} \Phi_\delta = \prod_{d|n} \left(\prod_{i=0}^{r} \Phi_{p^i d}\right)$$

implique

$$\prod_{i=0}^{r} \Phi_{p^i d} = \Phi_d^{p^r}$$

pour tout diviseur d de n, d'où l'on tire $\Phi_{p^i d} = \Phi_d^{p^{i-1}(p-1)}$ pour tout $i \in \{1, \ldots, r\}$ grâce à un raisonnement par récurrence élémentaire :

- comme $\Phi_{pd}\Phi_d = \Phi_d^p$ (faire $r = 1$), $\Phi_{pd} = \Phi_d^{p-1}$ et l'assertion est établie pour $i = 1$;
- si $\Phi_{p^j d} = \Phi_d^{p^{j-1}(p-1)}$ pour $1 \leq j \leq i-1$, l'identité $\Phi_{p^i d}\Phi_{p^{i-1} d} \ldots \Phi_d = \Phi_d^{p^i}$ implique $\Phi_{p^i d}\Phi_d^{(p^{i-1}-1)} = \Phi_d^{p^i}$ et donc $\Phi_{p^i d} = \Phi_d^{p^{i-1}(p-1)}$.

2. Tout élément α de $\overline{K}^\times$ est contenu dans une extension finie de K et donc appartient au groupe multiplicatif d'un corps fini ; il existe ainsi un plus petit entier naturel $n \geq 1$ tel que $\alpha^n = 1$. Cet entier est évidemment premier à p puisque le groupe multiplicatif d'un corps fini de caractéristique p est d'ordre premier à p.

Étant donnée une extension finie L de K dans $\overline{K}$ contenant α, le groupe de Galois $\mathrm{Gal}(L|K)$ est engendré par l'automorphisme de Frobenius relatif $L \to L,\ x \mapsto x^q$. Le degré de α sur K est l'indice du stabilisateur de α dans $\mathrm{Gal}(L|K)$; c'est donc le plus petit entier d tel que $\alpha^{q^d} = \alpha$, soit de manitère équivalente le plus petit entier d tel que $n | q^d - 1$ ou encore l'ordre de q dans le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$.

3. Le polynôme Φ_n est séparable sur $\mathbb{F}_p$ lorsque l'entier n est premier car c'est un diviseur du polynôme séparable $T^n - 1$. Deux racines du polynôme Φ_n dans $\overline{K}$ ont évidemment le même ordre dans le groupe $\overline{K}^\times$: en effet, le polynôme $T^n - 1$ étant séparable, la situation est analogue à celle rencontrée sur $\mathbb{Q}$ et la factorisation $T^n - 1 = \prod_{d|n} \Phi_d$ implique immédiatement que les racines du polynôme Φ_n dans $\overline{K}$ sont les $\varphi(n)$ éléments d'ordre n du groupe cyclique $\overline{K}^\times$.

Le degré d'un facteur irréductible de Φ_n ayant une racine α dans $\overline{K}$ est le degré de l'extension $K(\alpha)/K$; d'après ce que l'on vient de dire, il découle directement de la question précédente que ce degré est l'ordre de q dans le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ et c'est donc le même pour tout facteur irréductible.

Conclusion : (i) Pour tout entier naturel $n \geq 1$ premier à p, le polynôme cyclotomique Φ_n est irréductible sur K *si et seulement si q engendre le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$;* a contrario*, ce polynôme est scindé sur $\mathbb{F}_p$ si et seulement si $q \equiv 1$* (mod. n).

(ii) Lorsque $p \geq 3$, Φ_n est réductible sur $\mathbb{F}_p$ dès que p divise n en vertu de la question 1.

(iii) Pour tout entier impair $n \geq 1$, $\Phi_{2n} = \Phi_n$ dans $K[T]$ *si $p = 2$.*

Le premier résultat permet de démontrer un cas particulier du *théorème de la progession arithmétique de Dirichlet* — qui affirme que pour tous entiers $a, b \in \mathbb{Z} - \{0\}$ premiers entre eux, la suite arithmétique $a + b\mathbb{Z}$ contient une infinité de nombres premiers : quel que soit l'entier $k \geq 1$, un nombre premier p divisant $\Phi_n(k!)$ est

- congru à 1 modulo n car le polynôme Φ_n possède une racine dans $\mathbb{F}_p$ et donc est scindé dans $\mathbb{F}_p[T]$;
- supérieur à $k+1$ car p divise $(k!)^n - 1$.

Comme $\Phi_n(k!) \notin \{-1, 0, 1\}$ dès que l'entier k est suffisamment grand, il existe donc une infinité de nombres premiers congrus à 1 modulo n.

4. D'après ce qui précède, le polynôme cyclotomique Φ_n est réductible sur $\mathbb{F}_p$ pour tout nombre premier p dès que le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est *pas* cyclique, ce qui est le cas si et seulement si $n \notin \{1, 2, 4\}$ et si n n'est pas de la forme $2^\varepsilon p^\nu$ avec $\varepsilon \in \{0, 1\}$ et $\nu \geq 1$. Ceci fournit une infinité de polynômes irréductibles dans $\mathbb{Z}[T]$ devenant réductibles dans $\mathbb{F}_p[T]$ pour chaque nombre premier p ; tel est le cas par exemple du polynôme $T^4 + 1 = \Phi_8$.

Exercice 3 — Si $[L : K] > n$, il existe une extension finie K' de K dans L telle que $[K' : K] > n$; comme L/K est séparable, il en est de même de K'/K et le théorème de l'élément primitif garantit alors l'existence d'un élément x de L tel que $K' = K(x)$; on aboutit ainsi à une contradiction puisque un tel x est de degré $[K' : K] > n$ sur K.

Exercice 4 — 1. On a $[\mathrm{K}:\mathbb{Q}] = [\mathrm{K}:\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}]$ et $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$, $[\mathrm{K}:\mathbb{Q}(\sqrt{2}] = 2$ (le polynôme T^2+1 est irréductible sur $\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$), donc $[\mathrm{K}:\mathbb{Q}] = 4$. L'élément $\sqrt{2}+i$ de K est primitif car il est annulé par le polynôme

$$(\mathrm{T}-(\sqrt{2}+i))(\mathrm{T}-(\sqrt{2}-i))(\mathrm{T}+(\sqrt{2}+i))(\mathrm{T}+(\sqrt{2}-i)) = \mathrm{T}^4 - 8\mathrm{T}^2 + 9,$$

qui est irréductible sur $\mathbb{Q}$ puisqu'aucun de ses facteurs de degré 1 ou 2 sur K n'appartient à $\mathbb{Q}$.

2. L'extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ est galoisienne et $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ est le groupe cyclique d'ordre 2 engendré par le $\mathbb{Q}$-automorphisme

$$\mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2}), \ \ a+b\sqrt{2} \mapsto a-b\sqrt{2}.$$

L'extension $\mathrm{K}/\mathbb{Q}(\sqrt{2})$ étant séparable de degré 2, il existe deux plongements distincts de K dans le corps algébriquement clos $\mathbb{C}$ prolongeant un plongement donné de $\mathbb{Q}(\sqrt{2})$ dans $\mathbb{C}$; on obtient ainsi quatre plongements distincts $\tau_\ell : \mathrm{K} \to \mathbb{C}$, $1 \leq \ell \leq 4$, avec

$$\tau_1(\sqrt{2}) = \tau_2(\sqrt{2}) = \sqrt{2} \ \text{ et } \ \tau_3(\sqrt{2}) = \tau_4(\sqrt{2}) = -\sqrt{2}.$$

Chacun des plongements τ_ℓ envoyant nécessairement i sur l'une des racines du polynôme T^2+1 dans $\mathbb{C}$, $\tau_\ell(i) = \pm i$ pour tout ℓ et donc $\tau_\ell(\mathrm{K}) \subset \mathrm{K}$. Il existe ainsi $|\mathrm{K}:\mathbb{Q}] = 4$ automorphismes distincts de K au-dessus de $\mathbb{Q}$ et l'extension $\mathrm{K}/\mathbb{Q}$ est par conséquent galoisienne. Tout $\mathbb{Q}$-automorphisme de K étant complètement déterminé par son action sur $\{\pm\sqrt{2}, \pm i\}$, nous pouvons supposer que l'on a

$$\tau_1(\sqrt{2}) = \sqrt{2} \ \text{ et } \ \tau_1(i) = i, \ \ \tau_2(\sqrt{2}) = \sqrt{2} \ \text{ et } \ \tau_2(i) = -i,$$

$$\tau_3(\sqrt{2}) = -\sqrt{2} \ \text{ et } \ \tau_3(i) = i, \ \ \tau_4(\sqrt{2}) = -\sqrt{2} \ \text{ et } \ \tau_4(i) = -i.$$

La loi de groupe sur $\mathrm{Gal}(\mathrm{K}/\mathbb{Q}) = \{\tau_1, \tau_2, \tau_3, \tau_4\}$ est manifeste : c'est le produit des deux groupes cycliques $\{\tau_1, \tau_2\}$ et $\{\tau_1, \tau_3\}$.

3. Les sous-groupes de $(\mathbb{Z}/2\mathbb{Z})^2$ sont au nombre de cinq : outre $\{(0,0)\}$ et $(\mathbb{Z}/2\mathbb{Z})^2$, il y a les trois groupes cycliques d'ordre 2 respectivement engendrés par $(1,0)$, $(0,1)$ et $(1,1)$. Les sous-groupes de $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$ sont donc

$$\{\tau_1\}, \ \mathrm{Gal}(\mathrm{K}/\mathbb{Q}), \ \{\tau_1, \tau_2\}, \ \{\tau_1, \tau_3\} \text{ et } \{\tau_1, \tau_4\},$$

auquels correspondent respectivement les sous-corps K, $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$ et $\mathbb{Q}(i\sqrt{2})$ de K.

Exercice 5 — Soit $\mathrm{P} \in \mathrm{K}[\mathrm{T}]$ le polynôme minimal de x sur K et soit $\mathscr{R}$ l'ensemble des racines de P dans L. Le groupe de Galois $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$ opère *transitivement* sur $\mathscr{R}$ car le polynôme P est irréductible sur K tandis que le stabilisateur de x dans $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$ est un sous-groupe H d'indice $[\mathrm{K}(x):\mathrm{K}] = \deg(\mathrm{P})$ puisque $\mathrm{K}(x) = \mathrm{L}^{\mathrm{H}}$. On en déduit que l'ensemble $\mathscr{R}$ est de cardinal $(\mathrm{Gal}(\mathrm{L}/\mathrm{K}):\mathrm{H}) = \deg(\mathrm{P})$ et donc que le polynôme P est scindé sur L.

Les éléments σ de $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$ fixant x constituent une classe à gauche modulo le fixateur $\mathrm{H} = \mathrm{Gal}(\mathrm{L}/\mathrm{K}(x))$ de x dans $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$ et il y a par conséquent $|\mathrm{H}|$ tels éléments.

Exercice 6 — La clôture galoisienne de E dans $\overline{\mathrm{K}}$ est le sous-corps de $\overline{\mathrm{K}}$ engendré par tous les conjugués des éléments de E ou, de manière équivalente, par les images de E sous les différents K-plongements de E dans $\overline{\mathrm{K}}$. L'extension L/E étant séparable, tout K-plongement σ de E dans $\overline{K}$ se prolonge en un K-plongement $\tilde{\sigma}$ de L dans $\overline{\mathrm{K}}$ et $\tilde{\sigma}(\mathrm{L}) = \mathrm{L}$ puisque L est une extension galoisienne de K. Cela prouve que la clôture galoisienne de E dans $\overline{\mathrm{K}}$ est contenue dans L et peut donc être définie de manière équivalente comme la plus petite extension galoisienne de K dans $\overline{\mathrm{K}}$ contenant E.

La clôture galoisienne E^g de E dans $\overline{\mathrm{K}}$ (ou, de manière équivalente, dans L) est le plus petit sous-corps de L contenant E qui soit galoisien sur K. Notant H le sous-groupe de G fixant E, il découle de la correspondance de Galois que $\mathrm{E}^g = \mathrm{L}^{\mathrm{H}'}$, où H' est le plus grand sous-groupe distingué de G contenu dans H, soit

$$\mathrm{H}' = \bigcap_{g \in \mathrm{G}} g\mathrm{H}g^{-1}.$$

Exercice 7 — *Rappel* [(2)]. *Étant donné un anneau (commutatif) A, le groupe symétrique $\mathfrak{S}_n$ opère naturellement par A-automorphismes sur $A[\mathrm{T}_1, \ldots, \mathrm{T}_n]$ via $\sigma(\mathrm{T}_i) = \mathrm{T}_{\sigma(i)}$ et le sous-anneau $A[\mathrm{T}_1, \ldots, \mathrm{T}_n]^{\mathfrak{S}_n}$ des invariants est*

[(2)] Pour une démonstration, voir par exemple N. Bourbaki, *Algèbre*, Chap. V, Appendice 1 *l'anneau* $A[\Sigma_1,\ldots,\Sigma_n]$ *des polynômes en les fonctions symétriques élémentaires*

$$\Sigma_\lambda = \sum_{1\leq i_1<\ldots<i_\lambda\leq n} T_{i_1}\ldots T_{i_\lambda}.$$

1. On a manifestement $\mathrm{K}\subset\mathrm{L}^{\mathfrak{S}_n}$. Réciproquement, si $f\in k(\mathrm{T}_1,\ldots,\mathrm{T}_n)$ est une fraction rationnelle invariante sous l'action de $\mathfrak{S}_n$, écrivons f sous la forme d'un quotient de deux polynômes a, b premiers entre eux ; quelle que soit la permutation $\sigma\in\mathfrak{S}_n$, $\sigma(a)b = a\sigma(b)$, donc $\sigma(a) = a$, $\sigma(b) = b$ puisque l'anneau $k[\mathrm{T}_1,\ldots,\mathrm{T}_n]$ est factoriel et finalement $f\in\mathrm{K}$. Le corps K est par conséquent le sous-corps des invariants du groupe $\mathfrak{S}_n$ dans L, ce qui implique que l'extension L/K est galoisienne, de groupe de Galois $\mathfrak{S}_n$.

2. Lorsque le corps K est de caractéristique nulle (première à $n!$ suffit), tous les conjugués du polynôme $\mathrm{T}_1+2\mathrm{T}_2+\ldots+n\mathrm{T}_n$ sont distincts ; le polynôme

$$\prod_{\sigma\in\mathfrak{S}_n}(\mathrm{T}-(\mathrm{T}_\sigma(1)+2\mathrm{T}_{\sigma(2)}+\ldots+n\mathrm{T}_{\sigma(n)}))$$

de $\mathrm{K}[\mathrm{T}]$ est par conséquent irréductible sur K et $\mathrm{T}_1+2\mathrm{T}_2+\ldots+n\mathrm{T}_n$ est donc un élément primitif de l'extension L/K.

3. L'inclusion $\mathrm{K}(f)\subset\mathrm{L}^{\mathrm{H}}$ est évidente. D'autre part, $\prod_{g\in\mathfrak{S}_n/\mathrm{H}}(\mathrm{T}-g(f))$ est le polynôme minimal de f sur K donc

$$[\mathrm{K}(f):\mathrm{K}] = (\mathfrak{S}_n:\mathrm{H}) = [\mathrm{L}^{\mathrm{H}}:\mathrm{K}]$$

et $\mathrm{K}(f)=\mathrm{L}^{\mathrm{H}}$. L'extension $\mathrm{L}/\mathrm{K}(f)$ est par conséquent galoisienne et $\mathrm{Gal}(\mathrm{L}/\mathrm{K}(f)) = \mathrm{H}$.

4. Si $f,g\in\mathrm{L}$ sont deux fractions rationnelles ayant le même stabilisateur H dans $\mathfrak{S}_n$, $\mathrm{K}(f)=\mathrm{L}^{\mathrm{H}}=\mathrm{K}(g)$ et g peut donc s'exprimer sous la forme d'une fraction rationnelle en f à coefficients dans K ou, de manière équivalente, come une fraction rationnelle en f et les fonctions symétriques élémentaires à coefficients dans k.

Exemple explicite – Ici, H est le sous-groupe $\{1,(1,2)\}$ de $\mathfrak{S}_3$. Pour exprimer g en fonction de f et de Σ_1, Σ_2 et Σ_3, on peut observer que $(1,f,f^2)$ et $(1,g,g^2)$ sont deux bases du K-espace vectoriel L^{H} puis exprimer f et f^2 en fonction de g et g^2 — ce qui est aisé — et finalement inverser la matrice ainsi obtenue. Si l'on suit cette stratégie, il vient

$$f = \mathrm{T}_1\mathrm{T}_2+\mathrm{T}_3 = \Sigma_2-\mathrm{T}_3(\mathrm{T}_1+\mathrm{T}_2)+\mathrm{T}_3 = \Sigma_2-\mathrm{T}_3(\Sigma_1-\mathrm{T}_3)+\mathrm{T}_3 = \Sigma_2+(1-\Sigma_1)g+g^2$$

et

$$f^2 = \Sigma_2^2+2\Sigma_2(1-\Sigma_1)g+\big((1-\Sigma_1)^2+2\Sigma_2\big)g^2+2(1-\Sigma_1)g^3+g^4,$$

soit

$$f^2 = \big(\Sigma_2^2+2(1-\Sigma_1)\Sigma_3+\Sigma_1\Sigma_2\big)+\big(\Sigma_3-\Sigma_1\Sigma_2\big)g+(1+\Sigma_2)g^2 = \mathrm{A}+\mathrm{B}g+\mathrm{C}g^2$$

en utilisant l'identité $g^3-\Sigma_1g^2+\Sigma_2g-\Sigma_3=0$. On en déduit

$$g = (\mathrm{B}-\mathrm{C}(1-\Sigma_1)^{-1}\big((\mathrm{C}\Sigma_2-A)-\mathrm{C}f+f^2).$$

Exercice 8 — 1. Soient G un groupe et $g_1,\ldots,g_n$ des homomorphismes distincts de G dans le groupe multiplicatif d'un corps k. Si $g_1,\ldots,g_n$ n'étaient pas linéairement indépendants sur k, il existerait une relation de dépendance linéaire

$$\lambda_1g_1+\ldots+\lambda_ng_n=0$$

dont le nombre $r\geq 2$ de coefficients λ_i non nuls serait minimal. Après avoir réordonné les g_i de sorte que $\lambda_n\neq 0$ et avoir posé $\mu_i=\lambda_n^{-1}\lambda_i$, on obtient

$$\mu_1g_1+\ldots+\mu_{n-1}g_{n-1}+g_n=0.$$

Quel que soit alors $a\in\mathrm{G}$, $g_n(a)\neq 0$ et la relation précédente fournit

$$g_n(a)^{-1}g_1(a)\mu_1g_1+\ldots+g_n(a)^{-1}g_{n-1}(a)\mu_{n-1}g_{n-1}+g_n=0$$

en utilisant le fait que les g_i sont des homomorphismes de G dans $k^\times$, donc

$$\mu_1(1-g_n(a)^{-1}g_1(a))g_1+\ldots+\mu_{n-1}(1-g_n(a)^{-1}g_{n-1}(a))g_{n-1}=0.$$

Puisque g_1 et g_n sont, par hypothèse, distincts, il existe $a\in\mathrm{G}$ tel que $g_n(a)\neq g_1(a)$; ayant choisi un tel a, la relation de dépendance linéaire obtenue entre les g_i est non triviale et contient au plus $r-1$ coefficients non nuls, en contradiction avec la minimalité de r.

2. Étant donnés deux corps k, K et n homomorphismes distincts $\sigma_1, \dots, \sigma_n$ de k dans K, le sous-ensemble k_0 est un sous-corps de k. Si k était de dimension $m < n$ en tant que k_0-espace vectoriel, une base $(e_1, \dots, e_m)$ de k sur k_0 donnerait naissance à un système linéaire sous-déterminé

$$\left\{ \begin{array}{lllll} x_1\sigma_1(e_1) & +\dots+ & x_n\sigma_n(e_1) & = & 0 \\ \dots & \dots & \dots & \dots & \dots \\ x_1\sigma_1(e_m) & +\dots+ & x_n\sigma_n(e_m) & = & 0 \end{array} \right.$$

et il existerait donc des éléments $x_1, \dots, x_n$ de K, non tous nuls, tels que

$$x_1\sigma_1(e_i) + \dots + x_n\sigma_n(e_i) = 0$$

pour tout $i \in \{1, \dots, m\}$, ce qui équivaut à

$$x_1\sigma_1(a) + \dots + x_n\sigma_n(a) = 0$$

pour tout $a \in k$ vu la définition de k_0. En observant que les σ_i définissent des homomorphismes du groupe $k^\times$ dans $\mathrm{K}^\times$, ceci contredit l'indépendance linéaire des σ_i établie à la question précédente. Nous avons donc $[k : k_0] \geq n$.

Exercice 9 — 1. Supposons tout d'abord que le corps K soit fini, auquel cas le groupe G est cyclique et engendré par l'automorphisme de Frobenius relatif $\mathrm{L} \to \mathrm{L},\ \ x \mapsto x^q$, où $q = \mathrm{Card}(\mathrm{K})$. L'existence d'une base normale pour l'extension L/K est équivalente à l'existence d'un vecteur *cyclique* pour l'endomorphisme σ du K-espace vectoriel L, c'est-à-dire d'un vecteur $x \in \mathrm{L}$ tel que la famille $(x, \sigma(x), \dots, \sigma^{d-1}(x))$ constitue une base de L sur K, où l'on a posé $d = [\mathrm{L} : \mathrm{K}]$. Cette question relève de l'algèbre linéaire élémentaire et admet une réponse bien connue : un tel vecteur cyclique existe si et seulement si les polynômes minimal et caractéristique de l'endomorphisme σ coïncident [3] Le polynôme caractéristique de σ est $\mathrm{T}^q - \mathrm{T}$. Si un polynôme $\mathrm{Q} = \sum_n a_n \mathrm{T}^n \in \mathrm{K}[\mathrm{T}]$ annule σ, alors le polynôme $\sum_n a_n \mathrm{T}^{q^n}$ s'annule identiquement sur L et donc $q^{\deg(\mathrm{Q})} \geq q^d$; on a par conséquent $\deg(\mathrm{Q}) \geq d$ et $\mathrm{T}^q - \mathrm{T}$ est donc bien le polynôme minimal de σ. Le théorème est ainsi démontré lorsque le corps K est fini.

2. (i) On a $f = \prod_{\sigma \in \mathrm{G}} (\mathrm{T} - \sigma(x))$, donc

$$\frac{1}{f} = \sum_{\sigma \in \mathrm{G}} \frac{1}{(\mathrm{T} - \sigma(x)) f'(\sigma(x))}$$

et $\sum_{\sigma \in \mathrm{G}} \mathrm{R}_\sigma = 1$. Comme $\mathrm{R}_\sigma \mathrm{R}_\tau \equiv 0 \pmod f$ pour tous $\sigma, \tau \in \mathrm{G}$ distincts, on obtient $\mathrm{R}_\sigma^2 \equiv \mathrm{R}_\sigma (\mathrm{mod}\ f)$ en multipliant les deux membres de l'identité précédente par R_σ.

(ii) Le déterminant D de la matrice $(\mathrm{R}_{\tau\sigma})_{(\tau,\sigma) \in \mathrm{G}^2} \in \mathrm{M}_{[\mathrm{L}:\mathrm{K}]}(\mathrm{L}[\mathrm{T}])$ est un élément de $\mathrm{L}[\mathrm{T}]$. Vu la question précédente, la matrice $(\mathrm{R}_{\tau\sigma})^2$ est congrue à la matrice $\mathrm{diag}(\sum_\sigma \mathrm{R}_\sigma^2)_{\sigma \in \mathrm{G}} = \mathrm{I}_{[\mathrm{L}:\mathrm{K}]}$ modulo f et donc

$$\mathrm{D}^2 \equiv 1 (\mathrm{mod}\ f).$$

(iii) Par construction, $\mathrm{R}_{\tau\sigma} = \tau(\mathrm{R}_\sigma)$ pour tous $\sigma, \tau \in \mathrm{G}$; en particulier, $\mathrm{R}_\sigma = \sigma(\mathrm{R}_1)$. Étant donné un élément y de L, toute relation linéaire non triviale entre les $\sigma(\mathrm{R}_1(y))$ à coefficients dans K fournit une relation linéaire non triviale entre les colonnes de la matrice $(\mathrm{R}_{\tau\sigma}(y))_{(\sigma,\tau) \in \mathrm{G}^2}$ puisque

$$\sum_{\sigma \in \mathrm{G}} \lambda_\sigma \mathrm{R}_{\tau\sigma}(y) = \sum_{\sigma \in \mathrm{G}} \lambda_\sigma \tau(\mathrm{R}_\sigma(y)) = \tau \left(\sum_{\sigma \in \mathrm{G}} \lambda_\sigma \mathrm{R}_\sigma(y) \right)$$

pour tout $(\lambda_\sigma) \in \mathrm{K}^\mathrm{G}$. Le polynôme D étant non nul d'après la question précédente et le corps K étant infini, il existe un élément y de K tel que $\mathrm{R}_1(y) \neq 0$ et, d'après ce que l'on vient de dire, la famille $(\sigma(\mathrm{R}_1(y)))_{\sigma \in \mathrm{G}}$ est une base de L en tant que K-espace vectoriel.

---

[3] Si l'on fait de L un K[T]-module en posant $\mathrm{T}x = \sigma(x)$, l'existence d'un vecteur cyclique équivaut au fait que L soit un $\mathrm{A} = \mathrm{K}[\mathrm{T}]/(m_\sigma)$-module monogène, où m_σ désigne le polynôme minimal de σ. Pour cela, il est clairement nécessaire que m_u soit le polynôme caractéristique de σ pour des raison de dimension ; c'est également suffisant, car alors, pour chaque facteur irréductible p de m_σ, la composante p-primaire de L est monogène puisque de longueur égale à la multiplicité de p dans m_σ et il en est donc de même du A-module L en vertu du théorème chinois des restes.