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

Michel Waldschmidt
date de mise à jour: 25/01/2007

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 1 : introduction + sections 1.1 à 1.4 (10 pages) [1]

Introduction : équations Diophantiennes

Historiquement, la principale source du développement de la théorie algébrique des nombres est le problème de la résolution des équations en nombres entiers ou rationnels. Traditionnellement, on appelle *équation Diophantienne* une équation polynomiale $f(x_1, \ldots, x_n) = 0$, où f est un polynôme à coefficients rationnels, que l'on cherche à résoudre en nombres entiers ou rationnels. *Résoudre* une telle équation signifie d'abord décider si elle a ou non des solutions, quand elle en a il faut ensuite dire si leur ensemble est fini ou non, et pour la résoudre complètement il faut enfin déterminer toutes les solutions.

Un exemple simple est l'équation $y(y-1) = x^2$. Elle a 2 solutions en nombres entiers, à savoir $(x, y) = (0, 0)$ et $(0, 1)$, tandis qu'elle a une infinité de solutions en nombres rationnels : pour chaque nombre rationnel t distinct de ± 1 le couple

$$(x, y) = (t/(t^2-1)\ ,\ t^2/(t^2-1)) \in \mathbf{Q} \times \mathbf{Q}$$

est solution, et on les obtient toutes ainsi à part $(0, 1)$ (qu'on retrouverait en passant en coordonnées projectives, ce qui revient à prendre $t = \infty$).

Un des premiers mathématiciens à avoir considéré ce genre de question est Diophante d'Alexandrie (325–409). La traduction, par Bachet de Méziriac (1581–1638) de la partie de ses œuvres qui était parvenue dans le monde occidental grâce aux mathématiciens arabes a été la source d'inspiration de Fermat (1601–1665). Beaucoup d'énoncés formulés par Fermat, et bien d'autres, ont été démontrés par Euler (1707–1783). La théorie des équations quadratiques fait l'objet de nombreux travaux à partir du XVIIIè siècle, notamment par Lagrange (1736–1813) et Gauss (1777-1855). Le "dernier théorème de Fermat", selon lequel l'équation $x^n + y^n = z^n$ n'a pas de solution en nombres rationnels non nuls x, y, z dès que l'entier n est supérieur ou égal à 3, reste un défi jusqu'en 1994 où A. Wiles en donnera enfin une démonstration complète. Il motive les recherches de Kummer (1810–1893), Dedekind (1831–1916), Dirichlet (1805–1859) et bien d'autres ; c'est ce problème qui est à l'origine des principaux concepts dont il sera question dans ce cours.

Jusque vers la fin du XIXème siècle les méthodes employées seront spécifiques aux équations considérées. Il faudra attendre les contributions de Hurwitz (1859–1919) et Poincaré (1854–1912)

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

pour disposer d'énoncés portant sur des classes générales d'équations. Le début du XXème siècle verra apparaître d'abord les méthodes d'approximation diophantienne avec les travaux de Thue (1863–1922), puis grâce à ces outils puissants les résultats de Siegel (1896–1981) sur les points entiers sur des courbes algébriques (il s'agit de décider si une équation $f(x, y) = 0$ a une infinité de solution entières, Siegel donne en 1929 des conditions nécessaires et suffisantes sur le polynôme $f \in \mathbf{Z}[X]$). Un énoncé semblable pour les points rationnels a été proposé par Mordell (1888–1972) et démontré par G. Faltings en 1983. On sait maintenant dire si une équation Diophantienne $f(x, y) = 0$ a une infinité de solution rationnelles ou non, mais quand il y en a seulement un nombre fini on ne sait pas encore les déterminer toutes : on sait cependant en majorer le nombre.

Pour les équations Diophantiennes faisant intervenir un plus grand nombre de variables, Yu.V. Matiyasevich a résolu par la négative en 1970 une question posée par Hilbert en 1900 : *il n'y a pas d'algorithme général permettant de déterminer si une équation en nombres entiers $f(x_1, \ldots, x_n)$ a ou non une infinité de solutions dans $\mathbf{Z}^n$.*

Une extension de la notion d'équation Diophantienne est celle *d'équation Diophantienne exponentielle*, dans laquelle certains exposants sont considérés comme des inconnues. Une des plus connues est celle proposée en 1844 par Catalan $x^p - y^q = 1$, où les inconnues (x, y, p, q) sont des entiers tous ≥ 2. Catalan (1814-1894) a conjecturé que la seule solution était $(3, 2, 2, 3)$ correspondant à $3^2 - 2^3 = 1$. Cette conjecture a été démontrée en 2003 par Preda Mihailescu. Une démonstration complète et détaillée est donnée par H. Cohen [1].

Une question plus vaste que celle de Catalan a été posée par S.S. Pillai (1901–1950) en 1945 : *pour chaque entier $k > 0$, l'équation $x^p - y^q = k$ n'a qu'un nombre fini de solutions en entiers (x, y, p, q) tous ≥ 2.* Il n'y a que le cas $k = 1$ qui soit résolu. La conjecture de Pillai signifie que la distance entre deux termes consécutifs de la suite

$$1, 4, 8, 9, 16, 25, 27, 32, 36, 49, 64, 81, 100, 121, 125, 128, 144, \ldots$$

des puissance parfaites tend vers l'infini.

Remarque : On trouve des informations biographiques concernant les différents mathématiciens cités sur le site internet
The MacTutor History of Mathematics archive
http ://www-gap.dcs.st-and.ac.uk/∼history/

Considérons pour commencer la plus simple des équations Diophantiennes en deux variables : on fixe deux entiers a et b et on cherche à résoudre l'équation $ax + by = 0$ où les inconnues x, y sont dans $\mathbf{Z}$. Si on note d le pgcd de a et b, et $a' = a/d$, $b' = b/d$, alors la solution générale est $(x, y) = (tb', -ta')$, $t \in \mathbf{Z}$. Cet exemple élémentaire se généralise aisément aux systèmes de m équations en n inconnues : on se donne une matrice de format $m \times n$ à coefficients entiers et on cherche les vecteurs colonnes $X = {}^t(x_1, \ldots, x_n)$ à coefficients dans $\mathbf{Z}$ qui satisfont $AX = 0$. L'algèbre linéaire permet de résoudre la question.

Si maintenant on se donne, en plus, un vecteur colonne B (matrice $m \times 1$) et que l'on veut résoudre $AX = B$, pour en obtenir la solution générale il suffit d'ajouter à une solution particulière de cette équation la solution générale de l'équation homogène associée $AX = 0$.

Revenant au cas particulier d'une équation en deux inconnues ($m = 1$, $n = 2$), pour résoudre l'équation de Bézout $ax + by = c$ on utilise l'algorithme d'Euclide : cette équation a une solution $(x, y) \in \mathbf{Z} \times \mathbf{Z}$ si et seulement si le pgcd de a et b divise c.

Passons aux équations quadratiques. La plus célèbre est sans doute celle de Pythagore (VIème siècle avant J.-C) : $x^2 + y^2 = z^2$. Comme elle est homogène, la résoudre en nombres entiers

revient à résoudre en nombres rationnels l'équation $x^2 + y^2 = 1$, c'est-à-dire à déterminer les points rationnels sur un cercle. La méthode géométrique, qui permet plus généralement de trouver les points rationnels sur une conique (c'est-à-dire de résoudre en nombres rationnels une équation $f(x, y) = 0$ où f est un polynôme en deux variables de degré 2), consiste à tracer une droite passant par un point rationnel : elle coupe la courbe en question en un autre point et cela fournit une paramétrisation des solutions. Pour le cercle on peut partir par exemple du point $(x, y) = (-1, 0)$ et considérer la droite $y = t(x + 1)$ de pente $t \in \mathbf{Q}$. Le second point d'intersection est obtenu en résolvant l'équation

$$x^2 + t^2(x + 1)^2 - 1 = 0$$

qui possède bien entendu la solution $x = -1$. On peut donc mettre $x+1$ en facteur dans le membre de gauche : si $x \neq -1$ alors on peut diviser par $x + 1$ et l'équation devient linéaire

$$x - 1 + t^2(x + 1) = 0,$$

ce qui donne

$$x = \frac{1 - t^2}{1 + t^2}, \quad y = \frac{2t}{1 + t^2}.$$

Pour chaque $t \in \mathbf{Q}$ ces formules donnent un point rationnel (x, y) sur le cercle, et inversement tout point rationnel sur le cercle distinct de $(-1, 0)$ est de cette forme. On retrouve le point exceptionnel $(-1, 0)$ en autorisant $t = +\infty$, c'est-à-dire en passant en coordonnées projectives. En écrivant $t = a/b$ on retrouve les formules

$$x = \frac{b^2 - a^2}{b^2 + a^2}, \quad y = \frac{2ab}{b^2 + a^2}$$

qui conduisent à la solution générale en nombres entiers de l'équation de Pythagore $x^2 + y^2 = z^2$. On remarque d'abord que si x, y, z sont des entiers positifs qui satisfont $x^2 + y^2 = z^2$, et si d est leur pgcd, alors le triplet (x', y', z') défini par $x' = x/d$, $y' = y/d$, $z' = z/d$ satisfait encore l'équation de Pythagore, et en plus ces trois entiers x', y', z' sont premiers entre eux dans leur ensemble (ils sont même premiers entre eux deux-à-deux). De plus z' est impair. On en déduit facilement que l'un des deux nombres x', y' est pair, l'autre bien entendu est impair. Voici l'énoncé auquel on aboutit (voir par exemple [3], § 1.2, Th.1 ou [2], Th. 5.9).

Théorème 0.1. *Si x, y, z sont des entiers positifs premiers entre eux dans leur ensemble avec y pair qui vérifient l'équation de Pythagore $x^2 + y^2 = z^2$, alors il existe des entiers a et b premiers entre eux tels que*

$$x = b^2 - a^2, \quad y = 2ab, \quad z = b^2 + a^2.$$

Le procédé géométrique de la corde et de la tangente que nous venons de voir est utile aussi pour les équations cubiques : si on dispose d'un point rationnel sur une courbe $f(x, y) = 0$ où f est un polynôme de degré 3, la tangente à la courbe en ce point coupe généralement la cubique en un autre point, si le premier est rationnel alors le second l'est aussi (on est amené à résoudre une équation de degré 3 en x, qui a une racine double, donc se décompose en un produit d'un terme linéaire au carré par un autre terme linéaire). De même si on dispose de deux points rationnels sur la courbe, la droite joignant ces deux points coupe généralement la cubique en un autre point rationnel. C'est la base de la théorie des courbes elliptiques.

Le processus géométrique permet de paramétrer les solutions rationnelles d'une équation de degré 2 en 2 inconnues. Il ne donne pas forcément d'information sur les solutions entières. Par exemple si d est un entier qui n'est pas un carré, les points rationnels $\neq (0,0)$ sur la courbe $x^2 - dy^2 = 1$ sont paramétrés par

$$x = \frac{dt^2+1}{dt^2-1}, \quad y = \frac{2t}{dt^2-1}.$$

Quand d est un entier positif qui n'est pas un carré, l'équation $x^2 - dy^2 = \pm 1$, où les inconnues x et y sont dans $\mathbf{Z}$, porte le nom de Pell–Fermat. Pourtant elles ont été étudiées par le mathématicien indien Brahmagupta (598–670) bien avant Pell (1611–1685) et Fermat. Il a trouvé la plus petite solution en entiers positifs de l'équation $x^2 - 92y^2 = 1$, qui est $(x, y) = (1151\ ,\ 120)$. On peut noter que l'équation $x^2 - 23y^2$ possède la solution $(x, y) = (24, 5)$, puisque $24^2 = 576$ et $5^2 \cdot 23 = 575$. En développant $(24 + 5\sqrt{23})^2 = 1151 + 120\sqrt{23}$ on retrouve la solution donnée par Brahmagupta.

Au XIIème siècle Bhaskara II a trouvé pour l'équation $x^2 - 61y^2 = 1$ (qui sera plus tard considérée par Fermat) la solution

$$(x, y) = (1\,766\,319\,049\ ,\ 226\,153\,980).$$

Plus tard Narayana (∼1340–∼1400) a obtenu pour $x^2 - 103y^2 = 1$ la solution $(x, y) = (227\,528\ ,\ 22\,419)$.

Un algorithme pour résoudre une équation de Pell–Fermat consiste à développer $\sqrt{d}$ en *fraction continue* (voir par exemple [2] Chap. 3 et 4). La résolution de l'équation $x^2 - dy^2 = \pm 1$ est étroitement liée à la recherche des *unités* du corps quadratique $\mathbf{Q}(\sqrt{d})$. Nous allons voir de quoi il s'agit (l'algèbre classique enseigne que les unités d'un corps sont les éléments non nuls du corps, mais en théorie algébrique des nombres ce que l'on appelle *unité d'un corps de nombres* est autre chose).

Quelques rappels

Consulter [3] (§ 1.1) et [2] (notamment le chapitre 5) pour revoir les notions de base sur la divisibilité dans les anneaux (on les suppose toujours commutatifs unitaires), sur les unités (= 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.

1 Extensions Algébriques

Tous les corps sont supposés commutatifs.

Quand K est un corps, l'intersection de tous les sous-corps de K est un sous-corps de K, c'est le plus petit d'entre eux, on l'appelle le *sous-corps premier de* K. Ce sous-corps est isomorphe (de manière unique) soit à $\mathbf{Q}$, soit à un corps $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ avec p nombre premier. On dit que K est de caractéristique 0 dans le premier cas, p dans le second.

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.

Quand L/K est une extension et E une partie de L, on note $K[E]$ le sous-anneau de L engendré par $K \cup E$ et par $K(E)$ le sous-corps de L engendré par $K \cup E$. Ainsi $K(E)$ est le corps des fractions de $K[E]$, c'est l'intersection des sous-corps de L qui contiennent E et K, on l'appelle *sous-corps de L engendré par E sur K*. C'est encore l'ensemble des éléments de L 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 $K(\{\alpha\})$. 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*

$$[F : K] = [F : L][L : K].$$

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. Comme l'anneau $K[X]$ est principal, 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 : on l'appelle le *polynôme minimal de α sur K*. Si $K[\alpha]$ est intègre (ce qui est le cas par exemple quand A lui-même est intègre), alors le polynôme minimal f de α sur K est irréductible dans l'anneau $K[X]$; on dit encore que f est *le polynôme irréductible de α sur K*. L'idéal $\ker \Phi$ est alors 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 $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$.

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*.

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

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

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.

□

Lemme 1.3. *Soit L/K une extension et soient $\alpha_1, \ldots, \alpha_m$ des éléments de L qui sont algébriques sur K. Alors $K(\alpha_1, \ldots, \alpha_m)$ 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 $K(\alpha_1, \ldots, \alpha_{m-1})$ 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 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 $a_0, \ldots, a_m$ ses cœfficients ; chacun d'eux est un élément de L, donc est algébrique sur K. Maintenant α est algébrique sur $K(a_0, \ldots, a_m)$. Le lemme 1.1 montre que l'extension $K(a_0, \ldots, a_m, \alpha)/K$ 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 $\gamma^{-1} \in K[A]$.

□

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 L/K une extension de corps, E et F deux sous-corps de L qui contiennent K. Si l'extension F/K est algébrique, alors l'extension EF/E est aussi algébrique.*

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

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

Exemple. On peut montrer 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 L/K une extension. L'ensemble E des éléments de L algébriques sur K est un corps, algébriquement fermé dans L.*

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

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.

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. Le corps $\mathbf{C}$ est algébriquement clos et $\overline{\mathbf{Q}}$ est une clôture algébrique de $\mathbf{Q}$.

Nous admettrons l'existence, pour tout corps K, d'un corps Ω algébriquement clos contenant K.

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.

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 $\sigma(\alpha^i) = \beta^i$ $(0 \leq i \leq n-1)$. □

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. 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.

□

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 $\sigma(L) = K(\alpha_1, \ldots, \alpha_d) = L$.

□

Références

[1] H. Cohen – *Démonstration de la conjecture de Catalan*, http ://www.math.polytechnique.fr/xups/xups05-01.pdf

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

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

De nombreux documents sont disponibles sur internet. Voir notamment la liste disponible 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