Corps

Christophe Antonini[1], Olivier Teytaud[2], Pierre Borgnat[3], Annie Chateau[4], and Edouard Lebeau[5]

[1]Enseignant en CPGE, Institut Stanislas, Cannes
[2]Chargé de rechercher INRIA, Université d'Orsay, Orsay
[3]Chargé de recherche CNRS, ENS Lyon, Lyon
[4]Maitre de conférence, Université Montpellier-2, Montpellier
[5]Enseignant en CPGE, Lycée Henri Poincaré, Nancy

14 octobre 2022

Théorie des corps finis, extension de corps et théorème de Wedderburn.

1 Corps

Les corps sont la troisième des catégories abstraites classiquement vues en algèbre (après groupes et anneaux). Les corps sont pourtant extrêmement anciens ne fût-ce que pour le cas de $\mathbb{R}$; mais leur formalisation est tardive et leur essort date notamment de la résolution d'équations polynomiales. Les nombres complexes forment un autre corps très important $\mathbb{C}$, qui en est la clôture algébrique. Dans la suite $\mathbb{Z} \to \mathbb{Q} \to \mathbb{R} \to \mathbb{C}$, on utilise consécutivement le passage au corps des fractions ($\mathbb{Z} \to \mathbb{Q}$), le passage au complété ($\mathbb{Q} \to \mathbb{R}$), la clôture algébrique ($\mathbb{R} \to \mathbb{C}$). Ainsi, un anneau (sous certaines hypothèses techniques), peut être plongé dans un corps (le corps des fractions rationnelles), et un corps peut être plongé dans sa clôture algébrique. Des corps très différents (finis) existent aussi, quoiqu'ils soient beaucoup plus abstraits ; typiquement $\mathbb{Z}/p\mathbb{Z}$ avec p premier. Un autre exemple important de corps, non commutatif, est le corps des quaternions.

Après une section dédiée aux généralités, on se penchera sur les extensions de corps et sur les corps finis. Les extensions de corps sont importantes lorsque $k \subset K$ avec k et K des corps avec les mêmes lois. K est alors en particulier une k-algèbre. Pour aller plus loin, on pourra se référer à [**?**, **?**].

1.1 Définitions de base

Définition 0.1 **corps**

Un anneau $(K, +, .)$ est un **corps** si et seulement si le groupe des unités est $K - \{0\}$.
Un corps est dit **commutatif** si l'anneau sous-jacent est commutatif, c'est-à-dire si la multiplication est commutative.
On appelle **caractéristique** d'un corps k le plus petit $n \in \mathbb{N}$, s'il existe, tel que $0 = 1+1+1+\cdots+1$ (n fois). On dit que la caractéristique est nulle en cas contraire.

Propriétés :
•Dans un corps, tout élément est inversible.
•Un anneau commutatif intègre dont tout élément est inversible est un corps.
•Un anneau commutatif non nul est un corps si et seulement si ses seuls idéaux sont les idéaux triviaux.
•Un anneau intègre fini est un corps.

1.2 Extensions de corps

L'intérêt des extensions de corps (corps en contenant un autre) est qu'on arrive à dire des choses, alors que pour les anneaux inclus dans des anneaux, on en dit peu (noter toutefois les corps de fractions, qui étendent des anneaux à condition qu'ils soient intègres). Concrètement, l'intérêt des extensions de corps est aussi de permettre la résolution d'équations polynomiales. Il faut donc connaître quelques extensions fondamentales (parfois triviales, i.e. égales à k) de tout corps k : les corps de rupture "engendrés" par une racine d'un polynôme donné dans $k[X]$, les corps de décomposition "engendrés" par *toutes* les racines d'un polynôme donné, et la clôture algébrique (contenant toutes les racines de tous les polynômes).

Définition 0.2 **sous-corps**

Un sous-anneau L de l'anneau sous-jacent à un corps K est un **sous-corps** de K si c'est un corps pour les lois induites.
Si L est un sous-corps de K, on dit que K est un **sur-corps** ou une **extension** de L.
Avec L sous-corps de K, et $A \subset K$, on dit que A **engendre** K sur L si K est le plus petit sous-corps de K contenant A et L. On note alors $K = L(A)$. Si A est fini on note $K = L(a_1, ..., a_n)$.
L'extension est dite **monogène** si A contient un seul élément.

Avant de construire un corps "autour" d'un corps (i.e. une extension de corps) on va déjà étendre un anneau intègre en un corps :

Théorème 0.1

Etant donné un anneau intègre A, il existe un unique corps K (à isomorphisme près) contenant un anneau intègre B isomorphe à A et tel que tout sous-corps de K contenant B soit K lui-même.
On l'appelle **corps des fractions** de A.

Démonstration *On procède selon les étapes suivantes pour montrer l'existence :*
•*On considère les classes d'équivalences sur $A \times A$ pour la relation $\mathcal{R}$ définie par $(x,y)\mathcal{R}(x',y') \iff xy' = x'y$ (intuitivement les classes d'équivalence sont les fractions). Appelons K l'ensemble quotient ainsi obtenu.*
•*On considère ensuite l'addition sur ces classes, facile à retrouver au vu de la considération sur les fractions ; il s'agit de $(x,y)+(x',y') = (xy'+x'y, yy')$. De même la multiplication est définie par $(a,b).(a',b') = (aa', bb')$. Il est facile de voir que ces lois vérifient toutes les propriétés souhaitées, et qu'elles sont bien définies dans la structure quotient. On trouve un élément $(0,1)$ neutre pour l'addition, et un élément $(1,1)$ neutre pour la multiplication.*
•*L'application qui à x associe $(x,1)$ est un morphisme injectif de A dans K. C'est donc un isomorphisme de A sur son image A'.*
•*Etant donné un sous-corps de K contenant A', il contient nécessairement les quotients d'éléments de A', et donc K tout entier.*
•*Il ne reste plus qu'à vérifier l'unicité de K, à isomorphisme près. Cette tâche est laissée au lecteur.*
Apllication On a les cas suivants de corps de fractions :

— Construction de $\mathbb{Q}$ à partir de $\mathbb{Z}$.

— Construction du corps des fractions rationnelles, à partir de l'anneau des polynômes.

PROPOSITION 0.2
Algèbre linéaire et corps :
•Si L est un sous-corps de K, alors K est un L-espace vectoriel.
•Si la dimension de K en tant que L-espace vectoriel est finie alors on l'appelle **degré** de K pour L et on le note $[K:L]$.
•Si K et L sont finis, alors $|K| = |L|^{[K:L]}$.

Démonstration *Le premier point est clair.*
Le second point est une définition.
Le troisième point est clair.

THÉORÈME 0.3 **Théorème des bases téléscopiques**

Si $M \subset L \subset K$ (tous trois des corps) alors si e_i est une base de K en tant que L-espace vectoriel et si f_j est une base de L en tant que M-espace vectoriel alors $e_i.f_j$ est une base de K en tant que M-espace vectoriel Donc $[K:M] = [K:L].[L:M]$.

Démonstration *Facile.*

DÉFINITION 0.3 **Différentes extensions de corps**

Si L est une extension du corps K, alors un élément a de L est dit **algébrique sur** K s'il existe un polynôme P à coefficients dans K tel que $P(a) = 0$. Un nombre réel est souvent dit simplement **algébrique** s'il est algébrique sur $\mathbb{Q}$. L'ensemble des éléments de L algébriques sur K est appelée extension algébrique de K dans L.

Etant donné K un corps et $P \in K[X]$, on appelle **corps de rupture de** P un sur-corps L de K dans lequel P admet une racine a et tel que $L = K(a)$.

Etant donné K un corps et $P \in K[X]$, on appelle **corps de décomposition de** P un surcorps L de K dans lequel P est scindé et $L = K(Z)$, avec Z l'ensemble des zéros de P dans L.

Etant donné K un corps, on appelle **clôture algébrique** de K une extension de K algébriquement close et dont tous les éléments sont algébriques sur K.

On a existence du corps de décomposition, et existence du corps de rupture lorsque le polynôme est irréductible (s'il n'est pas irréductible, le corps lui-même contient une racine, et il n'est pas besoin de l'étendre !). Dans les deux cas, on a unicité à isomorphisme près. Le théorème de Steinitz (difficile) montre que tout corps admet une clôture algébrique, unique à isomorphisme près.

Démonstration *(de l'existence du corps de rupture) Le corps $K(X)/(P)$ convient (i.e. le quotient de K par l'idéal engendré par P).*

1.3 Corps finis

Cette section, très brève, peut être prolongée par la lecture de [1].

PROPOSITION 0.4

Un anneau intègre fini est un corps.

Démonstration *Si un anneau est intègre, l'application $x \mapsto yx$ est bijective pour tout y. En particulier, il existe x tel que $yx = 1$.*

THÉORÈME 0.5

Un corps fini n'est jamais algébriquement clos.

Démonstration *Il suffit de considérer le polynôme* $\prod_{k \in K} (X - k) + 1$.

THÉORÈME 0.6 **Wedderburn**

Tout corps fini est commutatif.

THÉORÈME 0.7 **Corps de Galois**

Quel que soit p premier, quel que soit n dans $\mathbb{N}$ non nul, il existe un unique corps, à isomorphisme près, de cardinal p^n. Tout corps fini est de cette forme.

Les corps finis sont appelés aussi **corps de Galois** (d'ordre q quand le cardinal du corps est q). p est égal à la caractéristique du corps.

Démonstration *Ces résultats, non triviaux, ne seront pas prouvés ici. On pourra consulter [1] pour une preuve compréhensible.*
Enfin deux résultats (non triviaux) donnés sans preuve :

PROPOSITION 0.8

Le groupe des automorphismes d'un corps fini de cardinal p^n est cyclique, d'ordre n, engendré par $x \mapsto x^n$.

PROPOSITION 0.9

Le groupe multiplicatif d'un corps fini est cyclique.

Notons aussi l'existence de résultats sur les extensions de corps finis : toute extension fini d'un corps fini est engendrée par un seul élément.

Références

[1] D. Perrin, *Cours d'algèbre*, Ellipses 1996.