Corps Cyclotomique

I) Racine n-ième de l'unité, Racine primitive n-ième de l'unité.

Définition 1

Soit P le polynôme K[X] s'écrivant sous la forme **$P(X) = X^n - 1$** avec **$n \in N^*$** , K un corps commutatif. Les racines de P sont appelées **racines n-ième** de l'unité. L'ensemble de ces racines est noté **$G_n = \{X \in K / X^n = 1\}$.**

Pour **K** = **C,** on a **$G_n = \{e^{(\frac{2\pi ik}{n})}$ avec $k \in \{0,..., n-1\}\}$** et est un sous-groupe cyclique de **C^*** isomorphe à **Z/nZ** et de cardinal n.

$P(X) = X^n - 1 = (X-1)(X^{n-1} + X^{n-2} + \dots + X + 1)$ Il ne s'agit donc pas d'un polynôme irréductible.

Exemple 1

Pour n=4, les racines 4èmes de l'unité sont : 1, -1, i, -i.

Pour n=3, les racines 3èmes de l'unité sont 1, exp(2πi/3), et exp(4πi/3).

Définition 2

Une racine n-ième de l'unité est dite **primitive** quand elle est d'ordre exactement n, c'est-à-dire quand c'est un générateur de **G_n**. On note **P_n** l'ensemble des racines primitives nième de l'unité.

Exemple 2

Pour n=4, les racines quatrième primitives de l'unité sont : $\{i, -i\}$

la première racine n-ième de l'unité noté $\alpha = e^{2\pi i/n}$ est toujours primitive card(α)=n

Proposition

Il y'a φ(n) racine primitives n-ème de l'unité,

$ord(\alpha^k) = n \iff pgcd(k, n) = 1$

Démonstration

Soit α^k une racine n-ième de l'unité.

-Si pgcd (k ,n)=1 alors $(\alpha^k)^n = (\alpha^n)^k = 1^K = 1$.

$\alpha^{kr} = (\alpha^k)^r = 1 \Rightarrow n/kr \Rightarrow n \leq r \Rightarrow ord(\alpha^k) = n$

-Si pgcd(k ,n) > 1

$(\alpha^k)^{(n/pgcd(n,k))} = (\alpha^n)^{(k/pgcd(n,k))} = 1^{(k/pgcd(n,k))} \Rightarrow ord(\alpha^k) < n$

L'ensemble des racines primitives nièmes de l'unités est $\mathbf{P_n}=\{\alpha^K / 0 \leq k \leq n-1$, pgcd(k ,n) = 1$\}=$ **φ(n)**

II) Corps cyclotomique, polynôme cyclotomique

Définition

Posons **K = Q(P_n)** le corps de racine primitive n-ième de l'unité**.** Ce corps est appelé le **n-ième corps cyclotomique** ou **le corps cyclotomique des racines n-ième de l'unité**.

Soit **K** un corps cyclotomique et n un entier qui n'est pas divisible par card **(K).** On appelle n-ième polynôme cyclotomique de **K** le polynôme

$\mathbf{\Phi_{n,k}(x)} = \prod_{\alpha \in P_n(x)} (X - \alpha)$

Quand **K** = **Q**, on note plus simplement $\mathbf{\Phi_{n,K} = \Phi_n}$.

a) Propriétés des polynômes cyclotomiques en caractéristique 0.

Propriétés :

1. $\Phi_n(x) \in Z[X]$
2. $\Phi_n(x)$ est irréductible dans Q [X] (donc dans Z[X])
3. Deg ($\Phi_n(x)$) = φ(n) = (| Z/nZ^* | par définition) avec φ l'indicateur d'Euler.
4. Dans C[x], on a $\mathbf{\Phi_n(x)} = \prod_{k \in (Z/nZ)^*} (X - \alpha_n^k)$ où $\alpha_n = e^{2\Pi i/n}$.

b) Propriétés des polynômes cyclotomiques en caractéristique p

Propriété :

1. Si $n = p^r - 1$, alors $\Phi_n(x)$ est un produit de polynômes irréductibles de degré r.

2. Si n et p sont premiers entre eux et r est l'ordre de p dans $(Z/nZ)^*$ alors $\Phi_n(x)$ est un produit de polynômes irréductibles de degré r.
3. Si n et p sont premiers entre eux, alors $\boldsymbol{\Phi_{pin}(X) = \Phi_n(X)^{\varphi(pi)}}$

EXEMPLE

$\Phi_n(x)=\prod(x-\boldsymbol{\alpha})$

Par la propriété précédente son degré est $\varphi(n)$

Pour n=1 , $\Phi_1(x)=x-1$

Pour n=2 , $\Phi_2(x)=x+1$

Pour n=3, $\Phi_3(x)=(x-j)(x-j^2)$

$=x^2- x(j+j^2)+j\ .j^2$

$=x^2+x+1$ car $j^2+j\approx -1$ et $j.j^2\approx 1$ avec j^2 le conjugué de j.

Exercice :

Déterminer pour n=3 le polynôme cyclotomique.

Solution :

On a, $x^3-1= (x-1)(x-j)(x-j^2) = \Phi_1(x).\Phi_3(x)$

$$=(x-1).\Phi_3(x) \Rightarrow \Phi_3(x)=\frac{x3-1}{(x-1)}$$

$$= x^2+x+1$$

De façon général, on a pour les nombres premiers

$X^p-1 = \Phi_1(x).\Phi_p(x) \Rightarrow \Phi p\ (x) =(X^p-1)/(x-1)$

$$\boldsymbol{\Phi p\ (x) = x^{p-1}+x^{p-2}+\ldots+1}$$

Quelques exemples de polynômes cyclotomiques :

- $\boldsymbol{\Phi_1(x)}=x-1$
- $\boldsymbol{\Phi_2(x)=x+1}$
- $\boldsymbol{\Phi_3(x) = x^2+x+1}$
- $\boldsymbol{\Phi_4(x)=x^2+1}$
- $\boldsymbol{\Phi_5(x) =x^4+x^3+ x^2+x+1}$
- $\boldsymbol{\Phi_6(x) = x^2-x+1}$

- $\Phi_7(x) = x^6+x^5+x^4+x^3+x^2+x+1$
- $\Phi_8(x) = x^4+1$
- $\Phi_9(x) = x^6+x^3+1$
- $\Phi_{10}(x) = x^4-x^3+x^2-x+1$

III) Extension cyclotomique

Définition

Une extension cyclotomique est une extension de la forme $\mathbf{K(\alpha_n)/K}$ où K est un corps de caractéristique premier à n et α_n une racine primitive nième de l'unité (dans un corps de décomposition de $X^n - 1$) sur K.

Si $\mathbf{K = Q}$ alors $\mathbf{K(\alpha_n) = Q(\alpha_n).}$ Elle sera noté $\mathbf{Q^{(n)}}$ et s'appelle nième corps cyclotomique. Autrement on appelle corps cyclotomique $\mathbf{K_n,}$ le corps de décomposition du polynôme cyclotomique $\mathbf{\Phi_n}$.

Propriété

Notons n l'ordre de α, c'est-à-dire que α est une racine primitive nième de l'unité, ou encore une racine du polynôme cyclotomique Φ_n.
1. L'extension $\mathbf{Q(\alpha)/Q}$ est de degré $\mathbf{\varphi(n),}$ où φ désigne la fonction indicatrice d'Euler.
2. L'extension cyclotomique est aussi le corps de décomposition du polynôme $\mathbf{\Phi_n}$. Elle est donc **galoisienne.**

Démonstration

L'extension contient α et toutes ses puissances, or les puissances de α forment l'ensemble des racines n-ièmes de l'unité et donc en particulier les racines primitives n-ièmes de l'unité qui sont les racines du polynôme cyclotomique. Ceci démontre que $\mathbf{Q(\alpha)}$ est le corps de décomposition de $\mathbf{\Phi_n}$.

Dans un corps parfait comme celui des rationnels (un corps parfait est un corps où tous les polynômes irréductibles sont séparables c'est-à-dire n'ont pas de racines multiples dans la clôture algébrique), un corps de décomposition est toujours une extension Galoisienne.

Proposition

Soient m et n deux entiers naturels non nuls. Si m et n sont premiers entre eux alors $\mathbf{Q(\alpha_n\alpha_m) = Q(\alpha_n, \alpha_m).}$

Démonstration :

En effet on a $\mathbf{Q(\alpha_n\alpha_m) \subset Q(\alpha_n, \alpha_m)}$. D'autre part si m et n sont premiers entre eux alors il existe **u** et **v** deux entiers tels que **u.n + v.m = 1**.

Donc $\mathbf{\alpha_m = (\alpha_m\alpha_n).nu}$ et $\mathbf{\alpha_n= (\alpha_n\alpha_m).vm}$.

Et par suite $\mathbf{Q(\alpha_n\alpha_m) = Q(\alpha_n, \alpha_m).}$

Corollaire:
Soient **m** et **n** deux entiers naturels non nuls premiers entre eux alors $\mathbf{Q(\alpha_n) \cap Q(\alpha_m) = Q}$

Démonstration :
En effet on sait que si **m** et **n** sont premiers entre eux alors $\mathbf{u_{mn} \simeq u_{m\,x}\,u_n}$ et par suite $\mathbf{Gal(Q(\alpha_{nm})/ Q) \simeq U_{mn} \simeq U_mxU_n \simeq Gal(Q(\alpha_m)/ Q)xGal(Q(\alpha_n)/ Q}$) qui permet de conclure que $\mathbf{Q(\alpha_n) \cap Q(\alpha_m) = Q}$.

IV) Groupe de Galois d'une extension cyclotomique

Théorème
1. Soit une extension cyclotomique $\mathbf{K(\alpha_n)/K}$ où **K** est un corps de caractéristique première à **n** et $\mathbf{\alpha_n}$ une racine primitive n-ième de 1.
Alors $\mathbf{K(\alpha_n)/K}$ est galoisienne de groupe de Galois isomorphe à un sous-groupe de $\mathbf{(Z/n\,Z)^*}$
2. Soit $\mathbf{\alpha_n \in C(x)}$, **n** éléments d'ordre n. L'extension **Q (n)/ Q** est galoisienne de groupe de Galois isomorphe à $\mathbf{(Z/n\,Z)^*}$.

Corollaire

Une extension cyclotomique est toujours abélienne.

Démonstration :

Soit **d**'un entier plus petit que **n** et premier à **n**. Alors $\mathbf{\alpha^d}$ est une racine du polynôme cyclotomique donc il existe un Q-automorphisme $\mathbf{m_d}$ (évidemment unique) du corps de décomposition $\mathbf{Q(\alpha)}$ qui envoie $\mathbf{\alpha}$ sur $\mathbf{\alpha^d}$.
Considérons alors l'application du groupe multiplicatif des éléments

inversibles de **Z/nZ** dans le groupe de Galois qui, à la classe de **d** associe l'automorphisme $\mathbf{m_d}$. Cette application est clairement un isomorphisme de groupes. Cet isomorphisme montre que le groupe de Galois est abélien.