

THÉORIE DE GALOIS III - CORRIGÉ

Exercice 1 — 1. Fixons une racine x de $T^p - T + a$ dans L . Quel que soit l'élément u de \mathbb{F}_p , $(x+u)^p - (x+u) = x^p + u^p - (x+u) = x^p - x$ et les racines de $T^p - T + a$ dans L sont donc les p éléments $x+u$, $u \in \mathbb{F}_p$. On en déduit une application injective

$$\text{Gal}(L/K) \rightarrow \mathbb{F}_p, \sigma \mapsto \sigma(x) - x,$$

qui est manifestement un homomorphisme de groupes puisque

$$(\sigma\tau)(x) - x = \sigma(\tau(x) - x) + \sigma(x) - x = \tau(x) - x + \sigma(x) - x$$

car $\tau(x) - x \in \mathbb{F}_p \subset K$.

Il y a deux possibilités :

- si $\text{Gal}(L/K) = \{1\}$, alors le polynôme $T^p - T + a$ est scindé sur K ;
- si $\text{Gal}(L/K) \simeq \mathbb{F}_p$, alors $[L : K] = p$ et, puisque L est un corps de rupture du polynôme $T^p - T + a$, celui-ci est irréductible sur K .

2. (i) Le groupe de Galois $\text{Gal}(L/K)$ est constitué des p automorphismes $\sigma^n : L \rightarrow L$, $0 \leq n \leq p-1$. En vertu du lemme de Dedekind, ces automorphismes sont linéairement indépendants sur L et il existe donc un élément y de L tel que

$$z = \sum_{n=0}^{p-1} \sigma^n(y) \neq 0.$$

On a par ailleurs

$$(\sigma - \text{id}_L) \left(\sum_{n=0}^{p-1} \sigma^n(y) \right) = \sigma^p(y) - y = 0,$$

ce qui prouve que z est un élément non nul de K ; il reste à poser $x = z^{-1}y$ pour obtenir un élément de L tel que $\sum_{n=0}^{p-1} \sigma^n(x) = 1$.

(ii) On a

$$\begin{aligned} \sigma(\alpha) &= \sum_{n=0}^{p-1} n\sigma^{n+1}(x) \\ &= \sum_{n=0}^{p-1} (n+1)\sigma^{n+1}(x) - \sum_{n=0}^{p-1} \sigma^{n+1}(x) \\ &= \sum_{n=0}^{p-1} n\sigma^n(x) - x + \sigma^p(x) - \sum_{n=0}^{p-1} \sigma^n(x) \\ &= \alpha - 1, \end{aligned}$$

ce qui prouve que α n'appartient pas au corps K ; d'autre part, comme

$$\sigma(\alpha^p - \alpha) = \sigma(\alpha)^p - \sigma(\alpha) = (\alpha - 1)^p - (\alpha - 1) = \alpha^p - \alpha,$$

$a = \alpha^p - \alpha \in K$. En vertu de la première question, le corps de décomposition $K(\alpha)$ du polynôme $T^p - T + a$ dans L est une extension de K de degré p ; puisque $[L : K] = p$, $L = K(\alpha)$.

Exercice 2 — 1. L'ensemble \mathfrak{B}_p des permutations de $\mathbb{Z}/p\mathbb{Z}$ de la forme $x \mapsto \sigma_{a,b}(x) = ax + b$, $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, $b \in \mathbb{Z}/p\mathbb{Z}$, est clairement un sous-groupe de $\mathfrak{S}(\mathbb{Z}/p\mathbb{Z})$ de cardinal $p(p-1)$.

Vu l'identité

$$\sigma_{a,b}\sigma_{c,d}\sigma_{a,b}^{-1} = \sigma_{a,b}\sigma_{c,d}\sigma_{a^{-1},-a^{-1}b} = \sigma_{c,ad-bc+b},$$

les permutations $\sigma_{1,b}$, $b \in \mathbb{Z}/p\mathbb{Z}$, constituent un sous-groupe distingué \mathfrak{C}_p de \mathfrak{B}_p , cyclique et d'ordre p . Le quotient $\mathfrak{B}_p/\mathfrak{C}_p$ est isomorphe au sous-groupe de \mathfrak{B}_p constitué des permutations de la forme $\sigma_{a,0}$, $a \in (\mathbb{Z}/p\mathbb{Z})^\times$; il s'agit donc d'un groupe cyclique d'ordre $p-1$ et la suite de composition

$$1 \triangleleft \mathfrak{C}_p \triangleleft \mathfrak{B}_p$$

à quotients cycliques montre que le groupe \mathfrak{B}_p est résoluble.

Quels que soient $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, $b \in \mathbb{Z}/p\mathbb{Z}$,

$$\sigma_{a,b}^n = \sigma_{a^n, (a^{n-1} + \dots + a + 1)b}$$

pour tout entier naturel $n \geq 1$. On a donc

$$\sigma_{a,b}^p = \begin{cases} \sigma_{a,b} & \text{si } a \neq 1 \\ \sigma_{1,0} = 1 & \text{si } a = 1 \end{cases},$$

ce qui prouve que la permutation $\sigma_{a,b}$ est d'ordre p si et seulement si $a \neq 1$ et $b \neq 0$.

2. (i) Soient G un sous-groupe transitif de $\mathfrak{S}(\mathbb{Z}/p\mathbb{Z})$ et H un sous-groupe distingué de G . Quel que soient $i, j \in \{1, \dots, p\}$, les sous-groupes de H fixant respectivement i et j sont conjugués dans G et on par conséquent le même cardinal ; les orbites de H sur $\{0, \dots, p-1\}$ ont ainsi le même cardinal, lequel doit diviser p . Il en découle que l'opération de H sur $\{0, \dots, p-1\}$ est soit triviale, soit transitive ; en particulier, le sous-groupe H de G opère transitivement sur $\{1, \dots, p\}$ s'il n'est pas trivial.

En appliquant successivement cet argument aux sous-groupes G_{i+1} et G_i à partir de $i = r-1$, on en déduit que le sous-groupe G_1 de $\mathfrak{S}(\mathbb{Z}/p\mathbb{Z})$ opère transitivement sur $\{0, \dots, p-1\}$. Soit finalement $\tau \in \mathfrak{S}(\mathbb{Z}/p\mathbb{Z})$ une permutation engendrant le groupe G_1 ; les supports des cycles intervenant dans la décomposition de τ étant manifestement stables sous toutes les puissances de τ , le groupe G_1 ne peut opérer transitivement sur $\{1, \dots, p\}$ que si τ est un p -cycle.

(ii) Si l'on note σ la permutation de $\mathbb{Z}/p\mathbb{Z}$ définie par $\sigma(i) = \tau^i(0)$ ($1 \leq i \leq p-1$), $\sigma^{-1}G_1\sigma$ est le sous-groupe cyclique de $\mathfrak{S}(\mathbb{Z}/p\mathbb{Z})$ engendré par la permutation $\sigma_{1,1} : \sigma^{-1}G_1\sigma = \mathfrak{C}_p$.

Soit $\lambda \in \sigma^{-1}G_2\sigma$ une permutation dont l'image engendre le groupe cyclique $(\sigma^{-1}G_2\sigma)/(\sigma^{-1}G_1\sigma)$. Puisque le sous-groupe $\sigma^{-1}G_1\sigma = \langle \sigma_{1,1} \rangle$ est distingué dans $\sigma^{-1}G_2\sigma$, il existe $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ tel que $\lambda\sigma\lambda^{-1} = \sigma_{1,1}^a = \sigma_{1,a}$ et donc

$$\lambda(x+1) = \lambda\sigma_{1,1}(x) = \sigma_{1,a}\lambda(x) = \lambda(x) + a$$

puis $\lambda(x) = ax + \lambda(0)$ pour tout $x \in \mathbb{Z}/p\mathbb{Z}$, ce qui prouve que le sous-groupe $\sigma^{-1}G_2\sigma$ de $\mathfrak{S}(\mathbb{Z}/p\mathbb{Z})$ est contenu dans \mathfrak{B}_p .

(iii) Il est clair que \mathfrak{C}_p est l'unique sous-groupe cyclique d'ordre p de \mathfrak{B}_p . Vu ce qui précède, on en déduit que G_1 est l'unique sous-groupe cyclique d'ordre p de G_2 ; il s'agit donc d'un sous-groupe caractéristique (i.e. stable sous tout automorphisme) de G_2 et G_1 est par conséquent un sous-groupe distingué de G_3 . En appliquant le raisonnement de la question (ii), on établit à partir de là que le groupe $\sigma^{-1}G_3\sigma$ est contenu dans \mathfrak{B}_p . En itérant $r-2$ fois ce raisonnement, on obtient finalement que G_1 est un sous-groupe distingué de G , puis que $\sigma^{-1}G\sigma$ est contenu dans le sous-groupe \mathfrak{B}_p de $\mathfrak{S}(\mathbb{Z}/p\mathbb{Z})$.

3. (i) Le polynôme minimal de β sur $K(\alpha)$ est un diviseur strict du polynôme P , de sorte que $[K(\alpha, \beta) : K(\alpha)] \leq p-1$. L'irréductibilité de P sur K garantit par ailleurs que l'on a $[K(\alpha) : K] = p$, d'où finalement

$$[L : K] = [K(\alpha, \beta) : K] = [K(\alpha, \beta) : K(\alpha)][K(\alpha) : K] \leq p(p-1).$$

(ii) L'extension intermédiaire $K(\alpha)/K$ étant de degré p , l'ordre du groupe $\text{Gal}(L/K)$ est de la forme pm avec $1 \leq m \leq p-1$. En appliquant le lemme de Cauchy, on en déduit l'existence d'un élément de $\text{Gal}(L/K)$ d'ordre p ; comme les seules permutations d'ordre p dans \mathfrak{S}_p sont les permutations circulaires (i.e. les p -cycles), le groupe $\text{Gal}(L/K)$, identifié à un groupe de permutations des racines de P dans L , contient une permutation circulaire.

Soient H et H' deux sous-groupes de $G = \text{Gal}(L/K)$ d'ordre p . Si $H \neq H'$, $H \cap H' = \{1\}$ et la projection canonique $G \rightarrow G/Hr$ induit une injection de H' dans G/Hr ; comme l'ensemble d'arrivée est de cardinal $m < p$, ceci est impossible et donc $H = H'$. Toutes les permutations circulaires contenues dans $\text{Gal}(L/K)$ engendrent donc le même sous-groupe.

(iii) Soit τ une permutation circulaire contenue dans $\text{Gal}(L/K)$. Le sous-groupe $H = \text{Gal}(L/K(\alpha))$ de $\text{Gal}(L/K)$ étant d'ordre $m < p$, $\langle \tau \rangle \cap H = \{1\}$ et donc $\alpha, \tau(\alpha), \dots, \tau^{p-1}(\alpha)$ sont les p racines de P dans L ; quitte à remplacer τ par une puissance convenable, on peut en outre supposer que l'on a $\beta = \tau(\alpha)$.

Le groupe $\text{Gal}(L/K(\alpha))$ est abélien : en effet, étant donnés $\sigma_1, \sigma_2 \in \text{Gal}(L/K(\alpha))$, il existe des entiers $i_1, i_2 \in (\mathbb{Z}/p\mathbb{Z})^\times$ tels que $\sigma_1\tau = \tau^{i_1}\sigma_1$ et $\sigma_2\tau = \tau^{i_2}\sigma_2$; on a alors

$$\sigma_1\sigma_2(\alpha) = \sigma_2\sigma_1(\alpha) = \alpha$$

et

$$\begin{aligned}
\sigma_1 \sigma_2(\beta) &= \sigma_1 \sigma_2 \tau(\alpha) \\
&= \sigma_1 \tau^{i_2} \sigma_2(\alpha) \\
&= \sigma_1 \tau^{i_2}(\alpha) \\
&= \tau^{i_1 i_2} \sigma_1(\alpha) \\
&= \tau^{i_1 i_2}(\alpha) \\
&= \sigma_2 \sigma_1(\beta),
\end{aligned}$$

donc $\sigma_1 \sigma_2 = \sigma_2 \sigma_1$.

Nous pouvons maintenant conclure. Notant Z le sous-groupe distingué de $\text{Gal}(L/K)$ engendré par les permutations circulaires, Z est cyclique d'ordre p et la projection canonique $\text{Gal}(L/K) \rightarrow \text{Gal}(L/K)/Z$ induit un isomorphisme de $\text{Gal}(L/K(\alpha))$ sur le quotient $\text{Gal}(L/K)/Z$; nous en déduisons que ce dernier groupe est abélien, ce qui établit que le groupe $\text{Gal}(L/K)$ est résoluble.

4. Supposons que le groupe $\text{Gal}(L/K)$ soit résoluble et considérons deux racines distinctes α, β de P dans L . Vu la question 2, un élément non trivial de $\text{Gal}(L/K)$ fixe au plus une racine de P dans L ; il en découle $\text{Gal}(L/K(\alpha, \beta)) = \{1\}$ et donc $L = K(\alpha, \beta)$.

Exercice 3 — I. Soit $f \in K[T]$ un polynôme séparable et soit \mathcal{R} l'ensemble de ses racines dans un corps de décomposition K' ; on identifie $G = \text{Gal}(K'/K)$ à un sous-groupe de $\mathfrak{S}(\mathcal{R})$.

Étant données des indéterminées $Y_i, i \in I$, le groupe $\text{Gal}(K'/K)$ opère naturellement sur l'anneau $K'[(Y_i)_{i \in I}]$ via

$$\sigma \left(\sum_{\nu} a_{\nu} Y^{\nu} \right) = \sum_{\nu} \sigma(a_{\nu}) Y^{\nu}.$$

On a clairement $K'[(Y_i)_{i \in I}]^G = K[(Y_i)_{i \in I}]$: en effet, l'inclusion évidente $K((Y_i)_{i \in I}) \subset K'((Y_i)_{i \in I})^G$ est une égalité car

$$[K'((Y_i)_{i \in I}) : K((Y_i)_{i \in I})] = [K' : K] = \text{Card}(G) = [K'((Y_i)_{i \in I}) : K'((Y_i)_{i \in I})^G]$$

et

$$K'[(Y_i)_{i \in I}]^G = K'[(Y_i)_{i \in I}] \cap K'((Y_i)_{i \in I})^G = K[(Y_i)_{i \in I}].$$

1. Quelles que soient les permutations $\sigma, \tau \in \mathfrak{S}(\mathcal{R})$,

$$\tau(L_{\sigma}) = \sum_{\xi \in \mathcal{R}} \tau(\xi) Y_{\sigma^{-1}(\xi)} = \sum_{\xi \in \mathcal{R}} \xi Y_{\sigma^{-1}\tau^{-1}(\xi)} = \sum_{\xi \in \mathcal{R}} \xi Y_{(\tau\sigma)^{-1}(\xi)} = L_{\tau\sigma};$$

on en déduit immédiatement que les polynômes Π_f et Θ_f appartiennent à l'anneau $K'[Y, (Y_{\xi})_{\xi \in \mathcal{R}}]^G = K[Y, (Y_{\xi})_{\xi \in \mathcal{R}}]$. En outre, si l'on désigne par X un ensemble de représentants des classes à gauche modulo G dans $\mathfrak{S}(\mathcal{R})$,

$$\Pi_f = \prod_{\sigma \in \mathfrak{S}(\mathcal{R})} (Y - L_{\sigma}) = \prod_{\sigma \in X} \prod_{\tau \in G} (Y - L_{\tau\sigma}) = \prod_{\sigma \in X} \prod_{\tau \in G} (Y - \tau(L_{\sigma}));$$

chacun des facteurs $\prod_{\tau \in G} (Y - \tau(L_{\sigma}))$ est manifestement invariant sous l'action de G , donc appartient à l'anneau $K[Y, (Y_{\xi})_{\xi \in \mathcal{R}}]$, et il est irréductible puisque le groupe de Galois G de l'extension $K'((Y_{\xi})_{\xi \in \mathcal{R}})/K((Y_{\xi})_{\xi \in \mathcal{R}})$ opère transitivement sur l'ensemble de ses racines de ce polynôme dans $K'((Y_{\xi})_{\xi \in \mathcal{R}})$. En particulier: le polynôme Θ_f est un facteur irréductible de Π_f dans $K[Y, (Y_{\xi})_{\xi \in \mathcal{R}}]$.

2. Vu la décomposition de Π_f en produit de facteurs irréductibles dans $K[Y, (Y_{\xi})_{\xi \in \mathcal{R}}]$, il est manifeste que le groupe $\mathfrak{S}(\mathcal{R})$ opère transitivement sur l'ensemble des facteurs irréductibles de Π_f dans $K[Y, (Y_{\xi})_{\xi \in \mathcal{R}}]$ et que le sous-groupe G est le fixateur du facteur Θ_f dans $\mathfrak{S}(\mathcal{R})$.

II. On suppose maintenant $K = \mathbb{Q}$ et $f \in \mathbb{Z}[T]$, unitaire de degré d .

1. Le polynôme f étant unitaire et à coefficients entiers, ses racines sont des entiers algébriques. Les coefficients des polynômes Π_f et Θ_f sont par conséquent des entiers algébriques et, comme ils sont par ailleurs rationnels, il s'agit de nombres entiers puisque l'anneau \mathbb{Z} est intégralement clos.

2. (i) Si l'on considère les racines ξ de f comme des indéterminées, le polynôme

$$\prod_{\sigma \in \mathfrak{S}(\mathcal{R})} \left(Y - \sum_{\xi \in \mathcal{R}} \xi Y_{\sigma^{-1}(\xi)} \right)$$

est à coefficients dans l'anneau $\mathbb{Z}[\Sigma_1, \dots, \Sigma_d]$, où Σ_i est la i -ème fonction symétrique élémentaire des $\xi \in \mathcal{R}$:

$$\Sigma_i = \sum_{I \subset \mathcal{R}, \text{Card}(I)=i} \prod_{\xi \in I} \xi.$$

On a de même

$$\prod_{\sigma \in \mathfrak{S}(\mathcal{R}_p)} \left(Y - \sum_{\zeta \in \mathcal{R}_p} \zeta Y_{\sigma^{-1}(\zeta)} \right) \in \mathbb{Z}[Z_1, \dots, Z_d][Y, (Y_\zeta)_{\zeta \in \mathcal{R}_p}],$$

où Z_1, \dots, Z_d sont les fonctions symétriques élémentaires des $\zeta \in \mathcal{R}_p$. Quelle que soit la bijection $\varphi : \mathcal{R} \rightarrow \mathcal{R}_p$ permettant d'identifier les anneaux $\mathbb{Z}[Y, (Y_\xi)_{\xi \in \mathcal{R}}]$ et $\mathbb{Z}[Y, (Y_\zeta)_{\zeta \in \mathcal{R}_p}]$, Z_i est la réduction de Σ_i modulo p et le polynôme $\Pi_{\bar{f}}$ est donc la réduction du polynôme Π_f modulo p .

On a vu que le groupe $\mathfrak{S}(\mathcal{R})$ opère transitivement sur l'ensemble des facteurs irréductibles de Π_f dans $\mathbb{Z}[Y, (Y_\xi)_{\xi \in \mathcal{R}}]$; toute bijection $\varphi : \mathcal{R} \rightarrow \mathcal{R}_p$ induisant un isomorphisme du groupe $\mathfrak{S}(\mathcal{R})$ sur le groupe $\mathfrak{S}(\mathcal{R}_p)$, ce dernier opère donc transitivement sur les réductions modulo p des facteurs irréductibles de Π_f .

(ii) Il existe évidemment un unique facteur irréductible de Π_f dont la réduction est divisible par $\Theta_{\bar{f}}$. Par suite, si $\Theta_{\bar{f}}$ divise la réduction $\overline{\Theta}_f$ de Θ_f modulo p , alors toute permutation de \mathcal{R}_p fixant le facteur $\Theta_{\bar{f}}$ de $\overline{\Pi}_f = \overline{\Pi}_f$ fixe nécessairement le facteur $\overline{\Theta}_f$; ainsi, quelle que soit la bijection admissible $\varphi : \mathcal{R} \rightarrow \mathcal{R}_p$, l'homomorphisme $\mathfrak{S}(\mathcal{R}_p) \rightarrow \mathfrak{S}(\mathcal{R})$, $\sigma \mapsto \varphi^{-1}\sigma\varphi$ envoie le stabilisateur de $\Theta_{\bar{f}}$ dans celui de Θ_f , c'est-à-dire le groupe de Galois $\text{Gal}(\mathbb{F}_p(\mathcal{R}_p)/\mathbb{F}_p)$ de \bar{f} dans le groupe de Galois $\text{Gal}(\mathbb{K}(\mathcal{R})/\mathbb{K})$ de f .

(iii) Fixons une bijection $\varphi : \mathcal{R} \rightarrow \mathcal{R}_p$ et utilisons-là pour identifier les anneaux $\mathbb{Z}[Y, (Y_\xi)_{\xi \in \mathcal{R}}]$ et $\mathbb{Z}[Y, (Y_\zeta)_{\zeta \in \mathcal{R}_p}]$. Si Q est un facteur irréductible de $\overline{\Pi}_f$ divisant la réduction de Θ_f modulo p , l'isomorphisme $\mathfrak{S}(\mathcal{R}_p) \rightarrow \mathfrak{S}(\mathcal{R})$, $\sigma \mapsto \varphi^{-1}\sigma\varphi$ envoie le stabilisateur H de Q dans $\text{Gal}(\mathbb{K}'/\mathbb{Q})$; comme $H = \tau^{-1}\text{Gal}(\mathbb{F}_p(\mathcal{R}_p)/\mathbb{F}_p)\tau$ pour une permutation convenable $\tau \in \mathfrak{S}(\mathcal{R}_p)$ en vertu de la question I.1, l'homomorphisme $\mathfrak{S}(\mathcal{R}_p) \rightarrow \mathfrak{S}(\mathcal{R})$, $\sigma \mapsto \varphi^{-1}\tau^{-1}\sigma\tau\varphi$ envoie $\text{Gal}(\mathbb{F}_p(\mathcal{R}_p)/\mathbb{F}_p)$ dans $\text{Gal}(\mathbb{K}'/\mathbb{Q})$ et la bijection $\tau \circ \varphi$ de \mathcal{R} sur \mathcal{R}_p est admissible.

Il est clair que deux bijections admissibles induisent des homomorphismes de $\mathfrak{S}(\mathcal{R}_p)$ dans $\mathfrak{S}(\mathcal{R})$ qui envoient $\text{Gal}(\mathbb{F}_p(\mathcal{R}_p)/\mathbb{F}_p)$ sur deux sous-groupes conjugués de $\mathcal{G} \uparrow (\mathbb{K}'/\mathbb{Q})$.

III. 1. Soit $f \in \mathbb{Z}[T]$ un polynôme unitaire de degré n et soit G le groupe de Galois d'un corps de décomposition de f , que l'on identifie à un sous-groupe du groupe symétrique \mathfrak{S}_n .

- L'irréductibilité de $f \pmod{p_1}$ implique l'irréductibilité de f dans $\mathbb{Q}[T]$ et donc la *transitivité* du sous-groupe G de \mathfrak{S}_n .
- L'automorphisme de Frobenius $\sigma_{p_2} : x \mapsto x^{p_2}$ détermine un élément du groupe de Galois du polynôme $f \pmod{p_2}$ de la forme tc ou tcc' , t étant une transposition et c, c' étant deux cycles de longueur impaire; $\sigma_{p_2}^{\text{ord}(c)\text{ord}(c')}$ est alors une transposition et, identifiant le groupe de Galois de $f \pmod{p_2}$ à un sous-groupe de G (cf. partie II), nous en déduisons que le groupe G contient une transposition.
- En raisonnant comme précédemment, on déduit de l'hypothèse sur $f \pmod{p_3}$ que le groupe G contient un cycle de longueur $n-1$.

Tout sous-groupe transitif G de \mathfrak{S}_n contenant une transposition t et un $n-1$ -cycle c est nécessairement égal à \mathfrak{S}_n .

- Si le support de t n'est pas contenu dans celui de c , alors $t = (i, j)$ avec $c(i) = i, c^k t c^{-k} = (c^k(i), c^k(j)) = (i, c^k(j))$ pour tout entier $k \geq 1$ et G contient donc toutes les transpositions de la forme (i, ℓ) avec $\ell \in \{1, \dots, n\} - \{i\}$; ces dernières engendrant le groupe \mathfrak{S}_n , $G = \mathfrak{S}_n$.
- Si le support de t est contenu dans celui de c , la transitivité de G garantit l'existence d'un élément g de G tel que $t = (i, j)$ et $g(i) \notin \text{Supp}(c)$; il suffit alors de remplacer t par la transposition $gtg^{-1} = (g(i), g(j))$ pour être ramené au cas précédent.

Remarque : lorsque $n = p$ est un nombre premier, il suffit d'avoir la première et la deuxième des trois conditions précédentes car une transposition t et un p -cycle c engendrent le groupe \mathfrak{S}_p : en effet, si $t = (1, 2)$, il existe un entier $k \geq 1$ tel que $c^k(1) = 2$ et donc, quitte à remplacer c par c^k , on peut supposer $c = (1, 2, \dots)$; on a alors $t_j = c^j t c^{-j} = (c^j(1), c^j(2)) = (c^{j-1}(2), c^j(2))$ pour tout $j \geq 1$ et, comme les p entiers $c^0(2), c(2), \dots, c^{p-1}(2)$ sont tous distincts, il existe une permutation $\sigma \in \mathfrak{S}_p$ telle que $t_j = \sigma(j+1, j+2)$ pour tout $j \in \{0, \dots, p-2\}$, ce qui prouve que t et c engendrent \mathfrak{S}_p .

2. La décomposition du polynôme $T^5 - T - 1$ en produit de facteurs irréductibles dans $\mathbb{F}_2[T]$ est

$$T^5 - T - 1 = (T^2 - T - 1)(T^3 + T^2 + 1).$$

Ce polynôme est par ailleurs irréductible dans $\mathbb{F}_3[T]$: en effet, si tel n'était pas le cas, il posséderait alors une racine ξ dans \mathbb{F}_9 ; comme $T^9 - T = (T^5 - T - 1)(T^4 + 1) + T^4 + 1$, ξ serait racine de $T^4 + 1$, et donc racine double de $T^9 - T$ puisque $T^4 + 1 \mid T^9 - T$...

Le polynôme $T^7 - T - 1$ est irréductible dans $\mathbb{F}_2[T]$: en effet, comme

$$T^8 - T = (T^7 - T - 1)T + T^2,$$

$T^7 - T - 1$ est premier au polynôme $T^8 - T$ et n'admet donc aucune racine dans \mathbb{F}_8 . Vu les identités

$$T^9 - T = T^2(T^7 - T - 1) + T(T^2 + T - 1) \quad \text{et} \quad T^9 - T = T(T - 1)(T + 1)(T^2 + 1)(T^2 + T - 1)(T^2 + 2T - 1)$$

dans $\mathbb{F}_3[T]$, $T^2 + T - 1$ est un facteur irréductible de $T^7 - T - 1$ dans $\mathbb{F}_3[T]$ et l'autre facteur, de degré 5 est irréductible puisqu'il est manifestement premier à $T^9 - T$ et n'admet donc aucune racine dans \mathbb{F}_9 .

Vu la remarque faite à l'issue de la question précédente, l'analyse que nous venons de faire prouve que les groupes de Galois des polynômes $T^5 - T - 1$ et $T^7 - T - 1$ sont respectivement \mathfrak{S}_5 et \mathfrak{S}_7 .

Exercice 4 — 1. L'application $\mathbb{F}_{p^n} \rightarrow \mathbb{F}_p[T]$ associant à ξ son polynôme minimal sur \mathbb{F}_p , induit une bijection entre l'ensemble des orbites de $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ sur $\mathbb{F}_{p^n} - \bigcup_{m \mid n, m \neq n} \mathbb{F}_{p^m}$ et l'ensemble des polynômes unitaires et irréductibles de degré n dans $\mathbb{F}_p[T]$. Notant $\lambda_1(n, p)$ le nombre de ces derniers, on a donc

$$\lambda_1(n, p) = \frac{1}{n} \left(p^n - \sum_{m \mid n, m \neq n} p^m \right) \geq \frac{1}{n} \left(p^n - \sum_{m=0}^{n-1} p^m \right) \geq \frac{1}{n} \left(p^n - \frac{p^n}{p-1} \right) \geq \frac{p^n}{2n}$$

dès que $p \geq 3$.

Selon un raisonnement totalement analogue, le nombre $\lambda_3(n, p)$ des polynômes unitaires $f \in \mathbb{F}_p[T]$, de degré n et s'écrivant comme le produit d'un facteur linéaire et d'un facteur irréductible de degré $n - 1$ vérifie :

$$\lambda_3(n, p) \geq p \frac{p^{n-1}}{2(n-1)} = \frac{p^n}{2(n-1)}.$$

Enfin, le nombre $\lambda_2(n, p)$ de polynômes unitaires $f \in \mathbb{F}_p[T]$, de degré n et s'écrivant sous la forme $f = qa$ ou $f = qab$ avec q, a, b unitaires et irréductibles, $\deg(q) = 2$ et $\deg(a), \deg(b)$ impairs vérifie :

$$\lambda_2(n, p) \geq \frac{p^2}{4} \max \left(\frac{p^{n-2}}{2(n-2)}, \sum_{a, b \text{ impairs}, a+b=n-2} \frac{p^a p^b}{2a 2b} \right) \geq \frac{p^2}{4} \frac{p^{n-2}}{2(n-2)} = \frac{p^n}{8(n-2)}.$$

Posant $k(n) = \max(2n, 8(n-2))$, nous obtenons finalement la minoration

$$\lambda_i(n, p) \geq \frac{p^n}{k(n)}$$

pour tout $i \in \{1, 2, 3\}$ et tout nombre premier $p \geq 3$.

2. Soit $i \in \{1, 2, 3\}$. L'homomorphisme canonique $\mathbb{Z}/P\mathbb{Z} \rightarrow \prod_{i=1}^r \mathbb{Z}/p_i\mathbb{Z}$ étant un isomorphisme, tout polynôme unitaire de degré n dans $\mathbb{Z}/P\mathbb{Z}[T]$ est uniquement déterminé par ses réductions modulo les r nombres premiers p_1, \dots, p_r ; on en déduit immédiatement que le nombre de ces polynômes dont aucune des réductions modulo p_1, \dots, p_r n'est de type (i) est minoré par

$$\prod_{j=1}^r \left(p_j^n - \frac{p_j^n}{k(n)} \right) = \left(1 - \frac{1}{k(n)} \right)^r \prod_{j=1}^r p_j^n = \left(1 - \frac{1}{k(n)} \right)^r P^n.$$

3. Quel que soit l'entier naturel $N \geq 3$, il découle de l'exercice précédent que $\sigma_n(N)$ est minoré par le nombre $\sigma'_n(N)$ des polynômes unitaires et de degré n $f \in \mathbb{Z}[T]$, dont les coefficients sont majorés par N en valeur absolue et tels qu'il existe, pour tout $i \in \{1, 2, 3\}$, un nombre premier parmi $p_1, \dots, p_{r(N)}$ modulo lequel f est de type (i). Désignant par P le produit des nombres premiers $p_1, \dots, p_{r(N)}$, on a manifestement

$$\sigma'_n(N) \geq (2N+1)^n - 3 \left(1 - \frac{1}{k(n)} \right)^{r(N)} P^n \geq (2N+1)^n - 3 \left(1 - \frac{1}{k(n)} \right)^{r(N)} N^n,$$

donc

$$\frac{\sigma_n(N)}{(2N+1)^n} \geq 1 - 3 \left(1 - \frac{1}{k(n)} \right)^{r(N)} \left(\frac{N}{2N+1} \right)^n \geq 1 - 3 \left(1 - \frac{1}{k(n)} \right)^{r(N)}.$$

Comme $r(N)$ tend vers $+\infty$ avec N , on en conclut :

$$\lim_N \frac{\sigma_n(N)}{(2N+1)^n} = 1.$$
