Université Pierre et Marie Curie - Paris VI — Faculté de Mathématiques
Master Mathématiques et applications — 2017–2018

Algèbre et théorie de Galois

Examen du 12 janvier 2017. Durée 3h00.
Aucun document autorisé. Smartphones éteints.

Exercice 1. Soit $f \in \mathbb{Q}[X]$ irréductible de degré 3 et soit G_f son groupe de Galois sur $\mathbb{Q}$.

i. Montrer que G_f est isomorphe à $\mathfrak{S}_3$ (groupe symétrique) ou $\mathfrak{A}_3$ (groupe alterné).

On sait que G_f agit fidèlement sur les racines de f qui sont toutes distinctes, donc il se plonge dans $\mathfrak{S}_3$. Puisque f est irréductible, K_f contient un corps de rupture de degré 3 de f donc $3||G_f|$ (alternativement : G_f agit transitivement sur les racines), ce qui implique $G_f = \mathfrak{A}_3$ ou $\mathfrak{S}_3$.

ii. Montrer que si f a une seule racine réelle, alors G_f est isomorphe à $\mathfrak{S}_3$.

La conjugaison complexe stabilise K_f et induit donc un élément de G_f. Elle permute les deux racines non réelles de f donc c'est une transposition. En particulier $6||G_f|$ et donc $G_f = \mathfrak{S}_3$.

iii. Soit $f = X^3 - 6X + 1$. Montrer que f est irréductible sur $\mathbb{Q}$ avec 3 racines réelles mais que G_f est isomorphe à $\mathfrak{S}_3$.

Irréductibilité : 2 arguments possibles. 1) un changement de variable $X = Y - 1$ donne un polynôme Eisenstein en $p = 3$. 2) f réductible $\Rightarrow$ f a une racine dans $\mathbb{Q}$, laquelle doit être entière (Gauss) et diviser le terme constant 1, mais ni 1 ni -1 n'est racine de f.

Racines réelles : on calcule qu'il y a un maximum local positif en $-\sqrt{2}$ et un minimum local négatif en $\sqrt{2}$, d'où 3 racines réelles.

$G_f = \mathfrak{S}_3$: en réduisant modulo 2 on trouve une factorisation $\bar{f} = (X-1)(X^2+X+1)$. Or, $X^2 + X + 1$ est irréductible dans $\mathbb{F}_2[X]$, donc par spécialisation il existe un 2-cycle dans G_f, d'où $6||G_f|$ et $G_f = \mathfrak{S}_3$. [On peut aussi réduire modulo 5]. Alternativement, si on connait la formule du discriminant, on peut constater qu'il n'est pas un facteur, donc $G_f \neq \mathfrak{A}_3$.

Exercice 2 (Intégralité)**.** Soit $A \subset B$ une extension d'anneaux. On dit que $b \in B$ est "entier sur A" s'il existe un polynôme unitaire $f \in A[X]$ tel que $f(b) = 0$.

i. Montrer que $b \in B$ est entier sur A si et seulement si la sous-A-algèbre $A[b]$ de B engendrée par b est un A-module de type fini.

Si b est entier sur A, soit $f = X^n + a_1 X^{n-1} + \cdots + a_n \in A[X]$ tel que $f(b) = 0$. Alors $b^n = -a_1 b^{n-1} + \cdots + (-a_n)$. Par récurrence immédiate, on montre que $b^{n+k} \in A + Ab + \cdots + Ab^{n-1}$. Puisque $A[b]$ est engendré par les b^k, $k \in \mathbb{N}$, on a donc $A[b] = A + Ab + \cdots + Ab^{n-1}$ qui est bien de type fini comme A-module.

Si $A[b]$ est de type fini comme A-module, il admet une famille génératrice de la forme $f_1(b), \cdots, f_r(b)$ pour des polynômes $f_1, \cdots, f_r \in A[X]$. En particulier, si $n \in \mathbb{N}$ il existe des éléments $a_1, \cdots, a_r$ de A tels que $b^n = a_1 f_1(b) + \cdots + a_r f_r(b)$. En choisissant $n > \max_i(\deg(f_i))$, on obtient un polynôme unitaire $X^n - a_1 f_1 - \cdots - a_r f_r$ annulant b.

TSVP

ii. Soient $b, b' \in B$ entiers sur A. Montrer que la sous-A-algèbre $A[b, b']$ engendrée par b et b' est un A-module de type fini.

Soient $f, f' \in A[X]$ unitaires de degrés respectifs n et n' et tels que $f(b) = f'(b') = 0$. Alors $A[b, b']$ est engendré par les $b^i b'^j$ pour $i, j \in \mathbb{N}$. Mais puisque $b^i \in A + Ab + \cdots + Ab^{n-1}$ et $b'^j \in A + Ab' + \cdots + Ab'^{n'-1}$ pour tous i, j, la famille finie des $b^i b'^j$, pour $0 \leqslant i < n$ et $0 \leqslant j < n'$ est aussi génératrice.

iii. Supposons A noethérien. Montrer que l'ensemble des $b \in B$ entiers sur A est une sous-A-algèbre de B.

Soient b, b' entiers. D'après ii), la A-algèbre $A[b, b']$ est de type fini comme A-module. Puisque A est noethérien, les sous A-algèbres $A[b + b']$ et $A[bb']$ de $A[b + b']$ sont aussi des A-modules de type fini donc, par i), $b + b'$ et bb' sont entiers. Comme par ailleurs tout $a \in A$ est évidemment entier sur A, on conclut.

iv. Supposons A factoriel et $B = \mathrm{Frac}(A)$. Montrer que tout b entier sur A est dans A.

Supposons $b^n = a_1 b^{n-1} + \cdots + a_n$ Deux arguments sont possibles (au moins). 1) on utilise les valuations. Soit p irréductible de A. Sa valuation ν_p est multiplicative (A factoriel) donc on a $n\nu_p(b) \geqslant \min(\nu_p(a_i) + (n - i)\nu_p(b))$ et en particulier il existe $i \neq 0$ tel que $i\nu_p(b) \geqslant \nu_p(a_i) \geqslant 0$, donc $\nu_p(b) \geqslant 0$. Ceci étant vrai pour tout p irréductible dans A factoriel, un résultat du cours assure que $b \in A$. 2) on peut écrire $b = p/q$ avec p et q sans diviseurs irréductibles communs et constater que $q|p^n$. Par factorialité, q divise p donc est une unité et $b \in A$.

Exercice 3 (Polynômes symétriques)**.** On fixe un entier $n > 1$, on note $A = \mathbb{Z}[X_1, \cdots, X_n]$ et $\mathfrak{S}_n$ le groupe des permutations de l'ensemble $\{1, \cdots, n\}$..

i. Pour $\sigma \in \mathfrak{S}_n$, justifier l'existence d'un unique automorphisme d'anneaux $\tilde{\sigma}$ de A tel que $\tilde{\sigma}(X_i) = X_{\sigma(i)}$ pour tout $i = 1, \cdots, n$. Puis montrer que cela définit une action de $\mathfrak{S}_n$ sur A par automorphismes d'anneaux, et que celle-ci se prolonge en une action sur $K = \mathbb{Q}(X_1, \cdots, X_n)$ par automorphismes de corps.

La propriété universelle des anneaux de polynômes assure l'existence et l'unicité d'un endomorphisme $\widetilde{\sigma}$ de l'anneau A tel que $\widetilde{\sigma}(X_i) = X_{\sigma(i)}$. L'unicité de $\widetilde{\sigma}$ nous assure que $\widetilde{\sigma\sigma'} = \widetilde{\sigma} \circ \widetilde{\sigma'}$, et en particulier $\widetilde{\sigma} \circ \widetilde{\sigma^{-1}} = \mathrm{id}$ de sorte que $\widetilde{\sigma}$ est bien un automorphisme d'anneaux, et que $\sigma \mapsto \widetilde{\sigma}$ définit bien une action. Puisque $K = \mathrm{Frac}(A)$, la propriété universelle du localisé assure que $\widetilde{\sigma}$ se prolonge en un endomorphisme de l'anneau K, et l'unicité de ce prolongement assure encore que l'on obtient une action par automorphismes d'anneaux (et donc de corps).

ii. Considérons le polynôme $f = (T - X_1) \cdots (T - X_n) \in A[T]$ et développons-le sous la forme $f = T^n - \Sigma_1 T^{n-1} + \cdots + (-1)^n \Sigma_n$ avec $\Sigma_i \in A$. Montrer que les Σ_i sont invariants par $\mathfrak{S}_n$ et en donner une formule explicite comme polynômes en les X_i.

On prolonge l'action de $\mathfrak{S}_n$ sur A en une action sur $A[T]$ en posant $\widetilde{\sigma}(T) = T$. On constate alors que $\widetilde{\sigma}(f) = (T - X_{\sigma(1)}) \cdots (T - X_{\sigma(n)}) = (T - X_1) \cdots (T - X_n) = f$ pour tout $\sigma \in \mathfrak{S}_n$. Donc f est invariant sous $\mathfrak{S}_n$, et donc ses coefficients dans A sont aussi invariants sous $\mathfrak{S}_n$. On peut énoncer (et éventuellement prouver par une récurrence immédiate) la formule $\Sigma_k = \sum_{J \subset \{1, \cdots, n\}, |J| = k} \prod_{j \in J} X_j$.

iii. Notons $K^{\mathfrak{S}_n}$ le sous-corps des invariants de K sous $\mathfrak{S}_n$ et $k := \mathbb{Q}(\Sigma_1, \cdots, \Sigma_n)$ le sous-corps de K engendré par les Σ_i. On a donc $k \subset K^{\mathfrak{S}_n}$.

(a) Rappeler pourquoi $[K : K^{\mathfrak{S}_n}] \geqslant n!$.

D'après le cours, on sait que $|\mathrm{Aut}_{K^{\mathfrak{S}_n}-alg}(K)| \leqslant [K : K^{\mathfrak{S}_n}]$. Or, l'action de $\mathfrak{S}_n$ sur K est $K^{\mathfrak{S}_n}$-linéaire donc est donnée par un morphisme $\mathfrak{S}_n \longrightarrow \mathrm{Aut}_{K^{\mathfrak{S}_n}-alg}(K)$, lequel est injectif (puisque $\mathfrak{S}_n$ agit fidèlement sur les X_i). D'où $[K : K^{\mathfrak{S}_n}] \geqslant n!$.

(b) Montrer que K est un corps de décomposition de f sur k et en déduire que $[K : k] \leqslant n!$.

Le polynôme $f \in k[T]$ est scindé dans $K[T]$ de racines les X_i, lesquelles engendrent K comme extension de $\mathbb{Q}$, donc a fortiori comme extension de k. Donc K est bien un corps de décomposition de f sur k. On peut en déduire l'inégalité voulue de deux manières : 1) en remarquant qu'elle découle de la construction d'un corps de décomposition par itération de corps de rupture. 2) en remarquant que K/k est Galoisienne et que son degré est le cardinal du groupe de Galois qui agit fidèlement sur les n racines.

(c) Conclure que $k = K^{\mathfrak{S}_n}$ et que les Σ_i sont algébriquement indépendants sur $\mathbb{Q}$.

On a $k \subset K^{\mathfrak{S}_n}$ et les deux inégalités précédentes montrent que $[K^{\mathfrak{S}_n} : k] = 1$ donc $k = K^{\mathfrak{S}_n}$. Puisque K est finie, donc algébrique, sur k, ces deux corps ont même degré de transcendance sur $\mathbb{Q}$, à savoir n. Or k est engendrée comme extension de $\mathbb{Q}$ par les n éléments Σ_i. Si ceux-ci étaient algébriquements liés, k serait une extension algébrique de l'extension engendrée par une sous-famille à $n-1$ éléments de $\{\Sigma_1, \cdots, \Sigma_n\}$ (cf résultat du cours) donc aurait un degré de transcendance $< n$, ce qui n'est pas le cas.

iv. Notons $A^{\mathfrak{S}_n}$ le sous-anneau des invariants de A sous $\mathfrak{S}_n$ et $B := \mathbb{Z}[\Sigma_1, \cdots, \Sigma_n]$ le sous-anneau de A engendré par les Σ_i.

(a) Montrer que tout élément de A est entier sur B (cf exercice 2).

Puisque les X_i sont annulés par le polynôme unitaire $f \in B[T]$, ils sont entiers sur B. Donc la B-algèbre qu'ils engendrent est formée d'éléments entiers sur A d'après le iii) de l'exercice 2. Mais cette B-algèbre n'est autre que A.

(b) Justifier que B est factoriel, puis montrer que $B = A^{\mathfrak{S}_n}$.

Puisque les Σ_i sont algébriquement indépendants, B est isomorphe à une algèbre de polynômes sur $\mathbb{Z}$ donc est factoriel d'après le cours. Mais alors, d'après le iv) de l'exercice 2, tout élément de $\mathrm{Frac}(B) = k$ entier sur B est dans B. Or $A^{\mathfrak{S}_n} \subset K^{\mathfrak{S}_n} = k$ est formée d'éléments entiers sur b. Donc $A^{\mathfrak{S}_n} \subset B$. L'autre inclusion est immédiate.

On a donc montré le théorème suivant : les Σ_i sont algébriquement indépendants sur $\mathbb{Z}$ et on a $\mathbb{Z}[X_1, \cdots, X_n]^{\mathfrak{S}_n} = \mathbb{Z}[\Sigma_1, \cdots, \Sigma_n]$

Exercice 4. Soient K_1, K_2 deux extensions Galoisiennes de $\mathbb{Q}$ contenues dans $\overline{\mathbb{Q}}$, et soit K la sous-extension de $\overline{\mathbb{Q}}$ engendrée par K_1 et K_2.

TSVP

i. Montrer que K est Galoisienne sur $\mathbb{Q}$.

Si K_i est le corps de décomposition de $f_i \in \mathbb{Q}[X]$, alors K est celui de $f_1 f_2$ donc est normale. Elle est aussi séparable (caractéristique 0 par exemple).

ii. Montrer que si $[K_1 : \mathbb{Q}]$ et $[K_2 : \mathbb{Q}]$ sont premiers entre eux, alors $[K : K_1] = [K_2 : \mathbb{Q}]$ et $[K : K_2] = [K_1 : \mathbb{Q}]$.

Les égalités $[K : \mathbb{Q}] = [K : K_i][K_i : \mathbb{Q}]$ pour $i = 1, 2$ montrent grâce au lemme de Gauss que $[K_j : \mathbb{Q}]$ divise $[K : K_i]$ pour $\{i, j\} = \{1, 2\}$. Par ailleurs, si α_i est un élément primitif pour $K_i/\mathbb{Q}$ alors $K = K_j(\alpha_i)$ donc, puisque le polynôme minimal de α_i sur K_j divise celui sur $\mathbb{Q}$, on a $[K : K_j] \leqslant [K_i : \mathbb{Q}]$. D'où les égalités annoncées.

iii. Sous la même hypothèse, montrer que les applications de restriction induisent des isomorphismes $\mathrm{Gal}(K/K_1) \xrightarrow{\sim} \mathrm{Gal}(K_2/\mathbb{Q})$ et $\mathrm{Gal}(K/K_2) \xrightarrow{\sim} \mathrm{Gal}(K_1/\mathbb{Q})$, et aussi que $\mathrm{Gal}(K/\mathbb{Q}) = \mathrm{Gal}(K/K_1) \times \mathrm{Gal}(K/K_2)$.

L'application de restriction $\mathrm{Gal}(K/K_i) \xrightarrow{\sim} \mathrm{Gal}(K_j/\mathbb{Q})$ est bien définie puisque K_j est normale, et c'est manifestement un morphisme de groupes. Ce morphisme est injectif car tout automorphisme trivial sur K_1 et K_2 est l'identité. Donc par cardinalité il est bijectif. Par ailleurs, les deux sous-groupes $\mathrm{Gal}(K/K_i)$ sont distingués et d'intersection triviale (puisque d'ordres premiers entre eux) et on a vu que $[K : \mathbb{Q}] = [K : K_1][K : K_2]$. Il s'ensuit que $\mathrm{Gal}(K/\mathbb{Q}) = \mathrm{Gal}(K/K_1) \times \mathrm{Gal}(K/K_2)$.