Université P. et M. Curie (Paris VI) date de mise à jour: 22/02/2011
Deuxième semestre 2010/2011

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

Théorie des nombres

Michel Waldschmidt

code UE : MMAT4020 code Scolar : MM020

Objectifs et descriptions

Ce cours vise à donner les bases de l'arithmétique, de la théorie algébrique des nombres et de la théorie analytique des nombres. Il est aussi utile en cryptographie et en théorie des codes.

Prérequis

Des connaissances en algèbre du niveau licence.

Contenu :

Arithmétique : factorisation, équations diophantiennes, fractions continues, approximation diophantienne, irrationalité et transcendance.

Extensions algébriques, corps de rupture et corps de décomposition, clôture algébrique, extensions normales et séparables, polynômes cyclotomiques.

Corps finis (existence, unicité, structure, construction, décomposition des polynômes cyclotomiques, loi de réciprocité quadratique, automorphisme de Frobenius et théorie de Galois). Polynômes à coefficients dans un corps fini. Applications : cryptographie, codes correcteurs d'erreurs.

Corps de nombres, norme, trace, discriminant ; entiers algébriques, unités et idéaux d'un corps de nombres, décomposition des idéaux premiers dans une extension.

Références

[1] H. Cohen – *A course in computational algebraic number theory*, Graduate texts in Math. **138**, Springer Verlag (1993).

[2] M. Demazure – *Cours d'algèbre. Primalité. Divisibilité. Codes*, Nouvelle Bibliothèque Mathématique Cassini, Paris, 1997.

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

[4] D. Duverney – *Théorie des nombres : cours et exercices corrigés*, Paris : Dunod. viii, 244 p., 1998.

[5] G.H. Hardy & E.M. Wright – *An introduction to the theory of numbers*, Oxford University Press, 1938. Fifth Ed. 1979.

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

[7] S. Lang – *Algèbre*, Dunod, 2004.

[8] R. Lidl & H. Niederreiter – *Introduction to finite fields and their applications*, Cambridge Univ. Press, 1994.
http://www.amazon.com/gp/reader/0521460948/ref=sib_dp_ptu#reader-link

[9] P. Samuel – *Théorie algébrique des nombres*, Hermann, Paris, 1967.

[10] V. Shoup – *A Computational Introduction to Number Theory and Algebra* (Version 2) second print editon, Fall 2008. Version électronique téléchargeable intégralement :
http://shoup.net/ntb/

De nombreux documents sont disponibles sur la toile. Voir notamment

MIT's open courseware
http://ocw.mit.edu/OcwWeb/web/home/home/index.htm
ainsi que la liste sur la page Online number theory lecture notes
http://www.numbertheory.org/ntw/lecture_notes.html
du site du réseau de théorie des nombres
http://www.numbertheory.org/ntw/web.html

Voir aussi
Robert B. Ash, Abstract Algebra : The Basic Graduate Year.
http://www.math.uiuc.edu/∼r-ash/Algebra.html
A.A. Pantchichkine, Magistère de Mathématiques (ENS Lyon), Algèbre 2, § 3.1.
http://www-fourier.ujf-grenoble.fr/%7Epanchish/05ensl.pdf

Sur le site
http://lib.org.by/
on trouve un grand nombre d'ouvrages à télécharger, ceux de théorie des nombres sont à la page
http://lib.org.by/_djvu/M_Mathematics/MT_Number%20theory/

Des informations biographiques généralement fiables concernant un grand nombre de mathématiciens sont données sur le site internet
The MacTutor History of Mathematics archive
http://www-gap.dcs.st-and.ac.uk/∼history/

Cours du mardi 4 et vendredi 7 janvier 2011 :

Résultats récents en théorie des nombres.

Référence :
Adam Grygiel : *Progress in number theory in the years 1998-2009.*
http://lanl.arxiv.org/abs/1010.2484
Voir aussi le texte de Michel Balazard : *Un siècle et demi de recherches sur l'hypothèse de Riemann*, Gazette de la Société Mathématique de France, **126** (2010), 7-24.
http://smf4.emath.fr/Publications/Gazette/2010/126/smf_gazette_126_7-24.pdf

Cours du mardi 11 et du vendredi 14 janvier 2011 :

L'équation dite de Pell-Fermat $x^2 - dy^2 = \pm 1$.

Références :
Présentation beamer :
http://www.math.jussieu.fr/∼miw/articles/pdf/PellFermat2011.pdf
Démonstrations :
http://www.math.jussieu.fr/∼miw/articles/pdf/BamakoPell2010.pdf

Voir aussi le texte de Marie-José Pestel : *2000 ans d'énigmes mathématiques*, Gazette de la Société Mathématique de France, **126** (2010), 47-57.
http://smf4.emath.fr/Publications/Gazette/2010/126/smf_gazette_126_47-57.pdf

1 Extensions Algébriques

Quelques rappels

Il est bon de réviser tout ce qui concerne l'arithmétiques sur $\mathbf{Z}$, les notions de divisibilité, le pgcd, l'algorithme d'Euclide, la relation de Bézout, les congruences. Il faut aussi connaître la théorie des groupes, la notion de morphisme, de sous-groupe et de quotient, les propriétés des groupes cycliques, la notion d'ordre (pour un groupe fini ou pour un élément de torsion). On utilisera aussi les propriétés fondamentales de l'anneau des polynômes sur un corps ou sur un anneau.

Le théorème de factorisation des applications entre ensemble, des applications linéaires entre espaces vectoriels, des morphismes entre groupes ou anneaux, est un outil indispensable qu'il faut maîtriser. Il joue un rôle essentiel quand on travaille avec des quotients.

Les chapitres 1, 8, 9, 14 et 15 ainsi que les débuts des chapitres 2 et 4 notamment de [10] sont conseillés.

On peut aussi consulter [7] (Chap. 2), [9] (§ 1.1) et [4] (notamment le chapitre 5) pour revoir les notions de base sur la divisibilité dans les anneaux (on les suppose toujours commutatifs unitaires et, sauf mention explicite du contraire, intègres), sur les corps (ils sont toujours supposés commutatifs), sur les *unités* d'un anneau (= éléments inversibles), les éléments *irréductibles*, les éléments *premiers* (dans un anneau intègre tout premier est irréductible), les idéaux, ainsi que les notions d'anneau principal, factoriel et euclidien.

Dans un anneau, l'élément neutre pour la multiplication (noté 1) est différent de l'élément neutre pour l'addition (noté 0). Un anneau a donc au moins deux éléments. L'homomorphisme canonique de $\mathbf{Z}$ dans un anneau A a pour noyau un idéal premier de $\mathbf{Z}$ (car A est supposé intègre), donc de la forme $\{0\}$ ou $p\mathbf{Z}$ avec p premier. Dans le premier cas, l'anneau A est de *caractéristique nulle* et on identifie $\mathbf{Z}$ à un sous-anneau de A, dans le second A est de *caractéristique* p et on identifie le corps fini $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ à un sous-anneau de A.

Une intersection de sous–anneaux est un sous-anneau, ce qui permet de définir le *sous-anneau de A engendré par une partie E de A* : c'est l'intersection de tous les sous-anneaux de A contenant E, qui est le plus petit sous-anneau de A contenant E. Par exemple, quand E est l'ensemble vide, on obtient ainsi le plus petit sous-anneau de A, qui est $\mathbf{Z}$ en caractéristique nulle et $\mathbf{F}_p$ en caractéristique p. Quand B est un sous-anneau de A et E une partie de A, on désigne par $B[E]$ le sous-anneau de A engendré par $B \cup E$. Si E est un ensemble fini $\{x_1, \ldots, x_n\}$, on écrit $B[x_1, \ldots, x_n]$ au lieu de $B[\{x_1, \ldots, x_n\}]$: c'est l'image de l'unique homomorphisme de B–algèbres de l'anneau des polynômes $B[X_1, \ldots, X_n]$ dans A qui envoie X_i sur x_i.

De même une intersection de sous-corps d'un corps K est un sous-corps de K. Si k est un sous-corps de K et E une partie de K, on désigne par $k(E)$ le sous corps de K engendré par $k \cup E$: c'est le corps des fractions de $k[E]$. Ainsi $k(E)$ est l'ensemble des éléments de K de la forme $R(\alpha_1, \ldots, \alpha_n)$ quand $\{\alpha_1, \ldots, \alpha_n\}$ décrit les familles finies d'éléments de E et R l'ensemble des fractions rationnelles dans $k(X_1, \ldots, X_n)$ dont le dénominateur ne s'annule pas au point $(\alpha_1, \ldots, \alpha_n)$.

On écrit encore $k(E, E')$ au lieu de $k(E \cup E')$ et $k(\alpha)$ au lieu de $k(\{\alpha\})$.

1.1 Extensions de corps

Soient L un corps et K un sous-corps de L. On dit alors que L est une *extension* de K. On écrit aussi une telle extension L/K. Dans ces conditions L est un K-espace vectoriel. On dit que

l'extension est *finie* si le K-espace vectoriel L est de dimension finie sur K. Cette dimension est notée $[L : K]$ et appelée le *degré* de l'extension L/K. On a $[L : K] = 1$ si et seulement si $L = K$.

Un *corps de nombres* est une extension finie du corps $\mathbf{Q}$ des nombres rationnels. Des exemples de corps de nombres sont

$$\mathbf{Q}(i), \quad \mathbf{Q}(\sqrt{2}), \quad \mathbf{Q}(e^{2i\pi/n}).$$

Une extension L/K est *de type fini* s'il existe un ensemble fini E tel que $L = K(E)$. Elle est *monogène* s'il existe $\alpha \in L$ tel que $L = K(\alpha)$; dans ce cas α est un *générateur* de l'extension L/K.

Lemme 1.1. *Soient $K \subset L \subset F$ trois corps. L'extension F/K est finie si et seulement si les deux extensions L/K et F/L sont finies. Dans ce cas $[F : K] = [F : L][L : K]$.*

$$\begin{matrix} & F & \\ [F:L] & | & \\ & L & \end{matrix}\Bigg)[F:K]$$
$$\begin{matrix} [L:K] & | \\ & K \end{matrix}\Big($$

Démonstration. Si $\{\alpha_i \ ; \ i \in I\}$ est une base de L/K et $\{\beta_j \ ; \ j \in J\}$ est une base de F/L, alors $\{\alpha_i\beta_j \ ; \ (i,j) \in I \times J\}$ est une base de F/K.

□

Avec les notations du lemme 1.1, on a les équivalences

$$[L : K] = 1 \Longleftrightarrow [F : L] = [F : K] \Longleftrightarrow L = K$$

et

$$[F : L] = 1 \Longleftrightarrow [L : K] = [F : K] \Longleftrightarrow L = F.$$

1.2 Extensions algébriques et extensions transcendantes

Soient A un anneau, K un sous-corps de A et α un élément de A. Considérons l'homomorphisme de K-algèbres $\Phi : K[X] \to A$ qui envoie X sur α. Son image $K[\alpha]$ est le sous anneau de A engendré par $K \cup \{\alpha\}$, son noyau $\ker \Phi$ est un idéal de $K[X]$. Les deux anneaux $K[X]/\ker\Phi$ et $K[\alpha]$ sont isomorphes.

Si $\ker \Phi = \{0\}$, c'est-à-dire si Φ est injectif, on dit que α est *transcendant* sur K. Alors les anneaux $K[X]$ et $K[\alpha]$ sont isomorphes et le corps des fractions $K(\alpha)$ de $K[\alpha]$ est isomorphe au corps des fractions rationnelles $K(X)$.

Supposons $\ker \Phi \neq \{0\}$. On dit alors que α est *algébrique* sur K. L'anneau $K[X]$ est principal, donc il existe un unique polynôme unitaire $f \in K[X]$ qui engendre l'idéal $\ker \Phi$. C'est le polynôme de degré *minimal* qui s'annule en α. Comme A est intègre, ce polynôme est irréductible dans l'anneau $K[X]$; on dit que f est *le polynôme irréductible*[1] *de α sur K*. L'idéal $\ker \Phi$ est maximal, le quotient $K[X]/\ker\Phi$ est un corps, donc $K[\alpha] = K(\alpha)$. L'extension $K(\alpha)/K$ est finie, de degré $[K(\alpha) : K]$ le degré du polynôme f, qu'on appelle encore le *degré* de α sur K. Une base de $K(\alpha)$ comme K-espace vectoriel est $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$.

1. Dans certains ouvrages ce que nous appelons polynôme irréductible est appelé *polynôme minimal de α sur K*. Nous garderons l'appellation *polynôme minimal* pour le polynôme irréductible sur $\mathbf{Z}[X]$ d'un nombre algébrique.

Une extension L/K est dite *algébrique* si tout élément de L est algébrique sur K. Dans le cas contraire on dit qu'elle est *transcendante*. Comme nous l'avons vu, quand le corps de base K est celui des rationnels, on dit seulement qu'un nombre est *algébrique* ou *transcendant*, en sous-entendant *sur* $\mathbf{Q}$.

Lemme 1.2. *Si L/K est une extension finie, alors c'est une extension algébrique et, pour tout $\alpha \in L$, le degré $[K(\alpha) : K]$ de α sur K divise le degré $[L : K]$ de L sur K.*

Démonstration. L'extension L/K étant finie, pour tout $\alpha \in L$, les éléments

$$1, \alpha, \alpha^2, \dots, \alpha^n, \dots$$

sont liés dans le K-espace vectoriel L, donc α est algébrique sur K. Comme $K(\alpha)$ est un sous-corps de L contenant K, son degré $[K(\alpha) : K]$ sur K divise $[L : K]$, d'après le lemme 1.1. □

L

|

$K(\alpha)$

|

K

Par exemple quand α est algébrique sur K, pour tout $\beta \in K(\alpha)$ le degré de β sur K divise le degré de α sur K.

Il résulte aussi du lemme 1.2 que si L est une extension finie de K de degré premier p, alors pour tout élément α de L qui n'est pas dans K on a $L = K(\alpha)$. Dans ce cas en effet, il n'y a pas de sous–corps de L contenant K autres que K et L.

Lemme 1.3. *Soit L/K une extension et soient $\alpha_1, \dots, \alpha_m$ des éléments de L qui sont algébriques sur K. Alors $K(\alpha_1, \dots, \alpha_m)$ est une extension finie de K.*

Démonstration. On peut démontrer ce résultat par récurrence sur m. Pour $m = 1$ l'extension $K(\alpha_1)/K$ est finie car α_1 est algébrique sur K. Comme α_m est algébrique sur K, il l'est sur le corps $K(\alpha_1, \dots, \alpha_{m-1})$ et le lemme 1.1 joint à l'hypothèse de récurence permet de conclure. □

Il est évident qu'une extension finie est de type fini et, d'après le lemme 1.2, elle est aussi algébrique ; le lemme 1.3 montre que, réciproquement, une extension algébrique de type fini est finie.

Lemme 1.4. *Soient $K \subset L \subset E$ trois corps. L'extension E/K est algébrique si et seulement si les deux extensions L/K et E/L sont algébriques.*

Démonstration. Si l'extension E/K algébrique, il est clair sur la définition que chacune des deux extensions L/K et E/L est algébrique. Inversement, supposons les deux extensions L/K et E/L algébriques. Soit $\alpha \in E$. Comme E est algébrique sur L, il existe un polynôme non nul de $L[X]$ qui s'annule en α. Soient $a_0, \dots, a_m$ ses cœfficients ; chacun d'eux est un élément de L, donc est algébrique sur K. Maintenant α est algébrique sur $K(a_0, \dots, a_m)$. Le lemme 1.1 montre que l'extension $K(a_0, \dots, a_m, \alpha)/K$ est finie, donc (lemme 1.2) algébrique et ainsi α est algébrique sur K.

□

Lemme 1.5. *Soit L/K une extension et soit A une partie de L. On suppose que tous les éléments de A sont algébriques sur K. Alors $K(A)$ est une extension algébrique de K et on a $K[A] = K(A)$.*

Démonstration. Soit $\beta \in K(A)$. Il existe une partie finie $\{\alpha_1, \ldots, \alpha_m\}$ de A telle que $\beta \in K(\alpha_1, \ldots, \alpha_m)$. Le lemme 1.4 montre que β est algébrique sur K. Il reste à vérifier que $K[A]$ est un corps. Soit $\gamma \in K[A]$, $\gamma \neq 0$. Alors $K[\gamma] \subset K[A]$ et comme γ est algébrique sur K on a $K(\gamma) = K[\gamma]$, d'où $\gamma^{-1} \in K[A]$.

□

Exercice. Soient L/K une extension, $\alpha \in L$ un élément algébrique sur K de degré d et soit

$$\gamma = a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1}$$

un élément non nul de $K(\alpha)$ avec $a_i \in K$ $(0 \leq i \leq d-1)$. On note P le polynôme irréductible de α sur K. En utilisant l'algorithme d'Euclide pour calculer un pgcd, dire comment on peut écrire $1/\gamma$ sous la forme

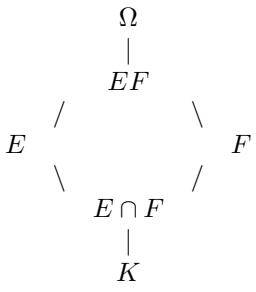
$$\frac{1}{\gamma} = b_0 + b_1\alpha + \cdots + b_{d-1}\alpha^{d-1}$$

avec $b_i \in K$ $(0 \leq i \leq d-1)$.

Soient E et F deux sous-corps d'un corps Ω. L'intersection de tous les sous-corps de Ω qui contiennent $E \cup F$ est le plus petit sous-corps de Ω qui contienne E et F, c'est à la fois $E(F)$ et $F(E)$. On le note EF et on l'appelle *le composé* (ou *compositum*) de E et F.

Quand K est un sous corps de $E \cap F$, on a $EF = K(E, F)$; de plus l'extension EF/K est finie (resp. algébrique) si et seulement si les deux extensions E/K et F/K sont finies (resp. algébriques).

Lemme 1.6. *Soient Ω/K une extension de corps, E et F deux sous-corps de Ω qui contiennent K. Si l'extension F/K est algébrique, alors l'extension EF/E est aussi algébrique et $EF = E[F]$.*



Démonstration. Soit $\alpha \in F$. Par hypothèse α est algébrique sur K, donc sur E. Le lemme 1.5 avec $A = F$ et $L = EF$ montre que $E[F] = E(F)$ et que l'extension $E(F)/E$ est algébrique. □

Soit Ω/K une extension de corps. On dit que K est *algébriquement fermé* dans Ω si tout élément de Ω algébrique sur K appartient à K.

Exemple 1. *On montre dans le cours d'analyse complexe que le corps $\mathbf{C}(z)$ des fractions rationnelles est algébriquement fermé dans le corps des fonctions méromorphes sur $\mathbf{C}$.*

Lemme 1.7. *Soit Ω/K une extension. L'ensemble E des éléments de Ω algébriques sur K est un corps, algébriquement fermé dans Ω.*

Démonstration. Soient α et β deux éléments de E. Les lemmes 1.2 et 1.3 entraînent que l'extension $K(\alpha,\beta)$ est algébrique, donc $\alpha+\beta \in E$ et $\alpha\beta \in E$; de plus $\alpha^{-1} \in E$ si $\alpha \neq 0$.

Soit γ un élément de Ω algébrique sur E. L'extension $E(\gamma)/E$ est finie (lemme 1.3), donc algébrique (lemme 1.2), par conséquent $E(\gamma)$ est une extension algébrique de K (lemme 1.4). Il s'ensuit que γ est algébrique sur K, et par définition de E cela veut dire que γ est dans E.

□

Ce corps E, qui est la plus grande extension algébrique de K contenue dans Ω, est la *fermeture algébrique de K dans Ω*. C'est aussi la plus petite extension de K contenue dans Ω qui soit algébriquement fermée dans Ω.

On désignera par $\overline{\mathbf{Q}}$ l'ensemble des nombres complexes algébriques sur $\mathbf{Q}$; c'est le *corps des nombres algébriques*. La fermeture algébrique de $\mathbf{Q}$ dans $\mathbf{R}$ est le corps $\overline{\mathbf{Q}} \cap \mathbf{R}$ des nombres algébriques réels.

Exercice. Montrer que $\overline{\mathbf{Q}}$ est une extension algébrique de $\mathbf{Q}$ qui n'est pas finie.

Un corps Ω est dit *algébriquement clos* s'il vérifie les propriétés équivalentes suivantes :
(i) tout polynôme non constant de $\Omega[X]$ a au moins une racine dans Ω
(ii) tout polynôme non constant de $\Omega[X]$ se décompose complètement dans $\Omega[X]$
(iii) les éléments irréductibles de l'anneau $\Omega[X]$ sont les polynômes de degré 1.

Un corps algébriquement clos est algébriquement fermé dans toute extension.

Si K est un corps, une extension Ω de K est appelée *clôture algébrique de K* si Ω est un corps algébriquement clos et Ω/K est une extension algébrique.

Quand Ω est un corps algébriquement clos et K un sous-corps de Ω, la fermeture algébrique de K dans Ω est une clôture algébrique de K.

Exemple 2. *Le corps $\mathbf{C}$ est algébriquement clos et $\overline{\mathbf{Q}}$ est une clôture algébrique de $\mathbf{Q}$ (voir par exemple [9] § 2.3 et appendice du Chap. 2, [7] Chap. V § 2).*

Nous admettrons l'existence, pour tout corps K, d'un corps Ω algébriquement clos contenant K (voir par exemple [7] Chap. V § 2 Theorem 2.5).

Théorème 1.8. *Tout corps K admet une clôture algébrique.*

Démonstration. Soit Ω un corps algébriquement clos contenant K. Soit $\overline{K}$ la fermeture algébrique de K dans Ω. Alors $\overline{K}$ est une clôture algébrique de K. □

Remarque. On peut aussi montrer que si $\overline{K}_1$ et $\overline{K}_2$ sont deux clôtures algébriques de K, alors il existe un isomorphisme de $\overline{K}_1$ sur $\overline{K}_2$ dont la restriction à K est l'identité. Il n'y a pas unicité d'un tel isomorphisme : le groupe des automorphismes d'une clôture algébrique de K dont la restriction à K est l'identité est le *groupe de Galois absolu de K*.

Étant donné que tout homomorphisme d'un corps dans un anneau est injectif, se donner une extension revient à se donner un homomorphisme d'un corps dans un autre. Plus précisément, si $\sigma : K \to L$ est un homomorphisme de corps, alors le corps $\sigma(K)$ est isomorphe à K et L est une extension de $\sigma(K)$. Dans ces conditions on dit que σ est un isomorphisme de K *dans* L. On étend σ en l'unique homomorphisme (encore noté σ) de $K[X]$ dans $L[X]$ qui envoie X sur X et coïncide avec σ sur K :

$$\sigma\big(a_0 + a_1X + \cdots + a_nX^n\big) = \sigma(a_0) + \sigma(a_1)X + \cdots + \sigma(a_n)X^n.$$

Soient E et L deux extensions d'un même corps K et soit $\sigma : E \to L$ un isomorphisme de E dans L. On dit que σ est un *K-isomorphisme* si la restriction de σ à K est l'identité.

Si E_1 et E_2 sont deux corps entre lesquels il existe un homomorphisme de corps $\sigma : E_1 \to E_2$, alors E_1 et E_2 ont la même caractéristique et le même sous-corps premier F (plus précisément, il y a un isomorphisme unique entre leurs sous-corps premiers, ce qui nous autorise à les identifier). Dans ce cas σ est un F-isomorphisme de E_1 dans E_2.

Soit L/K une extension. Deux éléments α et β de L sont dits *conjugués* sur K s'il existe un K-isomorphisme σ de $K(\alpha)$ dans $K(\beta)$ tel que $\sigma(\alpha) = \beta$. Dans ce cas σ est unique et surjectif. La conjugaison définit une relation d'équivalence sur L.

Lemme 1.9. *Soient L/K une extension et α, β deux éléments de L. Si α est transcendant sur K, alors β est conjugué de α sur K si et seulement si β est aussi transcendant. Si α est algébrique sur K, alors β est conjugué de α si et seulement si β est algébrique sur K avec le même polynôme irréductible que α sur K.*

Démonstration. Si α est transcendant sur K, alors $K(\alpha)$ est isomorphe au corps $K(X)$ des fractions rationnelles sur X, donc à tout $K(\beta)$ avec β transcendant sur K. Dans ces conditions, comme $K(\alpha)$ n'est pas de degré fini sur K, il ne peut pas être isomorphe à $K(\beta)$ quand β est algébrique sur K.

Supposons maintenant α et β algébriques sur K et conjugués. Soit $\sigma : K(\alpha) \to K(\beta)$ un K-isomorphisme tel que $\sigma(\alpha) = \beta$. Notons $f \in K[X]$ le polynôme irréductible de α sur K. On a $f(\alpha) = 0$, donc $\sigma\big(f(\alpha)\big) = 0$. Mais, comme la restriction à K de σ est l'identité et que les coefficients de f sont dans K, on a

$$\sigma\big(f(\alpha)\big) = f\big(\sigma(\alpha)\big) = f(\beta).$$

Donc β est racine de f.

Enfin si α et β sont algébriques racines du même polynôme irréductible $f \in K[X]$, alors $K(\alpha)$ et $K(\beta)$ sont tous deux isomorphes au corps $K[X]/(f)$. En effet le morphisme d'anneaux $K[X] \to K[\alpha]$ qui envoie X sur α et laisse fixe les éléments de K a pour image $K[\alpha] = K(\alpha)$ et pour noyau l'idéal (f) de $K[X]$. L'isomorphisme de corps de de $K(\alpha)$ sur $K(\beta)$ qui rend commutatif le diagramme

$$\begin{array}{ccc} K[X] & \to & K[\beta] \\ \downarrow & \nearrow_{\sigma} & \\ K[\alpha] & & \end{array}$$

n'est autre que l'application K-linéaire σ de $K(\alpha)$ dans $K(\beta)$ définie sur la base $\{1, \alpha, \ldots, \alpha^{n-1}\}$ (où n désigne le degré de α) par $\sigma(\alpha^i) = \beta^i$ $(0 \le i \le n-1)$. □

1.3 Corps de rupture d'un polynôme

Soient K un corps et $f \in K[X]$ un polynôme irréductible. Une extension L/K est un *corps de rupture de f sur K* s'il existe une racine α de f dans L telle que $L = K(\alpha)$.

Exemple 3. *Si 1, j et j^2 désignent les trois racines cubiques de l'unité dans $\mathbf{C}$, chacun des trois corps $\mathbf{Q}(\sqrt[3]{2})$, $\mathbf{Q}(j\sqrt[3]{2})$ et $\mathbf{Q}(j^2\sqrt[3]{2})$ est un corps de rupture sur $\mathbf{Q}$ du polynôme $X^3 - 2$.*

L'existence d'un corps de rupture est donnée par le lemme suivant :

Lemme 1.10. *Soient K un corps et f un polynôme irréductible de $K[X]$. L'idéal principal (f) de $K[X]$ est maximal, le quotient $L = K[X]/(f)$ contient (un sous-corps isomorphe à) K et L est un corps de rupture de f sur K.*

Démonstration. Soit j l'injection naturelle de K dans $K[X]$ et soit $s : K[X] \to K/(f)$ la surjection canonique de noyau l'idéal (f) engendré par f. Alors $\sigma = s \circ j$ est un isomorphisme de K dans L. Soit $\alpha \in L$ la classe de X modulo f et soit $g = \sigma(f) \in \sigma(K)[X]$. On a

$$g(\alpha) = s(f) = 0.$$

Ainsi on voit que L est un corps de rupture sur $\sigma(K)$ du polynôme $g = \sigma(f)$. Comme $\sigma(K)$ est un corps isomorphe à K on peut l'identifier avec K et alors $g = f$. □

Un corps de rupture est unique à isomorphisme près :

Lemme 1.11. *Soient K un corps, f un polynôme irréductible de $K[X]$, $\varphi : K \to K'$ un isomorphisme de K sur un corps K', L un corps de rupture de f sur K, α une racine de f dans L, L' un corps de rupture de φf sur K' et α' une racine de φf dans L'. Alors il existe un unique isomorphisme ψ de L sur L' dont la restriction à K soit φ et tel que $\psi(\alpha) = \alpha'$.*

Démonstration. Comme $L = K(\alpha)$ et $L' = K(\alpha')$, l'unicité de ψ est claire. Pour l'existence, on reprend l'argument de la démonstration du lemme 1.9.

□

Exercice. Soit L/K une extension finie de degré d et soit $P \in K[X]$ un polynôme irréductible sur K de degré m. On suppose que m et d sont premiers entre eux. Montrer que P est irréductible sur L.

1.4 Corps de décomposition d'un polynôme

Comme nous venons de le voir dans le §1.3, un corps de rupture d'un polynôme f irréductible sur un corps K est une extension de K qui contient au moins une racine de f (et qui est minimale pour cette propriété). Nous recherchons maintenant une extension qui contienne toutes les racines de f - il n'est alors plus nécessaire de supposer f irréductible pour étudier la question.

Soient K un corps et f un polynôme non constant de $K[X]$. Quand L est une extension de K, on dit que le polynôme f est *complètement décomposé* dans L si f est produit de facteurs linéaires de $L[X]$. On dit que L est un *corps de décomposition de f sur K* si f est complètement décomposé dans L et s'il existe des racines $\alpha_1, \ldots, \alpha_m$ de f dans L telles que $L = K(\alpha_1, \ldots, \alpha_m)$. Ainsi, f est complètement décomposé dans une extension L de K si et seulement si on peut écrire

$$f(X) = a_0(X - \alpha_1) \cdots (X - \alpha_d)$$

avec $\alpha_1, \ldots, \alpha_d$ dans L (ici d est le degré de f et $a_0 \in K$ est le coefficient directeur de f). Alors *le* corps de décomposition de f dans L est $K(\alpha_1, \ldots, \alpha_d)$.

L'énoncé suivant assure l'existence d'un corps de décomposition.

Lemme 1.12. *Soient K un corps et f un polynôme non constant de $K[X]$. Alors il existe un corps de décomposition L de f sur K.*

Démonstration. On démontre le résultat par récurrence sur le degré d de f. Si $d = 1$ on prend $L = K$. Supposons le résultat vrai pour tous les corps et pour les polynômes de degré $< d$. Soit g un facteur irréductible de f, soit E un corps de rupture sur K de g et soit $\alpha \in E$ une racine de g dans E telle que $E = K(\alpha)$. Alors dans $E[X]$ on a $f(X) = (X - \alpha)h(X)$ avec h de degré $d-1$. Il suffit maintenant de prendre pour L un corps de décomposition de $h(X)$ sur E en utilisant l'hypothèse de récurrence. □

Voici maintenant l'unicité :

Lemme 1.13. *Soient K un corps, f un polynôme non constant de $K[X]$, $\varphi : K \to K'$ un isomorphisme de K sur un corps K', L un corps de décomposition de f sur K et L' un corps de décomposition de φf sur K'. Alors il existe un isomorphisme ψ de L sur L' dont la restriction à K soit φ.*

Démonstration. On va démontrer le résultat par récurrence sur le degré d de f, le cas $d = 1$ étant banal. Supposons le résultat vrai pour tous les corps et tous les polynômes de degré $< d$. Soient g un facteur irréductible de f dans $K[X]$, α une racine de g dans L, α' une racine de $\varphi \circ g$ dans L'. Le lemme 1.11 montre qu'il existe un isomorphisme θ de $K(\alpha)$ sur $K(\alpha')$ qui envoie α sur α' et dont la restriction à K soit φ. On remarque que L est un corps de décomposition sur $K(\alpha)$ du polynôme $h(X) = f(X)/(X - \alpha)$ et L' est un corps de décomposition sur $K'(\alpha')$ du polynôme $\theta\big(h(X)\big) = \varphi\big(f(X)\big)/(X - \alpha')$. L'hypothèse de récurrence permet de conclure.

□

L'isomorphisme ψ qui étend φ n'est en général pas unique. Si on en choisit un, on obtient tous les autres en le composant avec un K-automorphisme de L. Un tel automorphisme est déterminé par son action sur les racines de f, qui est une permutation. La théorie de Galois a pour but d'étudier ces permutations.

Nous allons voir maintenant qu'un corps de décomposition contenu dans une extension E de K est stable sous tout K-automorphisme de E :

Lemme 1.14. *Soit L un corps de décomposition d'un polynôme de $K[X]$, soit E une extension de L et soit σ un K-isomorphisme de L dans E. Alors $\sigma(L) = L$.*

Démonstration. Soient $\alpha_1, \ldots, \alpha_d$ les racines dans L du polynôme considéré. On a $L = K(\alpha_1, \ldots, \alpha_d)$ et σ permute les α_i, donc $\sigma(L) = K(\alpha_1, \ldots, \alpha_d) = L$.

□

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 σ 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 $1 \leq i \leq m$ 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, $K \subset E \subset L$, il résulte du théorème 1.15 que 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 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 parmi les extensions finies :

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) $\mathrm{pgcd}(f, f') = 1$.

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 non nul 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 non nul 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 le polynôme irréductible 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 non nul 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 4. *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 $x_1, \ldots, x_d$ 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 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 $K = k(\alpha)$.*

La démonstration va utiliser le lemme auxiliaire suivant :

Lemme 1.22. *Soient m un entier positif et k un corps ayant au moins m éléments. Si un k–espace vectoriel V est égal à une réunion de m sous-espaces $V_1, \ldots, V_m$, alors V est égal à l'un d'eux.*

Démonstration. On raisonne par récurrence sur m. Le résultat est banal pour $m = 1$ (et aussi pour $m = 2$). Supposons le vrai pour $m - 1$. Soit V un espace vectoriel sur k égal à une réunion de sous-espaces $V = V_1 \cup \cdots \cup V_m$ avec $V_m \neq V$ et $V_m \neq 0$. Soit $t \in V_m$ et soit $x \in V$, $x \notin V_m$. Pour chaque $a \in k$, comme $x + at$ n'appartient pas à V_m, il existe un indice j (dépendant de a) dans l'intervalle $1 \leq j \leq m - 1$ tel que $x + at \in V_j$. Par le principe des tiroirs, il existe un indice j tel

que $x + at \in V_j$ et $x + a't \in V_j$ pour deux éléments distincts a et a' de k. Alors $t \in V_j$, donc V_m est contenu dans $V_1 \cup \cdots \cup V_{m-1}$; il en résulte que V égal à $V_1 \cup \cdots \cup V_{m-1}$, et par l'hypothèse de récurrence il est égal à l'un des sous–espaces $V_1, \ldots, V_{m-1}$. □

Démonstration du corollaire 1.21. Nous verrons au § 2 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 $\sigma_1, \ldots, \sigma_d$ les k-isomorphismes de K dans N.

Comme k est infini, on déduit du lemme 1.22 qu'il existe un élément α de K dont les images $\sigma_1(\alpha), \ldots, \sigma_d(\alpha)$ 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 $\mathrm{pgcd}(n, k) = 1$. 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 $n \geq 1$,

$$X^n - 1 = \prod_{d|n} \Phi_d(X). \tag{1.23}$$

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 1.24. *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 1.24 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 1.25 (Lemme de Gauss)**.** *Pour f et g dans $\mathbf{Z}[X]$ non nuls,*

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

Démonstration. Comme $c(f)$ divise $c(fg)$, il suffit de montrer que le produit de deux polynômes primitifs est primitif, c'est–à–dire que les conditions $c(f) = c(g) = 1$ impliquent $c(fg) = 1$. . 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

$$\Psi_p : \mathbf{Z}[X] \to \mathbf{F}_p[X] \tag{1.26}$$

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.

□

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 1.25 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 1.24 utilisera le lemme suivant, sur lequel nous reviendrons au § 2 :

Lemme 1.27. *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 1.24. 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

$$h(X) = \prod_{\substack{d \mid n \\ d \neq n}} \Phi_d(X)$$

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 (1.23). 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 (1.26). dans la démonstration du lemme 1.25. 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 1.27 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 $\mathrm{pgcd}(m,n) = 1$ est l'ensemble des générateurs de ce groupe, donc l'ensemble des racines de Φ_n. D'où $g = 1$.

Remarque. L'irréductibilité des polynômes cyclotomiques d'indice p premier résulte aussi du *critère d'Eisenstein* : le polynôme

$$\frac{(Y+1)^p - 1}{Y}$$

(obtenu à partir de $(X^p-1)/(X-1)$ par le changement de variable $Y = X-1$) est unitaire, tous ses coefficients sauf le coefficient de Y^{p-1} sont divisible par p, et le terme constant n'est pas divisible par p^2.

□

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 le lemme 1.27 montre que l'on a

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

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 sur la caractéristique qui va apparaître dans la proposition 1.28.

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 (1.26) : on note encore Φ_n cette image.

Proposition 1.28. *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 $X^n - 1$ n'a pas de racines multiples dans un corps de décomposition, donc il 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 (1.23) 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 $\{1, \zeta, \ldots, \zeta^{\varphi(n)-1}\}$ est une base de R_n comme espace vectoriel sur $\mathbf{Q}$.

Proposition 1.29. *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 $\varphi \in \mathrm{Aut}(R_n)$, 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 $\mathrm{Aut}(R_n/\mathbf{Q})$ sur $(\mathbf{Z}/n\mathbf{Z})^\times$.

□

Exemple 5. *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 $[R_n : R_n^+] = 2$.