Université P. et M. Curie (Paris VI),
Deuxième semestre 2006/2007

Michel Waldschmidt
date de mise à jour: 15/02/2007

Master de sciences et technologies 1ère année -
Spécialité : Mathématiques Fondamentales

Mention : Mathématiques et applications
MO11 : Théorie des nombres (12 ECTS)

Première partie: Théorie des Corps

Fascicule 3 : Chapitre 1 (fin), section 1.9 (9 pages) [1]

1.9 Théorie de Galois : quelques exemples

1.9.1 Constructions à la règle et au compas

Les trois questions classiques posées par les géomètres grecs sur les constructions à la règle et au compas sont les suivantes : peut-on construire, en utilisant uniquement ces deux instruments,
• (*Duplication du cube*) un cube ayant un volume double d'un cube donné ?
• (*Trisection d'un angle*) un angle égal au tiers d'un angle donné ?
• (*Quadrature du cercle*) un carré ayant une aire égale à celle d'un disque donné ?

Ces questions reviennent à construire respectivement la racine cubique d'un nombre donné, le cosinus du tiers d'un angle dont le cosinus est donné, le nombre π.

En termes algébriques on considère le plan cartésien $\mathbf{R}^2$ avec l'unité de longueur donnée par la distance entre $(0,0)$ et $(0,1)$ et à partir de ces deux points on itère les constructions suivantes, dont la réunion produit l'ensemble des *points constructibles* :
– On peut construire la droite qui passe par deux points donnés.
– On peut construire un cercle de rayon donné et de centre préalablement construit.
– À chaque étape on peut ajouter à l'ensemble déjà construit l'intersection de deux droites, de deux cercles, d'une droite et d'un cercle, chacune de ces lignes ayant été précédemment construites.

Un nombre réel est dit *constructible* si le point $(x,0)$ est constructible à la règle et au compas à partir de $(0,0)$ et $(0,1)$.

Des constructions géométriques classiques montrent que les nombres constructibles forment un sous-corps de $\mathbf{R}$ et que si x est constructible, alors $\sqrt{x}$ l'est aussi. Les images suivantes sont extraites de [1] § 13.3.

[1] Ce texte est téléchargeable à partir de la page http ://www.math.jussieu.fr/∼miw/enseignement.html

It is an elementary fact from geometry that if two lengths a and b are given one may construct using straightedge and compass the lengths $a \pm b$, ab and a/b (the first two are clear and the latter two are given by the construction of parallel lines (Figure 1)).

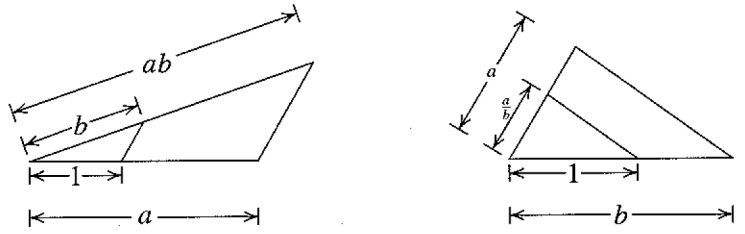

Fig. 1

It is also an elementary geometry construction to construct $\sqrt{a}$ if a is given: construct the circle with diameter $1 + a$ and erect the perpendicular to the diameter as indicated in Figure 2. Then $\sqrt{a}$ is the length of this perpendicular.

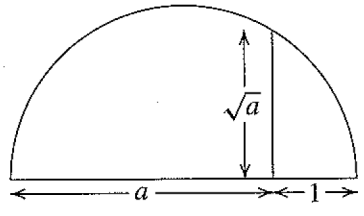

Fig. 2

L'énoncé suivant est facile à démontrer (voir par exemple [1] § 13.3).

Proposition 1.34. *Soit x un nombre réel. Les assertions suivantes sont équivalentes :*
- *x est constructible.*
- *x est algébrique sur $\mathbf{Q}$ et son corps de décomposition sur $\mathbf{Q}$ a pour degré une puissance de 2.*
- *x appartient à un corps de nombres galoisien sur $\mathbf{Q}$ de degré une puissance de 2.*

Comme $\sqrt[3]{2}$ est de degré 3 sur $\mathbf{Q}$, on en déduit l'impossibilité de la duplication du cube.

Il existe des angles dont on peut construire le tiers à la règle et au compas (par exemple π), mais il en existe aussi pour lesquels une telle construction est impossible. Un exemple est $\pi/3$. On a $\cos(\pi/3) = -1/2$ et la formule

$$\cos\theta = 4\cos^3(\theta/3) - 3\cos(\theta/3)$$

montre que le nombre $\beta = 2\cos(\pi/9) = 1,87938\ldots$ est racine du polynôme $X^3 - 3X + 1$. Ce polynôme est irréductible sur $\mathbf{Q}$. Donc β est de degré 3 sur $\mathbf{Q}$, par conséquent il n'est pas constructible.

Pour la quadrature du cercle, l'impossibilité vient de la transcendance du nombre π que nous ne démontrons pas ici (une démonstration est donnée dans l'Annexe A du livre de Lang *Algèbre* [4]).

Un nombre complexe est dit *exprimable par radicaux* s'il existe un corps de nombres K le contenant, une tour de corps

$$\mathbf{Q} = K_0 \subset K_1 \subset \cdots \subset K_{s-1} \subset K_s = K,$$

et, pour $1 \leq i \leq s$, un entier $n_i \geq 1$ et un élément $\alpha_i \in K_i$ tels que $K_i = K_{i-1}(\alpha_i)$ avec $\alpha_i^{n_i} \in K_{i-1}$.

On pose $a_i = \alpha_i^{n_i}$ et on écrit $\alpha_i = \sqrt[n_i]{a_i}$ (avec un léger abus de notation : il y a plusieurs racines n_i-ièmes de α_i, mais le corps engendré ne dépend pas de ce choix lorsque les racines n_i-ièmes appartiennent au corps de base, ce qui est une hypothèse licite ici) et donc $K_i = K_{i-1}(\sqrt[n_i]{a_i})$.

Soit K un corps de caractéristique nulle. On définit le *groupe de Galois d'un polynôme séparable* $f \in K[X]$ comme le groupe de Galois d'un corps de décomposition de f sur K.

Un polynôme est *résoluble par radicaux* si toutes ses racines sont exprimables par radicaux.

D'autre part un groupe fini G est *résoluble* s'il existe une suite de sous-groupes

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_{s-1} \subset G_s$$

dans laquelle chaque G_i est un sous-groupe normal de G_{i+1} avec un quotient G_{i+1}/G_i cyclique $(0 \leq i \leq s-1)$.

Le théorème de Galois 1.33 permet de démontrer l'énoncé suivant (voir par exemple [1] § 14.7 Th. 39).

Théorème 1.35. *Un polynôme f est résoluble par radicaux si et seulement si son groupe de Galois est résoluble.*

Soit n un entier ≥ 5. Il est connu que le groupe $\mathfrak{S}_n$ n'est pas résoluble et qu'il existe des corps de nombres galoisiens sur $\mathbf{Q}$ de groupe de Galois $\mathfrak{S}_n$. Un tel corps est le corps de décomposition d'un polynôme qui n'est donc pas résoluble par radicaux.

Par exemple le polynôme $X^5 - 6X + 3$ a pour groupe de Galois sur $\mathbf{Q}$ le groupe symétrique $\mathfrak{S}_5$ d'ordre $5! = 120$, il n'est donc pas résoluble par radicaux.

L'outil essentiel pour la démonstration du théorème 1.35 est un théorème dû à Kummer dont nous donnons seulement l'énoncé :

Théorème 1.36. *Soient L/K une extension et n un entier positif qui n'est pas divisible par la caractéristique de K. On suppose que K contient les racines n-ièmes de l'unité. Alors l'extension est cyclique si et seulement s'il existe $\alpha \in L$ tel que $L = K(\alpha)$ et $\alpha^n \in K$.*

1.9.2 Corps cyclotomiques

Soit n un entier positif. Le corps cyclotomique E_n d'indice n est le corps de décomposition sur $\mathbf{Q}$ du polynôme $X^n - 1$. C'est aussi le corps de rupture du polynôme cyclotomique Φ_n sur $\mathbf{Q}$. Notons ζ_n une racine primitive n-ième de l'unité, de sorte que $E_n = \mathbf{Q}(\zeta_n)$.

Nous avons vu (Proposition 1.28) que E_n est une extension galoisienne de $\mathbf{Q}$ de groupe de Galois $(\mathbf{Z}/n\mathbf{Z})^\times$.

Supposons n premier et notons $n = p$, $E_p = E$, $\zeta_p = \zeta$. Le groupe des éléments inversibles du corps $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ est cyclique, donc l'extension $E/\mathbf{Q}$ est cyclique de groupe de Galois $G \simeq (\mathbf{Z}/p\mathbf{Z})^\times$ d'ordre $p-1$. Si k est un entier premier à p, notons σ_k l'automorphisme de E déterminé par $\sigma_k(\zeta) = \zeta^k$.

Lemme 1.37. *L'ordre de σ_k dans G est égal à l'ordre de la classe de k modulo p.*

Démonstration. Pour $h \geq 1$ on a $\zeta^h = 1$ si et seulement si p divise h. Donc pour $n \geq 1$ on a $\zeta^n = \zeta$ si et seulement si $n \equiv 1 \pmod{p}$. D'autre part $\sigma_k^m(\zeta) = \zeta^{k^m}$. Donc l'ordre de σ_k dans G est le plus petit entier m tel que $k^m \equiv 1 \pmod{p}$, c'est l'ordre de la classe de k dans $(\mathbf{Z}/p\mathbf{Z})^\times$. □

Une base sur $\mathbf{Q}$ de E est $\{1, \zeta, \zeta^2, \ldots, \zeta^{p-2}\}$ puisque ζ est de degré $p-1$ sur $\mathbf{Q}$, racine du polynôme

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

On préfère d'utiliser comme base $\{\zeta, \zeta^2, \ldots, \zeta^{p-2}, \zeta^{p-1}\}$ car ce sont précisément les racines primitives p-ièmes de l'unité, qui sont donc permutés par les σ_k.

Soit H un sous-groupe de G. Posons

$$\alpha_H = \sum_{\sigma \in H} \sigma(\zeta).$$

On vérifie facilement que $\mathbf{Q}(\alpha_H)$ est le sous-corps E^H de E fixé par H.

Par exemple pour $p = 7$ le groupe G est cyclique d'ordre 6, il est engendré par σ_3 :

$$G = \{1,\ \sigma_3,\ \sigma_3^2 = \sigma_2,\ \sigma_3^3 = \sigma_6,\ \sigma_3^4 = \sigma_4,\ \sigma_3^5 = \sigma_5\},$$

ce qui correspond au fait que $(\mathbf{Z}/7\mathbf{Z})^\times$ est engendré par 3 (on dit que 3 est une *racine primitive modulo* 7) :

$$(\mathbf{Z}/7\mathbf{Z})^\times = \{1,\ 3,\ 3^2 \equiv 2,\ 3^3 \equiv 6,\ 3^4 \equiv 4,\ 3^5 \equiv 5\}.$$

Le groupe G a quatre sous-groupes, deux triviaux $\{1\}$ et G d'ordres 1 et 6 respectivement, et deux non triviaux $\{1, \sigma_6\}$ et $\{1, \sigma_2, \sigma_4\}$. Le seul élément d'ordre 2 dans G est σ_6 qui est la restriction à E de la conjugaison complexe, puisque $\sigma_6(\zeta) = \zeta^{-1} = \overline{\zeta}$. Le sous corps fixé par la conjugaison complexe est le sous-corps réel maximal M de E, il est engendré sur $\mathbf{Q}$ par $\alpha = \zeta + \overline{\zeta}$, comme nous l'avons déjà vu au § 1.7 comme exemple d'application de la proposition 1.28. Le corps $M = \mathbf{Q}(\alpha)$ est cubique cyclique sur $\mathbf{Q}$, le groupe de Galois est engendré par la restriction de σ_2 à M : les conjuqués de α sur $\mathbf{Q}$ sont

$$\alpha_1 = \alpha, \quad \alpha_2 = \sigma_2(\alpha) = \zeta^2 + \zeta^5 = \zeta^2 + \overline{\zeta}^2, \quad \alpha_3 = \sigma_2^2(\alpha) = \zeta^4 + \zeta^3 = \zeta^3 + \overline{\zeta}^3.$$

On trouve le polynôme irréductible de α sur $\mathbf{Q}$ en calculant (facilement) $\alpha_1 + \alpha_2 + \alpha_3 = -1$, $\alpha_1\alpha_2\alpha_3 = 1$ et (un peu moins facilement) $\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 = -2$. Le polynôme cherché est donc $X^3 + X^2 - 2X - 1$.

Il reste un dernier sous-corps N de E dont nous n'avons pas encore parlé, c'est le sous-corps fixé par le sous-groupe d'ordre 3 (et d'indice 2) de G. Donc N est l'unique sous-corps quadratique de E, engendré sur $\mathbf{Q}$ par

$$\beta = \zeta + \sigma_2(\zeta) + \sigma_4(\zeta) = \zeta + \zeta^2 + \zeta^4.$$

Le conjugué de β est

$$\beta^* = \tau(\beta) = \sigma_3(\beta) = \zeta^3 + \zeta^6 + \zeta^5.$$

On vérifie facilement $\beta + \beta^* = -1$, $\beta\beta^* = 2$, donc β est racine du polynôme quadratique $X^2 + X + 2$ dont le discriminant est -7. Ainsi l'unique sous-corps quadratique de L est $\mathbf{Q}(\sqrt{-7})$.

De façon générale, il résulte de la proposition 1.44 ci-dessous que *l'unique sous-corps quadratique de* $\mathbf{Q}(\zeta_p)$ *pour* p *premier est le corps* $\mathbf{Q}(\sqrt{\epsilon p})$, *où* $\epsilon = 1$ *si* $p \equiv 1 \pmod{4}$ *et* $\epsilon = -1$ *si* $p \equiv 3 \pmod{4}$ (voir aussi [1] § 14.5).

Soit $n = p_1^{a_1} \cdots p_k^{a_k}$ la décomposition en facteurs premiers d'un entier $n \geq 2$. La décomposition du groupe multiplicatif $(\mathbf{Z}/n\mathbf{Z})^\times$ par le théorème chinois :

$$(\mathbf{Z}/n\mathbf{Z})^\times \simeq (\mathbf{Z}/p_1^{a_1}\mathbf{Z})^\times \times \cdots \times (\mathbf{Z}/p_k^{a_k}\mathbf{Z})^\times$$

permet de déduire du théorème 1.28 l'énoncé suivant :

Corollaire 1.38. *Soit $n = p_1^{a_1} \cdots p_k^{a_k}$ un entier ≥ 2 décomposé en facteurs premiers. Notons E_n le corps cyclotomique $\mathbf{Q}(\zeta_n)$ d'indice n et F_i le corps cyclotomique $E_{p_i^{a_i}} = \mathbf{Q}(\zeta_{p_i^{a_i}})$ d'indice $p_i^{a_i}$. Alors*

$$\mathrm{Gal}(E_n/\mathbf{Q}) \simeq \mathrm{Gal}(F_1/\mathbf{Q}) \times \cdots \times \mathrm{Gal}(F_k/\mathbf{Q}).$$

On en déduit qu'un polygone régulier à n côtés peut être construit à la règle et au compas si et seulement si $\varphi(n)$ est une puissance de 2.

Pour un nombre premier p, dire que $\varphi(p) = p-1$ est une puissance de 2 revient à dire que p est de la forme $2^m + 1$. Il est facile de voir que dans ce cas l'exposant m est lui même une puissance de 2 : quand k est impair, l'identité $x^k + 1 = (x+1)(x^{k-1} - x^{k-2} + \cdots + x^2 - x + 1$ montre que $x^k + 1$ est divisible par $x + 1$.

On appelle *nombre premier de Fermat* tout nombre premier de la forme $F_s = 2^{2^s} + 1$ avec s entier ≥ 0. Les nombres

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65\,537$$

sont des nombres premiers de Fermat. On ignore s'il y en a d'autres (on s'attend à ce que leur nombre soit fini mais on ne le sait pas). Que $F_5 = 2^{2^5} + 1$ ne soit pas un nombre premier a été découvert par Euler. On peut le vérifier ainsi.

Lemme 1.39. *Le nombre $F_5 = 2^{32} + 1$ est divisible par* 641.

Démonstration. (D'après [3], § 2.5). On écrit

$$641 = 625 + 16 = 5^4 + 2^4 \quad \text{et} \quad 641 = 5 \cdot 128 + 1 = 5 \cdot 2^7 + 1.$$

L'identité $x^4 - 1 = (x+1)(x-1)(x^2+1)$ montre que $x^4 - 1$ est divisible par $x+1$, donc $5^4 \cdot 2^{28} - 1$ est divisible par 641. Mais 641 divise aussi $5^4 \cdot 2^{28} + 2^{32}$, donc il divise la différence $2^{32} + 1$. □

Le résultat que fournit le théorème de Galois 1.33 est le suivant :

Proposition 1.40. *Soit n un entier ≥ 3. Un polygone régulier peut être construit à la règle et au compas si et seulement si n est de la forme $2^k p_1 \cdots p_r$ où k est un entier ≥ 0 et $p_1, \ldots, p_r$ des nombres premiers de Fermat deux-à-deux distincts.*

On trouvera dans [1] § 14.5 d'autres informations sur ce thème, notamment une construction géométrique du polygone régulier à 17 côtés due à J.H. Conway (voir aussi [2]).

1.9.3 Résolution par radicaux

Soit $f \in K[X]$ un polynôme séparable de degré n à coefficient dans un corps K. Le groupe de Galois de f sur K a été défini (§ 1.9.1) comme le groupe de Galois $G = \mathrm{Gal}(L/K)$ du corps de décomposition L de f sur K. Ce groupe de Galois agit sur l'ensemble E des racines de f par permutation, donc s'injecte dans le groupe symétrique $\mathfrak{S}_n$.

Si f est produit de polynômes irréductibles $f = f_1 \cdots f_k$ dans $K[X]$ et si n_i désigne le degré de f_i, alors le groupe de Galois s'injecte dans le produit $\mathfrak{S}_{n_1} \times \cdots \times \mathfrak{S}_{n_k}$.

Si f est irréductible sur K, alors G agit sur E de façon *transitive* : pour tout α et β dans E il existe $\sigma \in G$ tel que $\sigma(\alpha) = \beta$.

Nous allons donner un sens précis à l'affirmation suivante :

• *Le groupe de Galois d'un polynôme "générique" de degré n est le groupe symétrique $\mathfrak{S}_n$.*

On désigne par L le corps $\mathbf{Q}(x_1, \ldots, x_n)$ des fractions rationnelles en n indéterminées sur $\mathbf{Q}$ (on peut remplacer le corps de base $\mathbf{Q}$ par un corps de caractéristique nulle, mais cela en fait n'ajoute rien). On définit les *fonctions symétriques élémentaires* $s_1, \ldots, s_n \in \mathbf{Q}[x_1, \ldots, x_n]$ par la relation

$$(X - x_1)(X - x_2) \cdots (X - x_n) = X^n - s_1 X^{n-1} + s_2 X^{n-2} - \cdots + (-1)^n s_n.$$

On a par exemple

$$s_1 = x_1 + \cdots + x_n, \quad s_n = x_1 \cdots x_n$$

et

$$s_2 = x_1x_2 + x_1x_3 + \cdots + x_1x_n + x_2x_3 + \cdots + x_2x_n + \cdots + x_{n-1}x_n.$$

Plus généralement, pour $1 \leq k \leq n$, la k-ième fonction symétrique élémentaire en n variables est

$$s_k = \sum_{i_1 < i_2 < \cdots < i_k} x_{i_1} x_{i_2} \cdots x_{i_k}.$$

Le *polynôme général de degré n* est le polynôme $f(X) = (X - x_1)(X - x_2) \cdots (X - x_n)$. On note encore K le corps $\mathbf{Q}(s_1, \ldots, s_n)$, qui est un sous-corps de L. Le polynôme f a ses coefficients dans K et son corps de décomposition sur K est L. Comme f est de degré n le groupe de Galois de L sur K est (isomorphe à) un sous-groupe de $\mathfrak{S}_n$. En particulier on a $[L : K] \leq n!$.

Toute permutation de $\{1, \ldots, n\}$ induit un automorphisme de L qui laisse invariant chacun des s_k $(1 \leq k \leq n)$. Donc K est contenu dans le sous-corps $L^{\mathfrak{S}_n}$ de L fixé par $\mathfrak{S}_n$. Par le théorème de Galois 1.33, l'extension $L/L^{\mathfrak{S}_n}$ est de degré $n!$ On en déduit $K = L^{\mathfrak{S}_n}$. Il en résulte que L est une extension de K de degré $n!$ et de groupe de Galois $\mathfrak{S}_n$.

Une fonction rationnelle $F(x_1, \ldots, x_n) \in L$ est appelée *symétrique* si elle est invariante sous l'action de $\mathfrak{S}_n$. Nous avons ainsi démontré :

Proposition 1.41. *Une fraction rationnelle $F(x_1, \ldots, x_n) \in \mathbf{Q}(x_1, \ldots, x_n)$ est symétrique si et seulement s'il existe une fraction rationnelle G en n indéterminées telle que*

$$F(x_1, \ldots, x_n) = G(s_1, \ldots, s_n).$$

La fraction rationnelle G est unique. Si F est un polynôme, alors G est aussi un polynôme : un algorithme pour calculer G est donné dans l'exercice 37 du § 14.6 de [1]. L'idée consiste à considérer le monome $Ax_1^{a_1} \cdots x_n^{a_n}$ de F qui est dominant pour l'ordre lexicographique et à soustraire $As_1^{a_1 - a_2} s_2^{a_2 - a_3} \cdots s_n^{a_n}$.

Pour revenir à notre affirmation sur les polynômes "génériques", on part d'un polynôme unitaire f de degré n dont les coefficients sont des indéterminées ; on l'écrit

$$f(X) = X^n - s_1 X^{n-1} + s_2 X^{n-2} - \cdots + (-1)^n s_n. \tag{1.42}$$

On désigne par K le corps des fractions rationnelles $\mathbf{Q}(s_1, \ldots, s_n)$ en n indéterminées sur $\mathbf{Q}$, par L un corps de décomposition de f sur K et par $x_1, \ldots, x_n$ les racines de f dans L. Ainsi $L = K(x_1, \ldots, x_n)$. Vérifions que les x_i sont *algébriquement indépendants sur* $\mathbf{Q}$, c'est-à-dire que si $p \in \mathbf{Q}[X_1, \ldots, X_n]$ est un polynôme non nul, alors $p(x_1, \ldots, x_n) \neq 0$. Sinon le produit

$$P(X_1, \ldots, X_n) = \prod_{\sigma \in \mathfrak{S}_n} p(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$$

serait un polynôme non nul symétrique qui s'annule en $(x_1, \ldots, x_n)$, ce qui fournirait une relation de dépendance algébrique non triviale entre $s_1, \ldots, s_n$. On en déduit :

Théorème 1.43. *Si $s_1, \ldots, s_n$ sont des indéterminées sur $\mathbf{Q}$, le polynôme générique (1.42) est séparable et a pour groupe de Galois $\mathfrak{S}_n$ sur le corps $\mathbf{Q}(s_1, \ldots, s_n)$.*

Un exemple de polynôme symétrique est donné par le *discriminant*.

Définition. Soient L un corps et $x_1, \ldots, x_n$ des éléments de L. On définit le *discriminant* de $(x_1, \ldots, x_n)$ par

$$D = \prod_{1 \leq i < j \leq n} (x_i - x_j)^2 = (-1)^{n(n-1)/2} \prod_{1 \leq i \neq j \leq n} (x_i - x_j).$$

Le *discriminant générique* est celui pour lequel $x_1, \ldots, x_n$ sont des indéterminées et $L = \mathbf{Q}(x_1, \ldots, x_n)$. C'est un polynôme symétrique, donc d'après la proposition 1.41 il s'exprime comme un polynôme en les fonctions symétriques élémentaires $s_1, \ldots, s_n$. Une des deux racines carrées de D est

$$\sqrt{D} = \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

Le corps quadratique engendré par $\sqrt{D}$ sur $\mathbf{Q}$ est le sous-corps fixé par le groupe alterné $\mathfrak{A}_n$ de $\mathfrak{S}_n$.

On définit aussi le discriminant d'un polynôme unitaire $f \in K[X]$ en considérant un corps de décomposition L de f sur K : dans $L[X]$ ce polynôme se factorise complètement

$$f(X) = (X - \alpha_1) \cdots (X - \alpha_n)$$

et le discriminant de f est défini comme le discriminant de $(\alpha_1, \ldots, \alpha_n)$. D'après ce qui précède il appartient à K.

Le groupe de Galois G d'un polynôme irréductible f de degré n sur $\mathbf{Q}$ est un sous-groupe de $\mathfrak{S}_n$; on obtient un tel isomorphisme en numérotant les racines de f dans L et en considérant G comme un groupe de permutation de ces racines. Alors G est un sous-groupe de $\mathfrak{A}_n$ si et seulement si le discriminant D de f est un carré dans $\mathbf{Q}$.

Le discriminant d'un polynôme quadratique $X^2 + aX + b$ est $a^2 - 4b$, celui d'un polynôme cubique $X^3 + pX + q$ est $-4p^3 - 27q^2$. Un polynôme irréductible de degré 3 a pour groupe de Galois sur $\mathbf{Q}$ le groupe cyclique d'ordre 3 (qui n'est autre que le groupe alterné $\mathfrak{A}_3$) si le discriminant est

un carré dans $\mathbf{Q}$, c'est le groupe symétrique $\mathfrak{S}_3$ (groupe non commutatif d'ordre 6) sinon. Cela permet de distinguer les polynômes cubiques dont un corps de rupture est galoisien des autres.

Voici une méthode pour calculer un discriminant. Soit L un corps, soient $x_1, \ldots, x_n$ des éléments de L et soit D leur discriminant. Considérons le polynôme

$$P(X) = \prod_{i=1}^{n} (X - x_i).$$

Sa dérivée est

$$P('X) = \sum_{i=1}^{n} \prod_{\substack{1 \leq j \leq n \\ j \neq i}} (X - x_j).$$

Ainsi pour $1 \leq i \leq n$ on a

$$P'(\alpha_i) = \prod_{\substack{1 \leq j \leq n \\ j \neq i}} (x_i - x_j).$$

Par conséquent

$$\prod_{i=1}^{n} P'(\alpha_i) = (-1)^{n(n-1)/2} D.$$

Comme exemple nous utilisons cet argument pour calculer le discriminant des polynômes cyclotomiques d'indice un nombre premier ([2] Chap. 10, § 10.5, Exemple 10.12).

Proposition 1.44. *Soit p un nombre premier impair. Le discriminant du polynôme cyclotomique Φ_p d'indice p est*

$$(-1)^{(p-1)/2} p^{p-2}.$$

Démonstration. On utilise ce qui précède avec $P = \Phi_p$, $n = p - 1$ et $x_i = \zeta^i$ $(1 \leq i \leq p-1)$. On a

$$P(X) = \frac{X^p - 1}{X - 1} \quad \text{et} \quad P'(X) = \frac{pX^{p-1}}{X - 1} - \frac{X^p - 1}{(X-1)^2}.$$

Par conséquent pour $1 \leq i \leq p - 1$

$$P'(\zeta^i) = \frac{p\zeta^{i(p-1)}}{\zeta^i - 1}.$$

Le produit des racines de P est le terme constant $P(0)$ (le degré $p - 1$ est pair)

$$\prod_{i=1}^{p-1} \zeta^i = 1.$$

Le polynôme minimal des nombres $\zeta^i - 1$ $(1 \leq i \leq p-1)$ est $P(X+1)$ dont le terme constant est p :

$$\prod_{i=1}^{p-1} (\zeta^i - 1) = p.$$

On trouve ainsi

$$\prod_{i=1}^{p-1} P'(\zeta^i) = p^{p-2}.$$

□

1.9.4 Compléments

Nous avons vu que le corps cyclotomique $\mathbf{Q}(\zeta_p)$ contenait un unique sous-corps quadratique. Il n'est pas difficile de développer l'argument pour déduire qu'inversement, tout corps quadratique sur $\mathbf{Q}$ est contenu dans un corps cyclotomique. Un résultat beaucoup plus général est le *théorème de Kronecker-Weber : toute extension abélienne de* $\mathbf{Q}$ *est contenue dans une extension cyclotomique.*

Un des problèmes ouverts les plus important du sujet est le *problème inverse de Galois* : *Est-il vrai que tout groupe fini est un groupe de Galois sur* $\mathbf{Q}$ *?* C'est facile pour un groupe abélien, c'est connu pour beaucoup de groupes (en particulier pour $\mathfrak{S}_n$ et $\mathfrak{A}_n$), mais pas encore pour tous.

Références

[1] D.S. Dummit & R.M. Foote – *Abstract Algebra*, Prentice Hall 1991, 1999.

[2] D. Duverney – *Théorie des Nombres, cours et exercices corrigés*, Dunod, 2è cycle, 1998.

[3] G. H. ; Hardy & E. M. Wright – *An introduction to the theory of numbers*. Fifth edition. Oxford University Press, 1979.

[4] S. Lang – *Algèbre*, Dunod, 2004.