Racines de l'unité

1 Racines de l'unité

Soit K un corps et n un entier naturel non nul.

Définition Un élément $a \in K$ est une **racine n$^{\text{ème}}$ de l'unité** si, et seulement si, $a^n = 1$ .Soit $S_n(K)$ l'ensemble de toutes les racines $n^{ème}$ de l'unité dans K. Cet ensemble est non vide car $1 \in S_n(K)$.

Il résulte de cette définition que $a \in K$ est une racine $n^{ème}$ de l'unité si, et seulement si, a est une racine du polynôme $U(X) = X^n - 1 \in K[X]$.

Exemple $1 \in K$ est une racine $n^{ème}$ de l'unité pour tout $n \in \mathbb{N}^*$. i est une racine $4^{ème}$ de l'unité dans $\mathbb{C}$. $j = \dfrac{1}{2} + i\dfrac{\sqrt{3}}{2}$ est une racine cubique de l'unité dans $\mathbb{C}$.

Théorème Si m divise n, alors $S_m(K) \subseteq S_n(K)$.

Démonstration Si m divise n, alors n s'écrit $n = pm$ où $p \in \mathbb{N}^*$. Il en résulte

$$[a \in S_m(K)] \Longrightarrow [a^m = 1] \Longrightarrow [a^n = a^{mp} = (a^m)^p = 1] \Longrightarrow [a \in S_n(K)]$$

Théorème L'ensemble des racines n$^{\text{ème}}$ de l'unité $S_n(K)$ est un groupe multiplicatif.

Démonstration $S_n(K) \neq \emptyset$ comme nous l'avons vu. D'un autre côté, si a et b sont des racines $n^{ème}$ de l'unité, alors a et b sont non nuls et vérifient

$$\left(ab^{-1}\right)^n = a^n\left(b^{-1}\right)^n = a^n(b^n)^{-1} = 1$$

ce qui prouve le théorème.

Définition On appelle **corps premier** d'un corps K le plus petit sous-corps de K.

Théorème Le corps premier de K est le sous-corps de K engendré par 1.

Démonstration En effet, 1 appartient à tous les sous-corps de K . Il en résulte que le sous-corps de K engendré par 1 est le plus petit sous-corps de K c.d. son corps premier.

Théorème Le corps premier de K est l'intersection de tous les sous-corps de K.

Démonstration Facile à vérifier.

Théorème Le corps premier d'un corps K est isomorphe à $\mathbb{Q}$ si sa caractéristique est nulle, et à $\mathbb{Z}/(p)$ (où (p) est l'idéal engendré par p dans l'anneau $\mathbb{Z}$) si cette caractéristique est $p \neq 0$.

Démonstration Soit u l'application de $\mathbb{Z}$ dans K définie par $u(n) = n.1$. Il est facile de vérifier que u est un homomorphisme d'anneaux et que $\mathrm{Im}(u)$ est le sous-anneau de K engendré par 1. $Ker(u)$ est un idéal de $\mathbb{Z}$. Il est engendré par un élément p de $\mathbb{Z}$. p est la caractéristique de K. Si $p = 0$, alors $\mathbb{Z}$ est isomorphe à $\mathrm{Im}(u)$ et le corps des fractions de $\mathbb{Z}$ (c.à.d. $\mathbb{Q}$) au corps des fractions de $\mathrm{Im}(u)$. Mais ce corps est le plus petit sous corps de K contenant 1. Il est le corps premier de K. Donc, si K est de caratéristique nulle, son corps premier est isomorphe à $\mathbb{Q}$. Si $p \neq 0$, alors $\mathrm{Im}(u)$ est isomorphe à $\mathbb{Z}/Ker(u) = \mathbb{Z}/(p)$ qui est un corps (p est premier). Ce sous-corps de K est le sous-corps engendré par 1. Donc, si K est de caractéristique $p \neq 0$, son corps premier est isomorphe à $\mathbb{Z}/(p)$.

Exemple $\mathbb{Q}$ est le corps premier de $\mathbb{R}$ et de $\mathbb{C}$. $\mathbb{Z}/(p)$ est égal à son corps premier.

Théorème Soit P le corps premier du corps K. Nous avons $U(X) = X^n - 1 \in P[X]$. Soit R le corps des racines de U sur P. Si la caractéristique p de K est nulle ou si elle ne divise pas n, alors R contient n racines $n^{ème}$ de l'unité distinctes.

Démonstration Il suffit de prouver que les racines du polynôme U sont toutes simples. Sinon, U et son polynôme dérivé $U' = nX^{n-1}$ ont une racine commune. Or zéro est la seule racine de U' car $p = 0$ ou n est non divisible par p. Comme 0 n'est pas une racine de U, toutes les racines de U sont simples et R en contient n.

Pour démontrer que $S_n(K)$ est un groupe cyclique, nous avons besoin d'un théorème de la théorie de groupes.

Lemme Soient a et b deux éléments d'un groupe abélien multiplicatif G. Si $p = Ord(a)$ et $q = Ord(b)$ sont premiers entre eux, alors $Ord(ab) = pq$.

Démonstration Tout d'abord, $gr(a)$ désignant le sous groupe de Gengendré par a, $gr(a) \cap gr(b)$ est réduit à $\{e\}$ car si x est un élément de cette intersection, alors l'ordre r de x est un diviseur commun de p et q. Cet ordre est donc égal à 1 (p et q sont premiers entre eux) et $x = e$. D'un autre côté, $(ab)^{pq} = a^p b^q = ee = e$. Enfin, si d est l'ordre de ab, alors $(ab)^d = a^d b^d$. Il en résulte $a^d = \left(b^{-1}\right)^d \in gr(a) \cap gr(b) = \{e\}$ et par suite $a^d = e = b^d$. On en déduit que d est donc un multiple commun de p et q, donc de leur produit car ils sont premier entre eux. Ainsi pq est l'ordre de ab.

Lemme Soient a_1,...,a_n des élément d'un groupe abélien multiplicatif G. Si les ordres des a_1,...,a_n sont premiers deux à deux, l'ordre de leur produit est égal au produit des ordres de ces éléments.

Démonstration Par récurrence.

Théorème Si la caractéristique p de K est nulle ou si elle ne divise pas n, alors le groupe des racines n^{imes} de l'unité $S_n(K)$ est un groupe cyclique.

Démonstration Soit $n = p_1^{n_1}...p_t^{n_t}$ la décomposition de n comme produit de nombres premiers. Pour tout $i = 1,2,...,t$ il existe au plus $\frac{n}{p_i}$ éléments a qui vérifient $a^{\frac{n}{p_i}} = 1$, car le polynôme $X^{\frac{n}{p_i}} - 1$ possède au plus $\frac{n}{p_i}$ racines. Soit, pour $i = 1,2,...,t$, $a_i \in S_n(K)$ tel que $a_i^{\frac{n}{p_i}} \neq 1$. Considérons $m_i = \frac{n}{p_i^{n_i}}$ et $b_i = a_i^{m_i}$. Les éléments b_i sont d'ordre $p_i^{n_i}$ car $b_i^{p_i^{n_i}} = 1$ et $b_i^{p_i^{n_i-1}}$ sont différents de 1. Le produit $b = b_1...b_t$ est un produit d'éléments dont les ordres sont premiers entre eux, il en résulte que l'ordre de b est le produits des ordres des b_i. Ainsi b est d'ordre n. Il engendre $S_n(K)$.

Corollaire Le groupe des racines n^{imes} de l'unité $S_n(K)$ est isomorphe à $\mathbb{Z}/(n)$ où (n) désigne l'idéal engendré par n dans $\mathbb{Z}$.

Définition On dit qu'une racine $n^{ème}$ de l'unité est une **racine $n^{ème}$ primitive de l'unité** si, et seulement si, cette racine engendre le groupe $S_n(K)$.

Si $z \in S_n(K)$ est une racine $n^{ème}$ primitive de l'unité, alors

$$S_n(K) = \{1,z,z^2,...,z^{n-1}\}$$

Le nombre de ces racines primitives est celui des générateurs du groupe cyclique $S_n(K)$. Nous savons, d'après la théorie des groupes, que ces générateurs sont les z^q où $q \in \{1,2,...,n-1\}$ et q est premier avec n. Leur nombre est noté $\varphi(n)$ φ est en fait la **fonction caractéristique d'Euler**.

Exemple Les racine 12ème primitives de l'unité dans $\mathbb{C}$ sont ω,ω^5,ω^7 et ω^{11} où $\omega = \exp\left(\frac{i\pi}{6}\right)$.

2 Corps finis

Les exemples les plus simples de corps finis sont les corps $\mathbb{Z}/(p)$ où p est un nombre premier et où $(p) = \mathbb{Z}/p\mathbb{Z}$.

Théorème Soit K un corps fini. La caractéristique de K est non nulle.

Démonstration Car sinon, le corps premier de K serait isomorphe à $\mathbb{Q}$.

Théorème Soit K un corps fini. Si $Card\,(K) = q$, alors K est le corps des racines du polynôme $X^q - X$ le corps premier P de K.

Démonstration Soit a un élément de K. Si $a = 0$, alors $a^q - a = 0$. Si $a \neq 0$, alors a appartient au groupe multiplicatif de K qui est un groupe fini d'ordre $q-1$. Il en résulte $a^{q-1} = 1$ et $a^q - a = 0$. Ce qui précède prouve que K est un corps de décomposition pour $X^q - X$ sur P. Il est un corps des racines pour $X^q - X$ sur P car tout corps de décomposition pour pour ce polynôme sur P doit contenir tous les éléments de K.

Théorème Soit K un corps fini. Si $Card\,(K) = q$, alors q est une puissance de la caratéristique p de K.

Démonstration K est un P-espace vectoriel. Si $[K:P] = n$, alors $q = Card(K) = (Card(P))^n = p^n$.

Corollaire Deux corps finis de même cardinal ont la même caractéristique.

Démonstration Soient $Card(K) = q$,q' les cardinaux et p,p' les caractéristiques des deux corps. Nous avons

$$p^n = q = q' = \left(p'\right)^m$$

ce qui implique $p = p'$ car ces deux entiers sont des nombres premiers.

Théorème Deux corps finis de même cardinal sont isomorphes.

Démonstration Soit K et K' de même cardinal q. Soient P le corps premier de K et P' celui de K'. P et P' sont isomorphes car ils sont isomorphes chacun à $\mathbb{Z}/(p)$. Soit σ un isomorphisme entre K et K'. Le corps K est le corps des racines pour $X^q - X$ sur P. Il est isomorphe à K', corps des racines pour $X^q - X = \widehat{\sigma}\,(X^q - X)$ sur P'.

Théorème Pour tout nombre premier p et tout entier $n \geq 1$, il existe un corps fini, unique à un isomorphisme près, de cardinal $q = p^n$.

Démonstration Il suffit de prendre le corps des racines pour $X^q - X$ sur $P = \mathbb{Z}/(p)$.

Théorème Le groupe multiplicatif K^* d'un corps fini K est cyclique.

Démonstration Nous avons $K^* = S_n(K)$ où $n = Card(K) - 1$.