CARACTÉRISTIQUE D'UN ANNEAU

L'objet de cette annexe est de présenter la notion de caractéristique dans le cas d'un anneau puis d'un corps.

A. Caractéristique d'un anneau

Soit $(A, +, \times)$ un anneau. Si $a \in A$ et $n \in \mathbb{N}$, rappelons que la notation na signifie $a + \cdots + a$ où a est répété n fois (avec $0.a = 0_A$). Par ailleurs, si $n \in \mathbb{Z}_-^*$, la notation na désigne $(-n)(-a)$.

Prenons 1_A et additionnons le successivement avec lui-même. On obtient $1_A + 1_A = 2.1_A$, puis $1_A + 1_A + 1_A = 3.1_A$, puis 4.1_A, etc. Il se présente alors une alternative : ou bien on finit par tomber sur 0_A (le compteur est remis à 0_A périodiquement) ou bien au contraire on n'obtient jamais 0_A (le compteur ne revient jamais à 0_A). On comprend aisément que, selon qu'on est dans le premier cas ou dans le second, les calculs dans l'anneau vont être très différents.

Ce constat nous conduit à introduire, ci-dessous, une grandeur, caractéristique de l'anneau, qui permet de savoir s'il existe des sommes de l'unité 1_A qui sont nulles et, dans le cas où elles existent, de connaître le nombre minimal de 1_A qu'il faut ajouter pour obtenir 0_A.

Définition 1

L'application $\varphi : \mathbb{Z} \longrightarrow A$ définie par $\forall k \in \mathbb{Z},\ \varphi(k) = k.1_A = 1_A + \cdots + 1_A$ (k fois) est un morphisme d'anneaux. Son noyau est donc un idéal de $\mathbb{Z}$, ce qui justifie l'existence d'un unique entier naturel n tel que $\operatorname{Ker}\varphi = n\mathbb{Z}$. Cet entier n est appelé la caractéristique de A.

Autrement dit, s'il existe au moins un entier $k \in \mathbb{N}^*$ tel que $k.1_A = 0_A$, la caractéristique de A est, par définition, le plus petit entier naturel non nul n tel que $n.1_A = 0_A$ et si un tel entier n'existe pas alors la caractéristique est nulle.

■ On a $\varphi(1) = 1_A$ et, pour tous $k, \ell \in \mathbb{Z}$, $\varphi(k + \ell) = (k + \ell).1_A = k.1_A + \ell.1_A = \varphi(k) + \varphi(\ell)$ et $\varphi(k\ell) = (k\ell).1_A = (k.1_A)(\ell.1_A) = \varphi(k)\varphi(\ell)$, ce qui démontre que φ est un morphisme d'anneaux.
Il n'est d'ailleurs pas difficile de voir que φ est le seul morphisme d'anneaux de $\mathbb{Z}$ dans A. ■

On peut ainsi retenir que, dans un anneau A de caractéristique non nulle, la caractéristique est le nombre minimal de 1_A qu'il faut ajouter pour obtenir 0_A.

On peut remarquer que l'anneau est de caractéristique nulle lorsque le morphisme φ est injectif et de caractéristique non nulle lorsque φ n'est pas injectif.

Exemples :

- Le seul anneau de caractéristique 1 est l'anneau nul (pour les autres anneaux, 1.1_A ne vaut pas 0_A).
- Les anneaux $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont de caractéristique nulle.
- L'anneau $\mathbb{Z}/n\mathbb{Z}$ est de caractéristique n.
- Deux anneaux isomorphes ont la même caractéristique.

La proposition suivante rassemble les propriétés de la caractéristique d'un anneau.

Proposition 1

Notons $n \in \mathbb{N}$ la caractéristique de A. Alors

(i) $\forall a \in A,\ na = 0_A$;

(ii) pour tout $m \in \mathbb{Z}$, on a $(m.1_A = 0_A) \iff (n \text{ divise } m)$;

(iii) si B est un sous-anneau de A, alors B est de même caractéristique que A ;

(iv) si A est intègre, alors ou bien $n = 0$ ou bien n est un nombre premier.

■ On reprend le morphisme d'anneaux $\varphi : \mathbb{Z} \longrightarrow A$ défini par $\forall k \in \mathbb{Z},\ \varphi(k) = k.1_A$. Son noyau est $n\mathbb{Z}$.

(i) Pour tout $a \in A$, on a $na = n(1_A.a) = (n.1_A)a = 0_A.a = 0_A$.

(ii) Soit $m \in \mathbb{Z}$. On a $(m.1_A = 0_A) \iff (m \in \operatorname{Ker}\varphi) \iff (m \in n\mathbb{Z}) \iff (n \text{ divise } m)$.

(iii) Cela découle du fait que $1_B = 1_A$ et $0_B = 0_A$.

(iv) Supposons que A est intégre et que $n \neq 0$ et démontrons que cela impose à n d'être premier. Pour cela, raisonnons par l'absurde en supposant que n n'est pas premier, c'est-à-dire qu'il existe $c, d \in [\![2; n-1]\!]$ tels que $n = cd$. Alors $0_A = n.1_A = (cd)1_A = (c.1_A)(d.1_A)$, ce qui donne $c.1_A = 0_A$ ou $d.1_A = 0_A$ par intégrité. Les deux égalités contredisent la minimalité de n. Absurde ! ■

L'énoncé suivant précise la structure « profonde » d'un anneau selon que sa caractéristique est nulle ou qu'elle ne l'est pas.

Proposition 2

Le plus petit sous-anneau d'un anneau de caractéristique nulle est isomorphe à $\mathbb{Z}$.

Le plus petit sous-anneau d'un anneau de caractéristique n non nulle est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

■ Remarquons que le plus petit sous-anneau de A est $\operatorname{Im}(\varphi)$ où φ est le morphisme d'anneaux introduit à la définition 1. En effet, $\operatorname{Im}(\varphi)$ est bien un sous-anneau de A en tant qu'image de l'anneau $\mathbb{Z}$ par le morphisme d'anneaux φ et c'est bien le plus petit sous-anneau de A puisqu'il ne contient que 1_A et ses itérés (c'est le minimum que doit contenir un sous-anneau).

Dans le cas où la caractéristique est nulle, φ est injectif. Il induit donc un isomorphisme d'anneaux de $\mathbb{Z}$ sur $\operatorname{Im}(\varphi)$. Dans ce cas, le plus petit anneau de A est bien isomorphe à $\mathbb{Z}$.

Dans le cas où la caractéristique n est non nulle, on peut démontrer (et nous l'admettrons) que $\operatorname{Im}(\varphi)$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$. Dans ce cas, le plus petit anneau de A est bien isomorphe à $\mathbb{Z}/n\mathbb{Z}$. ■

Bref, un anneau contient ou bien une copie de $\mathbb{Z}$ ou bien une copie de $\mathbb{Z}/n\mathbb{Z}$.

Un anneau de caractéristique nulle est donc nécessairement infini (il contient une copie de $\mathbb{Z}$). En revanche, un anneau de caractéristique non nulle n peut être fini (c'est le cas de $\mathbb{Z}/n\mathbb{Z}$) mais aussi infini (c'est le cas de l'anneau des polynômes à coefficients dans $\mathbb{Z}/n\mathbb{Z}$).

Exercice 1.

On suppose que A est commutatif et que la caractéristique de A est un nombre premier p. Démontrer que l'application $F : A \longrightarrow A$ telle que $\forall a \in A,\ F(a) = a^p$ est un endomorphisme de l'anneau A, appelé endomorphisme de Frobenius.

◊ On a $F(1_A) = 1_A$.

Pour tous $a, b \in A$, on a $F(ab) = (ab)^p = a^p b^p = F(a)F(b)$ puisque A est commutatif.

Il reste à démontrer que, pour tous $a, b \in A$, on a $F(a+b) = F(a) + F(b)$, c'est-à-dire que l'on a la formule rigolote $(a+b)^p = a^p + b^p$. Soient $a, b \in A$. D'après la formule du binôme (qu'il est licite d'utiliser puisque A est commutatif), on a $(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}$. Or, dans le cours d'arithmétique, nous avons démontré que, lorsque p est premier, p divise $\binom{p}{k}$ pour $k \in [\![1; p-1]\!]$. Donc, pour tout $k \in [\![1; p-1]\!]$, on a $\binom{p}{k} a^k b^{p-k} = 0_A$ (puisque A est de caractéristique p), ce qui donne $(a+b)^p = a^p + b^p$. ◊

B. Caractéristique d'un corps

Un corps étant un anneau intègre, la propriété (iv) de la proposition 1 implique le résultat suivant.

Proposition 3

La caractéristique d'un corps est ou bien nulle ou bien un nombre premier.

■ AQT ■

Exemples :

- Les corps $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont de caractéristique nulle.
- Le corps $\mathbb{F}_p$ est de caractéristique p.

La proposition 2 permet de décrire le plus petit sous-corps d'un corps donné.

Proposition 4

Le plus petit sous-corps d'un corps de caractéristique nulle est isomorphe à $\mathbb{Q}$.

Le plus petit sous-corps d'un corps de caractéristique p, où p est un nombre premier, est isomorphe à $\mathbb{F}_p$.

■ Soient K un corps de caractéristique nulle et L un sous-corps de K. Alors L est aussi de caractéristique nulle. La proposition 2 dit donc que le plus petit sous-anneau de L, noté B, est isomorphe à $\mathbb{Z}$. Dès lors, comme L est un corps, il contient le corps des fractions de l'anneau intègre B, qui est isomorphe à $\mathbb{Q}$. Donc L contient un corps isomorphe $\mathbb{Q}$. Par conséquent, le plus petit sous-corps de K est isomorphe à $\mathbb{Q}$.

Soient K un corps de caractéristique p (où p est un nombre premier). La proposition 2 dit que le plus petit sous-anneau de K, noté A, est isomorphe à $\mathbb{F}_p$. Comme $\mathbb{F}_p$ est un corps, c'est aussi le cas de A. Par conséquent, A est le plus petit sous-corps de K et il est isomorphe à $\mathbb{F}_p$. ■

Bref, un corps contient ou bien une copie de $\mathbb{Q}$ ou bien une copie de $\mathbb{F}_p$.

On termine ce paragraphe par un énoncé concernant les corps finis.

Proposition 5

Tout corps fini a pour caractéristique un nombre premier, et pour cardinal une puissance de ce nombre.

Pour tout nombre premier p et tout entier $n \in \mathbb{N}^*$, il existe un corps fini de cardinal p^n, qui est unique (à isomorphisme de corps près). Il est noté $\mathbb{F}_{p^n}$.

■ Admis. ■

Précisons qu'un corps de caractéristique p (où p est un nombre premier) n'est pas toujours fini.

On a $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ mais, attention, n'allez pas croire que, pour $n \geqslant 2$, $\mathbb{F}_{p^n}$ est égal à $\mathbb{Z}/p^n\mathbb{Z}$. D'ailleurs, l'anneau $\mathbb{Z}/p^n\mathbb{Z}$ n'est pas un corps !!

Exercice 2.

Que dire de l'endomorphisme de Frobenius d'un corps fini ? Que dire de celui de $\mathbb{F}_p$?

◊ Un morphisme de corps est toujours injectif (nous l'avons vu dans le cous sur les structures algébriques). L'endomorphisme de Frobenius d'un corps fini est donc une application injective entre deux ensembles finis de même cardinal. À ce titre, c'est une bijection. Pour un corps fini, l'endomorphisme de Frobenius est donc un automorphisme.

Si le corps est $\mathbb{F}_p$, l'automorphisme de Frobenius est l'identité par le petit théorème de Fermat. ◊