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

Michel Waldschmidt
date de mise à jour: 06/02/2007

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 2 : sections 1.5 à 1.8 (10 pages) [1]

1.5 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 1.15. *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 1.13 il existe un isomorphisme ψ de L sur $L(\beta')$ dont la restriction à $K(\beta)$ est σ. Le lemme 1.14 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.

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

Proposition 1.16. *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 1.15 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 1.13 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 1.16 permet de donner une caractérisation des extensions normales :

Corollaire 1.17. *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 1.14 et du théorème 1.15.

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 1.16) 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 $\beta \in L$.

□

1.6 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 1.18. *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 1.18 que tout corps de caractéristique nulle est parfait.

Démonstration du lemme 1.18. 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 1.19. *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 1.20. *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 1.20. Pour chaque $\sigma \in H(k, L, N)$ choisissons un prolongement de σ en un automorphisme $\overline{\sigma}$ de N (proposition 1.16). 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 1.19. Si l'extension K/k est monogène on écrit $K = k(x)$ avec $x \in K$; il y a d conjugués $x_1, \dots, x_d$ 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 1.1 et 1.20.

□

Une première application du théorème 1.19 est le *théorème de l'élément primitif* :

Corollaire 1.21. *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 au § 2 que si k est un corps fini, alors toute extension finie de k est séparable sur k et 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.

1.7 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 $1 \le k \le n$ vérifiant $\operatorname{pgcd}(n,k)=1$. 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 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 $n \ge 1$,

$$X^n - 1 = \prod_{d|n} \Phi_d(X). \tag{1.22}$$

Les premiers polynômes cyclotomiques sont

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

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

Théorème 1.23. *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 1.23 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 1.24 (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

$$\Psi_p : \mathbf{Z}[X] \to \mathbf{F}_p[X] \tag{1.25}$$

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 $\Psi_p(f) \ne 0$ et $\Psi_p(g) \ne 0$. Comme p est premier, l'anneau $\mathbf{F}_p[X]$ est intègre, donc $\Psi_p(fg) = \Psi_p(f)\Psi_p(g) \ne 0$, ce qui montre que fg n'appartient pas au noyau de Ψ_p.

□

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 1.24 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 1.23 utilisera le lemme suivant, sur lequel nous reviendrons au § 2 :

Lemme 1.26. *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 1.23. 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 (1.22). 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 (1.25). dans la démonstration du lemme 1.24. 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 1.26 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 $g = 1$.

□

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 (1.25) : on note encore Φ_n cette image.

Proposition 1.27. *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 (1.22) cela signifie donc qu'elle est racine de Φ_n.

□

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 $\{1, \zeta, \dots, \zeta^{\varphi(n)-1}\}$ est une base de R_n comme espace vectoriel sur $\mathbf{Q}$.

Proposition 1.28. *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 $(\mathbf{Z}/n\mathbf{Z})^\times$.

□

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

1.8 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 1.29. *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 $K\big(\sigma(\alpha_1), \ldots, \sigma(\alpha_{i-1})\big)$). □

Théorème 1.30. *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 1.19 (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 1.29) $L = K(\alpha_1, \ldots, \alpha_m)$ 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.

□

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.*

Des définitions on déduit immédiatement :

Lemme 1.31. *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 1.32.
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.*
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 $P(\alpha) = 0$ α est algébrique sur K. Soit f le polynôme irréductible de α sur K. Comme $P \in K[X]$ s'annule en α, 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 $\leq |G|$ sur K ; d'après le corollaire 1.21 toute extension finie de K contenue dans L a un degré $\leq |G|$; donc L est une extension finie de K et $[L : K] \leq |G|$. Mais on a $[L : K] = \mathrm{Aut}(L/K)$; 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. D'après ce que nous venons de voir il existe des éléments $\sigma_1, \dots, \sigma_d$ dans $\mathrm{Aut}(L/K)$ tels que le polynôme irréductible de α sur K s'écrive $\prod_{j=1}^d \big(X - \sigma_j(\alpha)\big)$. Alors $\alpha \in L^{\mathrm{Aut}(L/K)}$ équivaut à $d = 1$, donc à $\alpha \in K$.

□

Du théorème 1.32 (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 1.33 (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 1.32. 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 1.32 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 $\mathrm{Aut}(M/K)$.

□

Une extension galoisienne est dite *abélienne, cyclique, résoluble,...* si son groupe de Galois l'est.