Université P. et M. Curie (Paris VI),
Deuxième semestre 2007/2008

Michel Waldschmidt
date de mise à jour: 14/02/2008

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

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

Quatrième fascicule : 18/02/2008

2.5 Extensions normales

Une extension L/K est dite *normale* si elle est algébrique et si tout polynôme irréductible de $K[X]$ ayant une racine dans L est complètement décomposé dans L.

Théorème 2.15. *Une extension finie L/K est normale si et seulement s'il existe un polynôme non constant f tel que L soit le corps de décomposition de f sur K.*

Démonstration. Supposons dans un premier temps que L est le corps de décomposition sur K du polynôme $f \in K[X]$. Soit $\beta \in L$, soit g le polynôme irréductible de β sur K, soit E un corps de décomposition sur L de g et soit β' une racine de g dans E. Il s'agit de vérifier que β' est dans L. Comme $K(\beta)$ et $K(\beta')$ sont deux corps de rupture sur K du polynôme g, il existe un K-isomorphisme de $K(\beta)$ sur $K(\beta')$ qui envoie β sur β'. Le corps de décomposition sur $K(\beta)$ de f est L et le corps de décomposition sur $K(\beta')$ de f est $L(\beta')$. D'après le lemme 2.13 il existe un isomorphisme ψ de L sur $L(\beta')$ dont la restriction à $K(\beta)$ est σ. Le lemme 2.14 implique $\psi(L) = L$, donc $L(\beta') = L$ et $\beta' \in L$.

Inversement supposons l'extension L/K finie et normale. Comme L/K est une extension de type fini il existe des éléments $\alpha_1, \ldots, \alpha_m$ de L tels que $L = K(\alpha_1, \ldots, \alpha_m)$. Pour $1 \le i \le m$ soit f_i le polynôme irréductible de α_i sur K et soit $f = f_1 \cdots f_m$. Toute racine de f_i est un conjugué de α_i, donc est dans L. Ainsi L est le corps de décomposition de f sur K.

□

Remarque. Si une extension L/K est normale et si E est un corps intermédiaire, $K \subset E \subset L$, alors l'extension L/E est encore normale.

Quand E/K est une extension finie, il existe une extension finie L/E telle que l'extension L/K soit normale : il suffit d'écrire $E = K(\alpha_1, \ldots, \alpha_m)$ et de prendre pour L un corps de décomposition de $f_1 \cdots f_m$ sur K, où f_i est le polynôme irréductible de α_i sur K. Si Ω est un corps algébriquement clos qui contient E, on définit la *clôture normale de l'extension E/K dans Ω* comme l'intersection (= le plus petit) des sous-corps L de Ω contenant E tels que l'extension L/K soit normale.

De même quand $E_1, \ldots, E_n$ sont des extensions finies de K, il existe une extension normale N de K et des isomorphismes de chacun des E_i dans N.

Proposition 2.16. *Soient $K \subset E \subset N$ trois corps. On suppose l'extension N/K finie et normale. Soit σ un K-isomorphisme de E dans N. Alors il existe un K-automorphisme τ de N dont la restriction à E est σ.*

Démonstration. D'après le théorème 2.15 il existe un polynôme $f \in K[X]$ dont le corps de décomposition sur K est N. Alors N est encore un corps de décomposition de f sur E et sur $\sigma(E)$. Comme $\sigma(f) = f$ le lemme 2.13 montre qu'il existe un isomorphisme de N sur N dont la restriction à E est σ.

□

Un tel automorphisme τ en général n'est pas unique.

La proposition 2.16 permet de donner une caractérisation des extensions normales :

Corollaire 2.17. *Soit L/K une extension finie. Alors L/K est normale si et seulement si, pour toute extension F de L et tout K-isomorphisme σ de L dans F, on a $\sigma(L) = L$.*

Démonstration. La condition est nécessaire pour que l'extension L/K soit normale : cela résulte du lemme 2.14 et du théorème 2.15.

Inversement, si cette condition est vérifiée, soit $\alpha \in L$, soit N une extension normale de K contenant L et soit $\beta \in N$ un conjugué de α sur K. Les corps $K(\alpha)$ et $K(\beta)$ sont K-isomorphes, donc (proposition 2.16) il existe un K-automorphisme de N qui envoie α sur β. Soit σ la restriction de cet automorphisme à L. On a $\sigma(\alpha) = \beta$, $\sigma(L) = L$ et $\alpha \in L$. Donc $\beta \in L$.

□

2.6 Extensions séparables

Soient K un corps, $f \in K[X]$ un polynôme non constant et α une racine de f dans K. Alors $f(X)$ est divisible par $X - \alpha$ dans $K[X]$: il existe $q \in K[X]$ tel que $f(X) = (X - \alpha)q(X)$. On dit que α est *racine simple* de f si $q(\alpha) \neq 0$; autrement on dit que α est *racine multiple* de f. Ainsi pour $f \in K[X]$ et $\alpha \in K$, les conditions suivantes sont équivalentes :
(i) α est racine multiple de f
(ii) $f(X)$ est divisible par $(X - \alpha)^2$
(iii) $f(\alpha) = f'(\alpha) = 0$.

On a noté f' la dérivée du polynôme f :

$$\text{pour} \quad f(X) = \sum_{i=0}^{n} a_i X^i, \quad \text{on a} \quad f'(X) = \sum_{i=1}^{n} i a_i X^{i-1}.$$

Pour un polynôme $f \in K[X]$ de degré ≥ 1 les conditions suivantes sont équivalentes :
(i) Les facteurs irréductibles de f dans l'anneau factoriel $K[X]$ apparaissent tous avec la multiplicité 1
(ii) Si g est un polynôme non constant, alors $f(X)$ n'est pas divisible par g^2
(iii) $\operatorname{pgcd}(f, f') = 1$.

Si un polynôme n'a pas de racines multiples dans un corps de décomposition, alors dans une extension quelconque de K il n'a pas des racines multiples.

Quand K est un corps et $f \in K[X]$ un polynôme irréductible, on dit que f est *séparable* si les racines de f dans un corps de décomposition sont toutes simples. Un polynôme de $K[X]$ est dit *séparable* si tous ses facteurs irréductibles le sont. Sinon il est dit *inséparable*.

Soit L/K une extension algébrique. Un élément α de L est dit *séparable* sur K si son polynôme irréductible sur K est séparable sur K. L'extension L/K est dite *séparable* si elle est algébrique et si tout élément de L est séparable sur K. Un élément algébrique ou une extension algébrique est dite *inséparable* si elle n'est pas séparable.

Lemme 2.18. *Soient K un corps et $f \in K[X]$ un polynôme irréductible. Alors les conditions suivantes sont équivalentes :*
(i) f est séparable sur K
(ii) $f' \neq 0$.

Un corps K est *parfait* si toutes ses extensions algébriques sont séparables, c'est-à-dire si tout polynôme de $K[X]$ est séparable. Il résulte du lemme 2.18 que tout corps de caractéristique nulle est parfait.

Démonstration du lemme 2.18. Si $f' = 0$ alors toute racine de f dans un corps de décomposition est multiple, donc f n'est pas séparable.

Réciproquement si f n'est pas séparable choisissons une racine multiple α de f dans un corps de décomposition de f sur K. Alors f est le polynôme irréductible de α sur K. Comme $f'(\alpha) = 0$ le polynôme f' est multiple de f et, comme il est de degré inférieur à celui de f, il est nul.

□

On en déduit que dans un corps de caractéristique nulle tout polynôme est séparable. En caractéristique finie p, un polynôme irréductible

$$f(X) = \sum_{i=0}^{n} a_i X^i,$$

est inséparable si et seulement si $ia_i = 0$ pour tout $i = 0, \ldots, n$, donc si et seulement si $a_i = 0$ pour tout i premier à p. Cela s'écrit encore : il existe $g \in K[X]$ tel que $f(X) = g(X^p)$.

Exemple. Sur $K = \mathbf{F}_p(T)$ le polynôme $X^p - T \in K[X]$ est irréductible et inséparable.

Théorème 2.19. *Soient $k \subset K \subset N$ trois corps. On suppose l'extension N/k finie et normale et l'extension K/k séparable. On pose $d = [K : k]$. Alors il existe d k-isomorphismes de K dans N.*

La démonstration se fait par récurrence grâce au lemme suivant, où on utilise la notation que voici : quand k est un corps et E, F deux extensions de K, $H(k; E, F)$ désigne l'ensemble des k isomorphismes de E dans F.

Lemme 2.20. *Soient $k \subset L \subset K \subset N$ quatre corps, avec N/k finie normale. Il existe une bijection entre l'ensemble $H(k, K, N)$ et le produit cartésien $H(k, L, N) \times H(L, K, N)$.*

Démonstration du lemme 2.20. Pour chaque $\sigma \in H(k, L, N)$ choisissons un prolongement de σ en un automorphisme $\overline{\sigma}$ de N (proposition 2.16). La bijection recherchée est obtenue en associant à $\varphi \in H(k, K, N)$ le couple (σ, ψ), où $\sigma \in H(k, L, N)$ est la restriction de φ à L et $\psi = \overline{\sigma}^{-1} \circ \varphi \in H(L, K, N)$.

□

Démonstration du Théorème 2.19. Si l'extension K/k est monogène on écrit $K = k(x)$ avec $x \in K$; il y a d conjugués $x_1, \ldots, x_d$ de x dans N et les d isomorphismes cherchés sont déterminés respectivement par $x \to x_i$.

Dans le cas général soit $x \in K \setminus k$ et soit $L = k(x)$. L'extension N/L est normale et l'extension K/L séparable. Il suffit alors d'appliquer l'hypothèse de récurrence en utilisant les lemmes 2.1 et 2.20.

□

Une première application du théorème 2.19 est le *théorème de l'élément primitif* :

Corollaire 2.21. *Soit K/k une extension finie séparable. Alors cette extension est monogène : il existe $\alpha \in K$ tel que $K = k(\alpha)$.*

Démonstration. Nous verrons que si k est un corps fini, alors toute extension finie de k est séparable sur k donc monogène.

Supposons k infini. Soit $d = [K : k]$. Soit N une extension finie normale de k contenant K et soient $\sigma_1, \dots, \sigma_d$ les k-isomorphismes de K dans N.

Comme le corps k est infini, si un k espace vectoriel V contient des sous-espaces $V_1, \dots, V_m$ et est contenu dans leur réunion, alors il est égal à l'un au moins des V_i (on utilise le fait que k a au moins m éléments et on procède par récurrence sur m). On en déduit qu'il existe un élément α de K dont les images $\sigma_1(\alpha), \dots, \sigma_d(\alpha)$ sont deux-à-deux distinctes. Le polynôme irréductible de α sur k a d racines distinctes dans N, donc est de degré d sur k, ce qui permet de conclure $K = k(\alpha)$. □

Notons que la réciproque n'est pas vraie : l'extension inséparable $K(\sqrt{T})$ du corps $K = \mathbf{F}_2(T)$ est monogène.

Exercice. Soit K le corps $\mathbf{F}_2(T_1, T_2)$ des fractions rationnelles en deux indéterminées T_1 et T_2 sur le corps à 2 éléments et soit L le corps de décomposition du polynôme $(X^2 - T_1)(X^2 - T_2)$ sur K. Montrer que l'extension L/K n'est pas monogène.

2.7 Polynômes cyclotomiques

Soit n un entier positif. Une racine n-ième de l'unité dans un corps K est un élément de $K^\times$ qui satisfait $x^n = 1$. Une racine primitive n-ième de l'unité dans K est un élément de $K^\times$ d'ordre n : il satisfait, pour k dans $\mathbf{Z}$, $x^k = 1$ si et seulement si n divise k.

Exercice. Soient K un corps, G un sous-groupe fini de $K^\times$, n l'ordre de G. Soit ℓ le plus grand ordre d'un élément de G. Vérifier $x^\ell = 1$ pour tout $x \in G$. En déduire $\ell = n$, montrer que G est cyclique, que G est l'ensemble des racines n-ièmes de l'unité dans K et que

$$X^n - 1 = \prod_{x \in G} (X - x)$$

dans $K[X]$.

L'application $\mathbf{C} \to \mathbf{C}^\times$ qui envoie z sur $e^{2i\pi z/n}$ est un homomorphisme du groupe additif $\mathbf{C}$ dans le groupe multiplicatif $\mathbf{C}^\times$ qui est périodique de période n. Donc il se factorise en un homomorphisme du groupe $\mathbf{C}/n\mathbf{Z}$ dans $\mathbf{C}^\times$: on le note encore $z \mapsto e^{2i\pi z/n}$.

Le groupe multiplicatif $(\mathbf{Z}/n\mathbf{Z})^\times$ de l'anneau $\mathbf{Z}/n\mathbf{Z}$ est formé des classes des entiers premiers avec n. Son ordre est donc le nombre, noté $\varphi(n)$, d'entiers k dans l'intervalle $1 \leq k \leq n$ vérifiant $\mathrm{pgcd}(n, k) = 1$. L'application $\varphi : \mathbf{N} \to \mathbf{Z}$ ainsi définie est appelée *indicatrice d'Euler*.

Les nombres complexes

$$e^{2i\pi k/n}, \qquad k \in (\mathbf{Z}/n\mathbf{Z})^\times$$

sont les $\varphi(n)$ racines primitives de l'unité dans $\mathbf{C}$.

On définit un polynôme $\Phi_n(X) \in \mathbf{C}[X]$ par

$$\Phi_n(X) = \prod_{k \in (\mathbf{Z}/n\mathbf{Z})^\times} (X - e^{2i\pi k/n}).$$

Ce polynôme est appelé *polynôme cyclotomique d'indice* n, il est unitaire, de degré $\varphi(n)$. La partition de l'ensemble des racines de l'unité suivant leur ordre montre que l'on a, pour tout $n \geq 1$,

$$X^n - 1 = \prod_{d|n} \Phi_d(X). \tag{2.22}$$

Les premiers polynômes cyclotomiques sont

$$\Phi_1(X) = X - 1, \quad \Phi_2(X) = X + 1, \quad \Phi_3(X) = X^2 + X + 1, \quad \Phi_4(X) = X^2 + 1,$$

$$\Phi_5(X) = X^5 + X^4 + X^3 + X^2 + X + 1, \quad \Phi_6(X) = X^2 - X + 1.$$

Exercice. Vérifier $\Phi_p(X) = X^{p-1} + \cdots + X + 1$ si p est premier.
Vérifier $\varphi(2m) = 2\varphi(m)$ si m est pair et $\varphi(2m) = \varphi(m)$ si m est impair.
Vérifier $\Phi_{2m}(X) = \Phi_m(X^2)$ si m est pair et $\Phi_{2m}(X) = (-1)^{\varphi(m)}\Phi_m(-X)$ si m est impair.
En déduire

$$\Phi_8(X) = X^4 + 1, \quad \Phi_{12}(X) = X^4 - X^2 + 1.$$

Théorème 2.23. *Pour tout entier positif n, le polynôme $\Phi_n(X)$ a ses coefficients dans $\mathbf{Z}$. De plus $\Phi_n(X)$ est irréductible dans $\mathbf{Z}[X]$.*

Avant de démontrer le théorème 2.23 nous allons rappeler quelques propriétés de l'anneau $\mathbf{Z}[X]$. Le pgcd des coefficients d'un polynôme $f \in \mathbf{Z}[X]$ est appelé *contenu* de f et noté $c(f)$. Un polynôme de $\mathbf{Z}[X]$ est dit *primitif* si son contenu est 1. Tout polynôme non nul $f \in \mathbf{Z}[X]$ s'écrit de manière unique $f = c(f)g$ avec $g \in \mathbf{Z}[X]$ primitif. Plus généralement pour tout $f \in \mathbf{Q}[X]$ non nul il existe un unique nombre rationnel positif c tel que le polynôme cf soit dans $\mathbf{Z}[X]$ et primitif.

Lemme 2.24 (Lemme de Gauss)**.** *Pour f et g dans $\mathbf{Z}[X]$ non nuls,*

$$c(fg) = c(f)c(g).$$

Démonstration. Il suffit de montrer que le produit de deux polynômes primitifs est primitif. Plus précisément, soit p un nombre premier, f et g deux polynômes de $\mathbf{Z}[X]$ dont le contenu n'est pas divisible par p. On va montrer que le contenu du produit fg n'est pas divisible par p.

Considérons le morphisme surjectif d'anneaux

$$\Psi_p : \mathbf{Z}[X] \to \mathbf{F}_p[X] \tag{2.25}$$

qui envoie X sur X et $\mathbf{Z}$ sur $\mathbf{F}_p$ par réduction modulo p des coefficients. Le noyau de Ψ_p est formé des polynômes dont le contenu est divisible par p. Donc $\Psi_p(f) \neq 0$ et $\Psi_p(g) \neq 0$. Comme p est premier, l'anneau $\mathbf{F}_p[X]$ est intègre, donc $\Psi_p(fg) = \Psi_p(f)\Psi_p(g) \neq 0$, ce qui montre que fg n'appartient pas au noyau de Ψ_p.

$\square$

L'anneau $\mathbf{Z}$ est *euclidien*, donc *factoriel* et, quand A est un anneau factoriel, l'anneau $A[X]$ des polynômes en une indéterminée à coefficients dans A est aussi factoriel. Par conséquent $\mathbf{Z}[X]$ est un anneau factoriel. Les éléments inversibles de $\mathbf{Z}[X]$ sont $\{+1, -1\}$. Les éléments irréductibles de $\mathbf{Z}[X]$ sont
– les nombres premiers $\{2, 3, 5, 7, 11, \ldots\}$,
– les polynômes irréductibles de $\mathbf{Q}[X]$ qui sont à coefficients dans $\mathbf{Z}$ et ont un contenu égal à 1
– et bien entendu le produit par -1 d'un de ces éléments.

Le lemme de Gauss 2.24 montre que, si f et g sont deux polynômes unitaires de $\mathbf{Q}[X]$ tels que $fg \in \mathbf{Z}[X]$, alors f et g sont dans $\mathbf{Z}[X]$. En particulier les facteurs irréductibles d'un polynôme unitaire de $\mathbf{Z}[X]$ sont des polynômes unitaires de $\mathbf{Z}[X]$.

La démonstration que nous allons donner du théorème 2.23 utilisera le lemme suivant, sur lequel nous reviendrons au § 2S :CorpsFinis :

Lemme 2.26. *Si p est un nombre premier et $A \in \mathbf{F}_p[X]$ un polynôme, alors $A(X^p) = A(X)^p$.*

Démonstration du théorème 2.23. La démonstration du fait que $\Phi_n(X) \in \mathbf{Z}[X]$ repose sur la division euclidienne dans $\mathbf{Z}[X]$: quand A et B sont deux éléments de $\mathbf{Z}[X]$ avec B *unitaire*, pour tout $A \in B[X]$ il existe un couple unique (Q, R) formé de deux polynômes de $\mathbf{Z}[X]$ tels que $A = BQ + R$ et soit $R = 0$, soit $\deg R < \deg B$.

On démontre alors le fait que $\Phi_n(X) \in \mathbf{Z}[X]$ par récurrence sur n. C'est vrai pour $n = 1$ car $\Phi_1(X) = X - 1$. Supposons $\Phi_m(X) \in \mathbf{Z}[X]$ pour tout entier $m < n$. L'hypothèse de récurrence implique que le polynôme
$$h(X) = \prod_{\substack{d|n \\ d \neq n}} \Phi_d(X)$$
est unitaire et à coefficients dans $\mathbf{Z}$. On divise le polynôme $X^n - 1$ par h dans $\mathbf{Z}[X]$: désignons par $Q \in \mathbf{Z}[X]$ le quotient et par $R \in \mathbf{Z}[X]$ le reste :
$$X^n - 1 = h(X)Q(X) + R(X).$$
On a aussi $X^n - 1 = h(X)\Phi_n(X)$ dans $\mathbf{C}[X]$ par (2.22). Par unicité de la division euclidienne dans $\mathbf{C}[X]$ il en résulte $Q = \Phi_n$ et $R = 0$, donc $\Phi_n \in \mathbf{Z}[X]$.

Montrons que le polynôme Φ_n est irréductible dans $\mathbf{Z}[X]$. Comme il est unitaire, son contenu est 1. Il s'agit donc de vérifier qu'il est irréductible dans $\mathbf{Q}[X]$.

Soit $f \in \mathbf{Q}[X]$ un facteur unitaire irréductible de Φ_n et soit $g \in \mathbf{Q}[X]$ le quotient : on a donc $\Phi_n = fg$. Le but est de montrer $g = 1$.

Soit $\zeta \in \mathbf{C}$ une racine de f (donc ζ est une racine primitive n-ième de l'unité) et soit p un nombre premier ne divisant pas n. On commence par vérifier que $f(\zeta^p) = 0$.

Comme ζ^p est aussi une racine primitive n-ième de l'unité, c'est une racine de Φ_n, donc si $f(\zeta^p) \neq 0$ on a $g(\zeta^p) = 0$. Comme f est le polynôme irréductible de ζ, il en résulte que $f(X)$ divise $g(X^p)$.

Considérons le morphisme d'anneaux Ψ_p de $\mathbf{Z}[X]$ sur $\mathbf{F}_p[X]$ déjà introduit en (2.25). dans la démonstration du lemme 2.24. Notons F et G les images dans $\mathbf{F}_p[X]$ de f et g respectivement. L'image de $\Phi_n(X)$ est FG et c'est un diviseur de $X^n - 1$ dans $\mathbf{F}_p[X]$. Le lemme 2.26 montre que l'image de $g(X^p)$ est $G(X^p) = G(X)^p$ car $G(X) \in \mathbf{F}_p[X]$. De plus $F(X)$ divise $G(X)^p$ dans $\mathbf{F}_p[X]$. Le polynôme $F(X)$ est unitaire de même degré que f, il admet un diviseur irréductible $k(X)$ dans $\mathbf{F}_p[X]$. Alors $k(X)$ divise $F(X)$ et $G(X)^p$, donc il divise $G(X)$ et son carré divise $F(X)G(X)$. Mais comme p ne divise pas n, le polynôme $X^n - 1$ n'est divisible par aucun carré de polynôme non constant dans $\mathbf{F}_p[X]$. On en conclut $f(\zeta^p) = 0$.

Par conséquent dès que f s'annule en ζ il s'annule en ζ^p quand p est un nombre premier ne divisant pas n. On en déduit (par récurrence sur le nombre de facteurs de m) qu'il s'annule en chaque ζ^m quand m est premier avec n ; mais dans le groupe cyclique formé par les racines n-ièmes de l'unité, l'ensemble des ζ^m avec $\operatorname{pgcd}(m, n) = 1$ est l'ensemble des générateurs de ce groupe, donc l'ensemble des racines de Φ_n. D'où $g = 1$.

$\square$

Quand K est un corps de caractéristique finie p et quand n est un multiple de p, le polynôme $X^n - 1$ est une puissance p-ième d'un polynôme de $K[X]$: plus précisément, si $n = p^a m$ avec m non divisible par p, alors

$$X^n - 1 = (X^m - 1)^{p^a}.$$

Ainsi, quand on veut étudier le polynôme $X^n - 1$, on est ramené à étudier $X^m - 1$ avec m non multiple de p. Cela justifie l'hypothèse qui va apparaître.

Comme le polynôme Φ_n est à coefficients dans $\mathbf{Z}$ pour tout corps K on peut considérer $\Phi_n(X)$ comme un élément de $K[X]$: en caractéristique nulle, c'est parce que K contient $\mathbf{Q}$, en caractéristique finie p on considère l'image de Φ_n par le morphisme Ψ_p introduit en (2.25) : on note encore Φ_n cette image.

Proposition 2.27. *Soient K un corps et n un entier positif. On suppose que K est soit de caractéristique nulle, soit de caractéristique p premier ne divisant pas n. Alors le polynôme $\Phi_n(X)$ est séparable sur K et ses racines dans K sont exactement les racines primitives de l'unité qui appartiennent à K.*

Démonstration. La dérivée du polynôme $X^n - 1$ est n. Dans K on a $n \neq 0$, donc $X^n - 1$ est séparable sur K et comme $\Phi_n(X)$ est un facteur de $X^n - 1$ il est aussi séparable sur K. Les racines dans K de $X^n - 1$ sont exactement les racines n-ièmes de l'unité contenues dans K. Dire qu'une racine n-ième de l'unité est primitive signifie qu'elle n'est pas racine d'un polynôme Φ_d avec $d|n$, $d \neq n$. D'après (2.22) cela signifie donc qu'elle est racine de Φ_n.

$\square$

Soit n un entier positif. On définit le *corps cyclotomique de niveau n sur $\mathbf{Q}$* par

$$R_n = \mathbf{Q}\big(\{e^{2i\pi k/n} \ ; \ k \in (\mathbf{Z}/n\mathbf{Z})^\times\}\big) \subset \mathbf{C}.$$

C'est le corps de décomposition de Φ_n sur $\mathbf{Q}$ et c'est aussi le corps de rupture de Φ_n sur $\mathbf{Q}$. Si $\zeta \in \mathbf{C}$ est une racine primitive de l'unité, alors $\{1, \zeta, \ldots, \zeta^{\varphi(n)-1}\}$ est une base de R_n comme espace vectoriel sur $\mathbf{Q}$.

Proposition 2.28. *Le groupe des automorphismes du corps R_n est naturellement isomorphe au groupe mulltiplicatif $(\mathbf{Z}/n\mathbf{Z})^\times$.*

Démonstration. Soit ζ_n une racine primitive n-ième de l'unité. Pour $\varphi \in \operatorname{Aut}(R_n)$, on définit $\theta(\varphi) \in (\mathbf{Z}/n\mathbf{Z})^\times$ par

$$\varphi(\zeta_n) = \zeta_n^{\theta(\varphi)}.$$

Alors l'application θ est un isomorphisme du groupe de $\operatorname{Aut}(R_n/\mathbf{Q})$ sur $(\mathbf{Z}/n\mathbf{Z})^\times$.

$\square$

Exemple. Le sous corps de R_n fixé par le sous-groupe $\theta^{-1}(\{1,-1\})$ de $G(R_n/\mathbf{Q})$ est le sous-corps réel maximal de R_n :

$$R_n^+ = \mathbf{Q}(\zeta_n + \zeta_n^{-1}) = \mathbf{Q}\big(\cos(2\pi/n)\big) = R_n \cap \mathbf{R}$$

avec $[R_n : R_n^+] = 2$.

2.8 Théorie de Galois

Une extension algébrique L/K est dite *galoisienne* si elle est normale et séparable. C'est équivalent à dire que pour tout $\alpha \in L$ le nombre de conjugués de α dans L est le degré $[K(\alpha) : K]$ de α sur K.

Soit L/K une extension. On note $\mathrm{Aut}(L/K)$ le groupe des K-automorphismes de L.

Lemme 2.29. *Quand L/K est une extension finie, le groupe $\mathrm{Aut}(L/K)$ est fini d'ordre $\leq [L : K]$.*

Démonstration. On écrit $L = K(\alpha_1, \ldots, \alpha_m)$. Un K-automorphisme σ de L est entièrement déterminé par $\big(\sigma(\alpha_1), \ldots, \sigma(\alpha_m)\big) \in L^m$. Pour $1 \leq i \leq m$ soit d_i le degré de α_i sur $K(\alpha_1, \ldots, \alpha_{i-1})$. Ainsi $[L : K] = d_1 \cdots d_m$. Quand σ décrit $\mathrm{Aut}(L/K)$, il y a au plus d_1 valeurs possibles $\sigma(\alpha_1) \in L$ (à savoir les conjugués sur K de α_1 dans L) et quand on impose les valeurs de $\sigma(\alpha_1), \ldots, \sigma(\alpha_{i-1})$, il y a au plus d_i valeurs possibles $\sigma(\alpha_i) \in L$ (les conjugués dans L de α_i sur le corps $K\big(\sigma(\alpha_1), \ldots, \sigma(\alpha_{i-1})\big)$). $\square$

Théorème 2.30. *Soit L/K une extension finie. Alors l'extension L/K est galoisienne si et seulement si le groupe $\mathrm{Aut}(L/K)$ est d'ordre égal à $[L : K]$.*

Démonstration. Si l'extension L/K est galoisienne finie, le théorème 2.19 (dans lequel on prend $N = K$) montre que le groupe $\mathrm{Aut}(L/K)$ a $[L : K]$ éléments.

Inversement, si $\mathrm{Aut}(L/K)$ a $[L : K]$ éléments, soit $\alpha_1 \in L$; on peut écrire (comme dans la démonstration du lemme 2.29) $L = K(\alpha_1, \ldots, \alpha_m)$ avec des éléments $\alpha_2, \ldots, \alpha_m$ dans L. L'égalité $|\mathrm{Aut}(L/K)| = d_1 \cdots d_m$ montre en particulier que α_1 a d_1 conjugués sur K dans L, avec $d_1 = [K(\alpha_1) : K]$. Donc l'extension L/K est galoisienne. $\square$

$$\left.\begin{array}{r} H=\mathrm{Aut}(L/M)\left(\begin{array}{c} L \\ | \\ M=L^H\end{array}\right. \\ \begin{array}{c} | \\ K\end{array}\end{array}\right) G$$

Soit L/K une extension algébrique et soit $G = \mathrm{Aut}(L/K)$. Pour chaque extension M de K contenue dans L le groupe $\mathrm{Aut}(L/M)$ est un sous-groupe de G. Inversement pour chaque sous-groupe H de G, le sous-ensemble

$$L^H = \{x \in L\ ;\ \sigma(x) = x \text{ pour tout } \ \sigma \in H\}$$

de L est un sous-corps de L contenant K, appelé *sous-corps de L fixé par H*.

De ces définitions on déduit immédiatement :

$$\begin{tikzcd} L \arrow[d, dash] \arrow[d, bend right=60, dash, "H"'] \arrow[dd, bend left=60, dash, "H'"] \arrow[ddd, bend left=80, dash, "G"] \\ M = L^H \arrow[d, dash] \\ M' = L^{H'} \arrow[d, dash] \\ K \end{tikzcd}$$

Lemme 2.31. *Soit L/K une extension algébrique et soit $G = \mathrm{Aut}(L/K)$. Les deux applications*

$$M \mapsto \mathrm{Aut}(L/M) \quad \textit{et} \quad H \mapsto L^H$$

sont décroissantes :

Si H et H' sont des sous-groupes de G avec $H \subset H'$, alors $L^{H'} \subset L^H$.

Si M et M' sont deux extensions de K contenues dans L avec $M' \subset M$, alors

$$\mathrm{Aut}(L/M) \subset \mathrm{Aut}(L/M').$$

Quand L/K est une extension galoisienne, le groupe $\mathrm{Aut}(L/K)$ est appelé *groupe de Galois de L sur K* et noté $\mathrm{Gal}(L/K)$.

Théorème 2.32.

1. *Soient L/k une extension, G un sous-groupe de* $\mathrm{Aut}(L/k)$ *et K le corps L^G.*

   a) *Si G est fini, alors L/K est une extension galoisienne finie de groupe de Galois G.*

   b) *Si l'extension L/k est algébrique, alors L/K est une extension galoisienne.*

$$\begin{tikzcd} L \arrow[d, dash] \arrow[d, bend right=60, dash, "G"'] \\ K = L^G \arrow[d, dash] \\ k \end{tikzcd}$$

2. *Soit L/K une extension galoisienne de groupe de Galois $G = \mathrm{Aut}(L/K)$. Alors $L^G = K$.*

Démonstration. 1. a) Soit $\alpha \in L$. Soit m le nombre d'éléments de l'ensemble $E = \{\sigma(\alpha)\ ;\ \sigma \in G\}$. Notons $E = \{\alpha_1, \dots, \alpha_m\}$. Le groupe G opère sur E par $(\sigma, \alpha_i) \mapsto \sigma(\alpha_i)$, ce qui signifie que l'application qui à $\sigma \in G$ associe $\alpha_i \mapsto \sigma(\alpha_i)$ est un homomorphisme de G dans le groupe symétrique $\mathfrak{S}_E$.

Le polynôme $P(X) = \prod_{i=1}^m (X - \alpha_i)$ vérifie $\sigma(P) = P$. Par définition de K cela signifie $P \in K[X]$. Comme $P(\alpha) = 0$, on en déduit que α est algébrique sur K. Soit f le polynôme irréductible de α sur K. Comme $P \in K[X]$ s'annule en α, il en résulte que f divise P dans $K[X]$. Mais f s'annule en chaque conjugué de α sur K, donc en chaque élément de E et par conséquent P divise f, donc finalement $P = f$. Cela montre que E a autant d'éléments que le degré de α sur K, donc E est l'ensemble de tous les conjugués de α sur K et l'extension L/K est galoisienne. Nous venons de voir que tout élément de L est de degré $\le |G|$ sur K. Donc L est une extension algébrique de K. De plus, d''après le corollaire 2.21 toute extension finie de K contenue dans L a un degré $\le |G|$; donc L est une extension finie de K et $[L : K] \le |G|$. Mais on a $[L : K] \ge |\mathrm{Aut}(L/K)|$; de plus G est un sous-groupe de $\mathrm{Aut}(L/K)$. Par conséquent $G = \mathrm{Aut}(L/K)$.

1. b) Soit $\alpha \in L$. L'ensemble $E = \{\sigma(\alpha)\ ;\ \sigma \in G\}$ est constitué de conjugués de α sur k, donc est fini. Comme ci-dessus le polynôme irréductible de α sur K est $\prod_{\beta \in E}^m (X - \beta)$. On vérifie ainsi que le nombre de conjugués de α sur K est égal à $[K(\alpha) : K]$. Donc l'extension L/K est galoisienne.

2. Soit d le degré de α sur K. Le polynôme irréductible de α sur K est $\prod_{j=1}^d \bigl(X - \sigma_j(\alpha)\bigr)$ où $\sigma_1, \dots, \sigma_d$ sont des éléments de $\mathrm{Aut}(L/K)$ et $\sigma_1(\alpha), \dots, \sigma_d(\alpha)$ sont deux-à-deux distincts. De plus,

l'ensemble des $\sigma(\alpha)$ pour σ décrivant $\mathrm{Aut}(L/K)$ est $\{\sigma_1(\alpha), \ldots, \sigma_d(\alpha)\}$. Alors $\alpha \in L^{\mathrm{Aut}(L/K)}$ équivaut à $d = 1$, donc à $\alpha \in K$.

$\square$

Du théorème 2.32 (parties 1.b) et 2.) on déduit qu'une extension algébrique L/K est galoisienne si et seulement si $L^{\mathrm{Aut}(L/K)} = K$.

Voici le théorème principal de la théorie de Galois pour les extensions finies ; il affirme que, pour une extension galoisienne finie, la correspondance que nous venons d'introduire entre les extensions intermédiaires et les sous-groupes du groupe de Galois est bijective.

Théorème 2.33 (Théorème de Galois). *Soit L/K une extension galoisienne finie de groupe de Galois $G = \mathrm{Gal}(L/K)$.*

1. *Si M est une extension de K contenue dans L et si on note $H = \mathrm{Aut}(L/M)$, alors L/M est une extension galoisienne de groupe de Galois H et on a*

$$[L : M] = |H| \quad \textit{et} \quad M = L^H.$$

2. *Si H est un sous-groupe de G et $M = L^H$ le sous-corps de L fixé par H, alors L/M est une extension galoisienne et on a*

$$[L : M] = |H| \quad \textit{et} \quad H = \mathrm{Gal}(L/M).$$

3. *Si M est une extension de K contenue dans L et si on note H le sous-groupe $\mathrm{Gal}(L/M)$ de G, alors l'extension M/K est galoisienne si et seulement si H est normal dans G. Dans ce cas le groupe de Galois de M/K est isomorphe au quotient G/H.*

Démonstration. 1. L'extension L/M est séparable et normale, donc galoisienne et son groupe de Galois est $H = \mathrm{Aut}(L/M)$. On a $M \subset L^H \subset L$ et l'extension L/L^H est galoisienne finie de groupe de Galois H par le théorème 2.32. Donc $[L : M] = |H|$ et $M = L^H$.

2. Comme $M = L^H$ est un corps intermédiaire $K \subset M \subset L$, l'extension L/M est galoisienne de groupe de Galois $\mathrm{Aut}(L/M)$. Le théorème 2.32 montre que l'extension L/L^H est galoisienne finie de groupe de Galois H. Comme $M = L^H$ on en déduit $H = \mathrm{Aut}(L/M)$ et $[L : M] = |H|$.

3. Supposons l'extension M/K galoisienne. Soient $\sigma \in H$ et $\tau \in G$. Il s'agit de vérifier $\tau^{-1} \circ \sigma \circ \tau \in H$. Pour cela on prend $x \in M$; l'extension M/K étant galoisienne, on a $\tau(x) \in M$, donc $\sigma \circ \tau(x) = \tau(x)$ et ainsi $\tau^{-1} \circ \sigma \circ \tau(x) = x$. Cela montre que le sous-groupe H de G est normal.

Inversement si H est normal dans G soit $x \in M$ et soit $\tau \in G$. Il s'agit de vérifier $\tau(x) \in M$, c'est-à-dire $\sigma \circ \tau(x) = \tau(x)$ pour tout $\sigma \in H$. En effet comme $\sigma \in H$ et que H est normal dans G on a $\tau^{-1} \circ \sigma \circ \tau \in H$, donc $\tau^{-1} \circ \sigma \circ \tau(x) = x$.

On suppose encore que H est normal dans G, c'est-à-dire que l'extension M/K est galoisienne ; la restriction de σ à M est alors un K-automorphisme de M. L'application qui envoie un élément $\sigma \in \mathrm{Aut}(L/K)$ sur sa restriction M définit un homomorphisme de G dans $\mathrm{Aut}(M/K)$ de noyau H. Son image est donc isomorphe au quotient G/H. Comme

$$|G| = [L : K] = [L : M][M : K] = |H|[M : K],$$

il en résulte que cet homomorphisme est surjectif : son image est $\mathrm{Aut}(M/K)$.

$\square$

Exercice. Soient L/K une extension galoisienne finie de groupe de Galois G, H un sous-groupe de G, $M = L^H$ et $\sigma \in G$. Alors l'extension $L/\sigma(M)$ est galoisienne de groupe de Galois $\sigma H \sigma^{-1}$ et $\sigma(M) = L^{\sigma H \sigma^{-1}}$.

Une extension galoisienne est dite *abélienne, cyclique, résoluble,...* si son groupe de Galois l'est. Rappelons qu'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 $(0 \le i \le s-1)$.

2.9 Théorie de Galois : quelques exemples

2.9.1 Corps cyclotomiques

Soient n un entier positif, E_n le corps cyclotomique de niveau n et ζ_n une racine primitive n-ième de l'unité, de sorte que $E_n = \mathbf{Q}(\zeta_n)$.

Nous avons vu (Proposition 2.28) 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 2.34. *L'ordre de σ_k dans G est égal à l'ordre de la classe de k modulo p.*

Démonstration. Pour $h \ge 1$ on a $\zeta^h = 1$ si et seulement si p divise h. Donc pour $m \ge 1$ on a $\zeta^m = \zeta$ si et seulement si $m \equiv 1 \pmod p$. D'autre part $\sigma_k^m(\zeta) = \zeta^{k^m}$. Il en résulte que 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 $(\mathbf{Z}/p\mathbf{Z})^\times$. □

Comme ζ est racine du polynôme

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

il est de degré $p-1$ sur $\mathbf{Q}$ et $\{1, \zeta, \zeta^2, \dots, \zeta^{p-2}\}$ est une base sur $\mathbf{Q}$ de E. On préfère d'utiliser comme base $\{\zeta, \zeta^2, \dots, \zeta^{p-2}, \zeta^{p-1}\}$ 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 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 § 2.7 comme exemple d'application de la proposition 2.28. 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 $\mathbf{Q}(\sqrt{-7})$.

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 2.28 l'énoncé suivant :

Corollaire 2.35. *Soit $n = p_1^{a_1} \cdots p_k^{a_k}$ un entier ≥ 2 décomposé en facteurs premiers. Notons E_n le corps cyclotomique $\mathbf{Q}(\zeta_n)$ de niveau n et F_i le corps cyclotomique $E_{p_i^{a_i}} = \mathbf{Q}(\zeta_{p_i^{a_i}})$ de niveau $p_i^{a_i}$. Alors*

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

2.9.2 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.

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)).

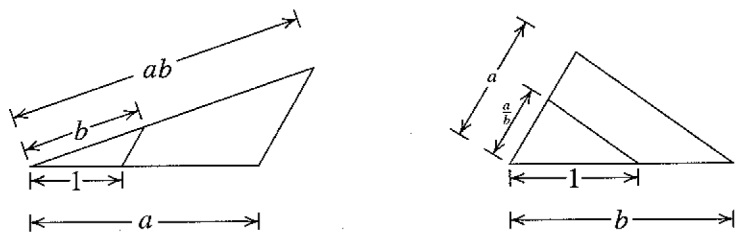

Fig. 1

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.

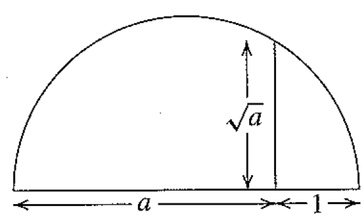

Fig. 2

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

Proposition 2.36. *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* [5]).

On déduit du corollaire 2.35 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 2.37. *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 théorème de Galois 2.33 permet de démontrer l'énoncé suivant :

Proposition 2.38. *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]).

2.9.3 Résolution par radicaux

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.

Le théorème de Galois 2.33 permet de démontrer l'énoncé suivant (voir par exemple [1] § 14.7 Th. 39).

Théorème 2.39. *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 2.39 est un théorème dû à Kummer dont nous donnons seulement l'énoncé :

Théorème 2.40. *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 $\alpha^n \in K$.*

2.9.4 Fonctions symétriques, discriminant

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 (§ 2.9.2) 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 2.33, 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 2.41. *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 $As_1^{a_1-a_2}s_2^{a_2-a_3}\cdots s_n^{a_n}$.

Ceci montre en passant que $s_1, \ldots, s_n$ sont algébriquement indépendants.

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

$$f(X) = X^n - s_1X^{n-1} + s_2X^{n-2} - \cdots + (-1)^n s_n. \tag{2.42}$$

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 2.43. *Si $s_1, \ldots, s_n$ sont des indéterminées sur $\mathbf{Q}$, le polynôme générique (2.42) 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 $x_1, \dots, x_n$ des éléments de L. On définit le *discriminant* de $(x_1, \dots, x_n)$ par

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

Le *discriminant générique* est celui pour lequel $x_1, \dots, x_n$ sont des indéterminées et $L = \mathbf{Q}(x_1, \dots, x_n)$. C'est un polynôme symétrique, donc d'après la proposition 2.41 il s'exprime comme un polynôme en les fonctions symétriques élémentaires $s_1, \dots, s_n$. Une des deux racines carrées de D est

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

L'autre est $-\sqrt{D}$. 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 $(\alpha_1, \dots, \alpha_n)$. 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 $x_1, \dots, x_n$ des éléments de L et soit D leur discriminant. Considérons le polynôme

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

Sa dérivée est

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

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

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

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 2.44. *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

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

□

Exercice. Soit p un nombre premier. Vérifier que l'unique sous-corps quadratique de $\mathbf{Q}(\zeta_p)$ 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 [1] § 14.5).

2.9.5 Compléments

Nous avons vu au § 2.9.1 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.* Voir par exemple le Théorème 2.10 de [4].

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.

2.9.6 Exercices

a) *Étude du corps de décomposition de $X^8 - 2$. Référence : [1].*

On désigne par θ la racine réelle du polynôme $X^8 - 2$ et par ζ une racine primitive 8ème de l'unité. Le corps de décomposition du polynôme $X^8 - 2$ est $K = \mathbf{Q}(\theta, \zeta)$. Sous un élément σ du groupe de Galois G de K sur $\mathbf{Q}$ l'image de ζ est une des 4 racines primitives 8èmes de l'unité, à savoir ζ, ζ^3, ζ^5 ou $\zeta^7 = \zeta^{-1} = \overline{\zeta}$. L'image de θ est l'un des 8 conjugués de θ, à savoir $\zeta^j\theta$. À priori cela fait $4 \times 8 = 32$ possibilités pour σ. Mais on a $K = \mathbf{Q}(\theta, i)$, donc K a pour degré 16 sur $\mathbf{Q}$. Donc σ est déterminé par l'image de θ et l'image de i ce qui ne fait plus que 16 possibilités et cela décrit donc tous les éléments de G. Noter que l'existence, pour chaque couple formé d'un conjugué de θ et d'un conjugué de i, d'un éléments du groupe de Galois qui envoie (θ, i) sur ce couple, résulte du dénombrement que nous venons de faire.

Comme $\theta^4 = \sqrt{2} = \zeta + \zeta^7$, les images par un automorphisme de K de θ et ζ doivent vérifier cette relation, ce qui justifie la réduction de 32 à 16.

b) Compositum d'une extension finie et d'une extension Galoisienne

Référence : polycopié online de Robert B. Ash (`www.math.uiuc.edu/~ash/Algebra.html`) Abstract algebra basic graduate year 11/02 Chapter 6 Galois Theory p.6 Theorem 6.2.2)

Dans la correspondance de Galois, si H_1 et H_2 sont deux sous-groupes du groupe de Galois, quel est le corps fixé par $H_1 \cap H_2$? Si K_1 et K_2 sont deux corps intermédiaires, quel est le groupe de Galois associé à $K_1 \cap K_2$?

Soient E/F une extension galoisienne (finie) et K/F une extension finie.
Montrer que EF est une extension galoisienne de K.
Montrer que le groupe de Galois de EK/K est (isomorphe à) un sous-groupe du groupe de Galois de E/F. En déduire que $[EK : K]$ divise $[E : F]$. Donner un exemple qui montre que l'hypothèse E/F galoisienne n'est pas superflue.
Montrer que $[EK : K] = [E : F]$ si et seulement si $E \cap K = F$.
On suppose de plus que l'extension K/F est galoisienne. Montrer que le groupe de Galois $G(EK/E \cap K)$ de EK sur $E \cap K$ est le produit direct de ses deux sous-groupes $G(EK/E)$ et $G(EK/K)$.

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] M. Hindry – *Arithmétique*, Calvage et Mounet, Tableau Noir, Paris, 2008.

[5] S. Lang – *Algèbre*, Dunod, 2004.