2. Anneaux de polynômes : complément

2.1 Rappels

1. $k[x]$ ou k est un corps ($k = \mathbb{R}, \mathbb{C}, \mathbb{F}_p, \mathbb{F}_q$) est l'anneau de polynômes à coefficients dans k.

2.1 Rappels

1. $k[x]$ ou k est un corps ($k = \mathbb{R}, \mathbb{C}, \mathbb{F}_p, \mathbb{F}_q$) est l'anneau de polynômes à coefficients dans k.
2. $k[x]$ est un anneau *principal* : tout idéal $I \subset k[x]$ est engendré par un seul élément $I = (P)$ où $P \in k[x]$ est un polynôme.

2.1 Rappels

1. $k[x]$ ou k est un corps ($k = \mathbb{R}, \mathbb{C}, \mathbb{F}_p, \mathbb{F}_q$) est l'anneau de polynômes à coefficients dans k.
2. $k[x]$ est un anneau *principal* : tout idéal $I \subset k[x]$ est engendré par un seul élément $I = (P)$ où $P \in k[x]$ est un polynôme.
3. les éléments inversibles (pour la multiplication) de $k[x]$ sont des polynômes constants non nuls $a \in k, a \neq 0$.

2.1 Rappels

1. $k[x]$ ou k est un corps ($k = \mathbb{R}, \mathbb{C}, \mathbb{F}_p, \mathbb{F}_q$) est l'anneau de polynômes à coefficients dans k.
2. $k[x]$ est un anneau *principal* : tout idéal $I \subset k[x]$ est engendré par un seul élément $I = (P)$ où $P \in k[x]$ est un polynôme.
3. les éléments inversibles (pour la multiplication) de $k[x]$ sont des polynômes constants non nuls $a \in k, a \neq 0$.
4. l'idéal (P) est premier $\Leftrightarrow$
   $\Leftrightarrow (P)$ est maximal : $k[x]/(P)$ est un corps $\Leftrightarrow$
   $\Leftrightarrow P$ est irréductible : si $P = Q \cdot R$, $Q, R \in k[x]$, alors Q ou R est inversible, c'est-à-dire, Q ou R est une constante.

2.2 Critères d'irréducibilité dans $\mathbb{Z}[x]$ et dans $\mathbb{Q}[x]$.

Outils :

1. *contenu* : $P \in \mathbb{Z}[x]$, alors le contenu $c(P)$ est le plus grand diviseur commun des coefficients de P.

2.2 Critères d'irréducibilité dans $\mathbb{Z}[x]$ et dans $\mathbb{Q}[x]$.

Outils :

1. *contenu* : $P \in \mathbb{Z}[x]$, alors le contenu $c(P)$ est le plus grand diviseur commun des coefficients de P.

Lemme. $P, Q \in \mathbb{Z}[x] \Rightarrow c(PQ) = c(P) \cdot c(Q)$ (au signe près).

2.2 Critères d'irréducibilité dans $\mathbb{Z}[x]$ et dans $\mathbb{Q}[x]$.

Outils :
1. *contenu* : $P \in \mathbb{Z}[x]$, alors le contenu $c(P)$ est le plus grand diviseur commun des coefficients de P.

Lemme. $P, Q \in \mathbb{Z}[x] \Rightarrow c(PQ) = c(P) \cdot c(Q)$ (au signe près).

Corollaire. $P \in \mathbb{Z}[x]$. Si P est irréductible dans $\mathbb{Z}[x]$, alors P est irréductible dans $\mathbb{Q}[x]$ (voir les notes).

2. *réduction*: $\mathbb{Z}[x] \to \mathbb{F}_p[x]$,

$$P(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_0 \mapsto \bar{P}(x) = \bar{a}_d x^d + \bar{a}_{d-1} x^{d-1} + \ldots + \bar{a}_0$$

où $\bar{a}_i$ est la classe de a_i dans $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, $0 \leq i \leq d$.

2. *réduction*: $\mathbb{Z}[x] \to \mathbb{F}_p[x]$,

$$P(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_0 \mapsto \bar{P}(x) = \bar{a}_d x^d + \bar{a}_{d-1} x^{d-1} + \ldots + \bar{a}_0$$

où $\bar{a}_i$ est la classe de a_i dans $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, $0 \leq i \leq d$.

Critère d'Eisenstein. $P(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_0 \in \mathbb{Z}[x]$.
Supposons qu'il existe p premier tel que

- p divise a_i, $0 \leq i < d-1$ mais p ne divise pas a_d;
- p^2 ne divise pas a_0.

Alors $P(x)$ est irréductible dans $\mathbb{Q}[x]$.

Critère d'Eisenstein

$P(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_0 \in \mathbb{Z}[x]$. Supposons qu'il existe p premier tel que

- p divise a_i, $0 \leq i < d-1$ mais p ne divise pas a_d;
- p^2 ne divise pas a_0.

Alors $P(x)$ est irréductible dans $\mathbb{Q}[x]$.

Preuve.

Critère d'Eisenstein

$P(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_0 \in \mathbb{Z}[x]$. Supposons qu'il existe p premier tel que

- p divise a_i, $0 \leq i < d-1$ mais p ne divise pas a_d;
- p^2 ne divise pas a_0.

Alors $P(x)$ est irréductible dans $\mathbb{Q}[x]$.

Preuve. Supposons le contraire.

Critère d'Eisenstein

$P(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_0 \in \mathbb{Z}[x]$. Supposons qu'il existe p premier tel que

- p divise a_i, $0 \leq i < d-1$ mais p ne divise pas a_d;
- p^2 ne divise pas a_0.

Alors $P(x)$ est irréductible dans $\mathbb{Q}[x]$.

Preuve. Supposons le contraire.
Alors $P = B \cdot C$ avec $B(x) = b_n x^n + b_{n-1} x^{n-1} + \ldots + b_0 \in \mathbb{Z}[x]$
et $C(x) = c_m x^m + c_{m-1} x^{m-1} + \ldots + c_0 \in \mathbb{Z}[x]$.

Critère d'Eisenstein

$P(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_0 \in \mathbb{Z}[x]$. Supposons qu'il existe p premier tel que

- p divise a_i, $0 \leq i < d-1$ mais p ne divise pas a_d;
- p^2 ne divise pas a_0.

Alors $P(x)$ est irréductible dans $\mathbb{Q}[x]$.

Preuve. Supposons le contraire.
Alors $P = B \cdot C$ avec $B(x) = b_n x^n + b_{n-1} x^{n-1} + \ldots + b_0 \in \mathbb{Z}[x]$
et $C(x) = c_m x^m + c_{m-1} x^{m-1} + \ldots + c_0 \in \mathbb{Z}[x]$.
En particulier: $d = m + n$,
$a_d = b_n c_m$ et $a_0 = c_0 b_0$.

Critère d'Eisenstein

$P(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_0 \in \mathbb{Z}[x]$. Supposons qu'il existe p premier tel que

- p divise a_i, $0 \leq i < d-1$ mais p ne divise pas a_d;
- p^2 ne divise pas a_0.

Alors $P(x)$ est irréductible dans $\mathbb{Q}[x]$.

Preuve. Supposons le contraire.
Alors $P = B \cdot C$ avec $B(x) = b_n x^n + b_{n-1} x^{n-1} + \ldots + b_0 \in \mathbb{Z}[x]$
et $C(x) = c_m x^m + c_{m-1} x^{m-1} + \ldots + c_0 \in \mathbb{Z}[x]$.
En particulier: $d = m + n$,
$a_d = b_n c_m$ et $a_0 = c_0 b_0$.
$\Rightarrow$ dans $\mathbb{Z}/p\mathbb{Z}[x]$: $\bar{a}_d x^d = \bar{P} = \bar{B} \cdot \bar{C}$ avec $\bar{a}_d \neq 0$

Critère d'Eisenstein

$P(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_0 \in \mathbb{Z}[x]$. Supposons qu'il existe p premier tel que

- p divise a_i, $0 \leq i < d-1$ mais p ne divise pas a_d;
- p^2 ne divise pas a_0.

Alors $P(x)$ est irréductible dans $\mathbb{Q}[x]$.

Preuve. Supposons le contraire.
Alors $P = B \cdot C$ avec $B(x) = b_n x^n + b_{n-1} x^{n-1} + \ldots + b_0 \in \mathbb{Z}[x]$
et $C(x) = c_m x^m + c_{m-1} x^{m-1} + \ldots + c_0 \in \mathbb{Z}[x]$.
En particulier: $d = m + n$,
$a_d = b_n c_m$ et $a_0 = c_0 b_0$.
$\Rightarrow$ dans $\mathbb{Z}/p\mathbb{Z}[x]$: $\bar{a}_d x^d = \bar{P} = \bar{B} \cdot \bar{C}$ avec $\bar{a}_d \neq 0$
$\Rightarrow \bar{B} = x^n$ et $\bar{C} = x^m$ à multiplication par une constante près.

Critère d'Eisenstein

$P(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_0 \in \mathbb{Z}[x]$. Supposons qu'il existe p premier tel que

- p divise a_i, $0 \leq i < d-1$ mais p ne divise pas a_d;
- p^2 ne divise pas a_0.

Alors $P(x)$ est irréductible dans $\mathbb{Q}[x]$.

Preuve. Supposons le contraire.
Alors $P = B \cdot C$ avec $B(x) = b_n x^n + b_{n-1} x^{n-1} + \ldots + b_0 \in \mathbb{Z}[x]$
et $C(x) = c_m x^m + c_{m-1} x^{m-1} + \ldots + c_0 \in \mathbb{Z}[x]$.
En particulier: $d = m + n$,
$a_d = b_n c_m$ et $a_0 = c_0 b_0$.
$\Rightarrow$ dans $\mathbb{Z}/p\mathbb{Z}[x]$: $\bar{a}_d x^d = \bar{P} = \bar{B} \cdot \bar{C}$ avec $\bar{a}_d \neq 0$
$\Rightarrow \bar{B} = x^n$ et $\bar{C} = x^m$ à multiplication par une constante près.
$\Rightarrow \bar{c}_0 = 0, \bar{b}_0 = 0$, c'est-à-dire, $p | c_0$ et $p | b_0$

Critère d'Eisenstein

$P(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_0 \in \mathbb{Z}[x]$. Supposons qu'il existe p premier tel que

- p divise a_i, $0 \leq i < d-1$ mais p ne divise pas a_d;
- p^2 ne divise pas a_0.

Alors $P(x)$ est irréductible dans $\mathbb{Q}[x]$.

Preuve. Supposons le contraire.
Alors $P = B \cdot C$ avec $B(x) = b_n x^n + b_{n-1} x^{n-1} + \ldots + b_0 \in \mathbb{Z}[x]$
et $C(x) = c_m x^m + c_{m-1} x^{m-1} + \ldots + c_0 \in \mathbb{Z}[x]$.
En particulier: $d = m + n$,
$a_d = b_n c_m$ et $a_0 = c_0 b_0$.
$\Rightarrow$ dans $\mathbb{Z}/p\mathbb{Z}[x]$: $\bar{a}_d x^d = \bar{P} = \bar{B} \cdot \bar{C}$ avec $\bar{a}_d \neq 0$
$\Rightarrow \bar{B} = x^n$ et $\bar{C} = x^m$ à multiplication par une constante près.
$\Rightarrow \bar{c}_0 = 0, \bar{b}_0 = 0$, c'est-à-dire, $p | c_0$ et $p | b_0$
$\Rightarrow p^2$ divise a_0, contradiction.

Exemple : polynômes cyclotomiques.

Exemple : polynômes cyclotomiques.
Soit $\mu_n \subset \mathbb{C}^*$ les racines n-ièmes de l'unités :
$\mu_n = \{\alpha \in \mathbb{C}, \alpha^n = 1\} = \{e^{2ik\pi/n} \mid 0 \leq k < n\}$.

Exemple : polynômes cyclotomiques.
Soit $\mu_n \subset \mathbb{C}^*$ les racines n-ièmes de l'unités :
$\mu_n = \{\alpha \in \mathbb{C}, \alpha^n = 1\} = \{e^{2ik\pi/n} \mid 0 \leq k < n\}$.
Racines *primitives* n-ièmes de l'unité :
$\mu_n^* = \{e^{2ik\pi/n} \mid 0 \leq k < n, (k, n) = 1\}$
le cardinal de μ_n^* est $\phi(n)$.

Exemple : polynômes cyclotomiques.
Soit $\mu_n \subset \mathbb{C}^*$ les racines n-ièmes de l'unités :
$\mu_n = \{\alpha \in \mathbb{C}, \alpha^n = 1\} = \{e^{2ik\pi/n} \mid 0 \leq k < n\}$.
Racines *primitives* n-ièmes de l'unité :
$\mu_n^* = \{e^{2ik\pi/n} \mid 0 \leq k < n, (k, n) = 1\}$
le cardinal de μ_n^* est $\phi(n)$.

$$\Phi_n(x) = \prod_{\xi \in \mu_n^*} (x - \xi).$$

Exemple : polynômes cyclotomiques.
Soit $\mu_n \subset \mathbb{C}^*$ les racines n-ièmes de l'unités :
$\mu_n = \{\alpha \in \mathbb{C}, \alpha^n = 1\} = \{e^{2ik\pi/n} \mid 0 \leq k < n\}$.
Racines *primitives* n-ièmes de l'unité :
$\mu_n^* = \{e^{2ik\pi/n} \mid 0 \leq k < n, (k,n) = 1\}$
le cardinal de μ_n^* est $\phi(n)$.

$$\Phi_n(x) = \prod_{\xi \in \mu_n^*} (x - \xi).$$

Proposition. On a $x^m - 1 = \prod_{n \mid m} \Phi_n(x)$. Pour tout $n \in \mathbb{N}^*$, le polynôme Φ_n est dans $\mathbb{Z}[x]$, c'est un polynôme irréductible.