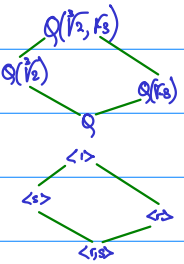
Théorie de Galois - Matilde Lalín

1

Théorie de Galois



M. Lalín

Introduction: La théorie de Galois s'occupe des extensions de corps. Rappelons qu'un anneau A est un ensemble muni de deux opérations $+$ et $\times$ (addition et multiplication) tels que

1. $(A,+)$ est un groupe abélien
2. $\times$ est associative ($(A,\times)$ demi-groupe)
3. $+$ et $\times$ satisfont les lois de distribution

$(a+b)\times c=(a\times c)+(b\times c)$ et $a\times(b+c)=a\times b+a\times c$ $\forall a,b,c\in A$

1. Un anneau $(A,+,\times)$ est commutative si $\times$ est commutative
2. Un anneau $(A,+,\times)$ est unitaire s'il y a un élément $1\in A$ tel que $1\times a=a\times 1=a$ $\forall a\in A$ ($(A,\times)$ monoïde)

Ex $(\mathbb{Z},+,\times)$, $(\mathbb{Z}/n\mathbb{Z},+,\times)$ (n entier positif)

$(\mathbb{Q}[x],+,\times)$ polynômes à coefficients sur $\mathbb{Q}$

Un corps est un anneau commutative, unitaire, non-nul ($1\neq 0$) dont tous les éléments non nuls sont inversibles par la multiplication $\times$

Si E et F sont des corps avec F un sous-corps de E, nous disons aussi que E est une extension de F.

Ex $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})=\{a+b\sqrt{2}\ /\ a,b\in\mathbb{Q}\}$

$$(a+b\sqrt{2})+(c+d\sqrt{2})=(a+c)+(b+d)\sqrt{2}$$
$$(a+b\sqrt{2})(c+d\sqrt{2})=(ac+2bd)+(ad+bc)\sqrt{2}$$

$\mathbb{Q}\subseteq\mathbb{Q}(\sqrt{2})$ est une extension

Ex $\mathbb{F}_2$

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

$\mathbb{F}_4$

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

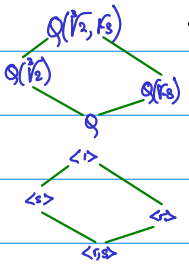
$\times$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

$\mathbb{F}_2\subseteq\mathbb{F}_4$ est une extension

Les extensions sont très importantes dans l'étude des équations algébriques. Dans les cas précédents on s'intéresse à $x^2-2=0$ (sur $\mathbb{Q}$) et à $x^2+x+1=0$ (sur $\mathbb{F}_2$)

La théorie de Galois montre les relations entre les extensions

Théorie de Galois



M. Larín

de corps et la théorie de groupes. Elle est née de l'étude des équations algébriques par Évariste Galois au XIXe siècle. Elle a des applications très variées qui s'étendent de la résolution de vieilles conjectures sur la construction à la règle et au compas, à la géométrie algébrique moderne.

Ex (Résolution d'équations) On connaît bien les solutions de l'équation quadratique.

$$ax^2+bx+c=0 \qquad a\neq 0 \qquad\qquad x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$$

En degré 3 on peut toujours travailler avec $x^3+ax+b=0$ dont les solutions ont été trouvées par Cardan au XVIe siècle. Les 3 solutions sont

$$x_j=\zeta^j\sqrt[3]{-\frac{b}{2}+\sqrt{\left(\frac{a}{2}\right)^3+\left(\frac{b}{2}\right)^2}}+\zeta^{2j}\sqrt[3]{-\frac{b}{2}-\sqrt{\left(\frac{a}{2}\right)^3+\left(\frac{b}{2}\right)^2}}$$

$j=0,1,2 \qquad \zeta=e^{\frac{2\pi i}{3}}=\frac{-1+\sqrt{3}\,i}{2}$, où les racines cubiques sont normalisées par

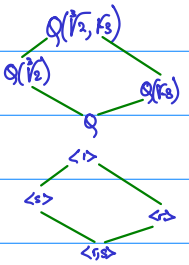
$$\sqrt[3]{-\frac{b}{2}+\sqrt{\left(\frac{a}{2}\right)^3+\left(\frac{b}{2}\right)^2}}\;\sqrt[3]{-\frac{b}{2}-\sqrt{\left(\frac{a}{2}\right)^3+\left(\frac{b}{2}\right)^2}}=-\frac{a}{3}$$

Il est possible de trouver les solutions aux équations de degré 4 aussi (trouvées par Ferrari, étudiant de Cardan)

Dans tous les cas, les racines complexes de l'équation générale initiale sont exprimées à l'aide de racines et polynômes sur les coefficients. On dit que les solutions s'expriment par radicaux.

Quand le degré est $n\geq 5$, il est impossible d'exprimer toutes les solutions par radicaux. Par exemple, on peut montrer à l'aide de la théorie de Galois que les racines de l'équation $x^5-x-1=0$ ne s'expriment pas par radicaux de rationnels

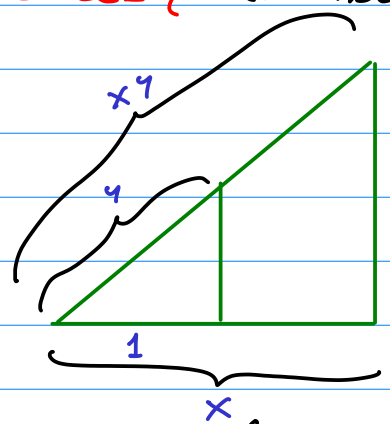
Ex (Construction à la règle et au compas) On identifie le plan euclidien à $\mathbb{C}$ muni de la norme usuelle. On décide que 0 et 1 sont constructibles, puis, étant donnée un famille de points constructibles, on construit les droites passant par deux points



M. Lalín

constructibles distincts, ou bien un cercle centré sur un point constructible de rayon une distance entre deux points constructibles. Ceci définit les droites et cercles admissibles. Les points qui se trouvent aux intersections finies entre deux {droites, cercles} admissibles sont aussi constructibles.

Ex



Étant donnés x, y, on peut construire xy

On peut montrer que l'ensemble de nombres complexes constructibles forme un sous-corps de $\mathbb{C}$. En étudiant ses propriétés, on trouve la réponse aux trois grands problèmes de l'antiquité. À l'aide d'une règle et d'un compas, est-il possible de...

1. ... construire un carré dont l'aire égale celle d'un disque? (Quadrature du cercle)
2. ... construire un cube de volume double? (Duplication du cube)
3. ... sectionner en trois parties égales n'importe quel angle? (Trisection de l'angle)

La réponse est toujours NON!

Quelques notions préliminaires des anneaux

Rappelons qu'un corps est un anneau commutatif unitaire non nul dont tous les éléments non nuls sont inversibles.

Ex : $\mathbb{Q}$ (rationnels), $\mathbb{R}$ (réels), $\mathbb{C}$ (complexes), $\mathbb{Z}/p\mathbb{Z}$ (entiers modulo p, p premier).

Déf : Un morphisme (ou homomorphisme) d'anneaux $\varphi : A \longrightarrow B$ est une application telle

1. $\varphi(a+b) = \varphi(a) + \varphi(b)$
2. $\varphi(ab) = \varphi(a)\,\varphi(b) \quad \forall a, b \in A.$

Ex $\varphi_1 : \mathbb{Z} \longrightarrow \mathbb{Z}/6\mathbb{Z}$ donné par $\varphi_1(a) = \overline{a}$

$\varphi_2 : \mathbb{Z} \longrightarrow \mathbb{Z}$ donné par $\varphi(a) = 6a$ n'est pas un morphisme d'anneaux

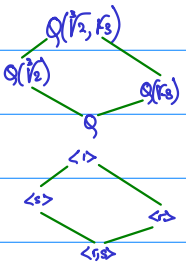
Théorie de Galois

M. Lalín

parce que $6 = \varphi(1) = \varphi(1\cdot 1)$ mais $\varphi(1)\cdot\varphi(1) = 6\cdot 6 = 36$

$\varphi_2 : \mathbb{C} \longrightarrow \mathbb{C}$ $\quad \varphi_2(a+bi) = a-bi$ conjugaison. est un morphisme d'anneaux.

L'ensemble de morphismes est noté par $\mathrm{Hom}(A,B)$



Notons que $\varphi(0_A) = 0_B$ et que $\varphi(-a) = -\varphi(a)$ $\forall a \in A$.

Si A, B unitaire B intègre, $\varphi \neq 0$, alors $\varphi(1_A) = 1_B$

Le noyau est donné par

$$\ker(\varphi) = \{a \in A \mid \varphi(a) = 0_B\}$$

<u>Ex</u> $\ker(\varphi_1) = 6\mathbb{Z} = \{6k \mid k \in \mathbb{Z}\}$ $\quad \ker(\varphi_2) = 0 \in \mathbb{C}$.

Le noyau d'un morphisme est un idéal

<u>Déf:</u> $I \subseteq A$ est un idéal à gauche (à droite) si

1. $a_1, a_2 \in I \Rightarrow a_1 + a_2 \in I$ $\quad$ le même si A commutatif
2. $a \in I,\ c \in A \Rightarrow ca \in I$. $(ac \in I)$

Un idéal $I \subseteq A$ est dit premier si $\forall a_1, a_2 \in A$, $a_1 a_2 \in I \Rightarrow a_1 \in I$ ou $a_2 \in I$.

Un idéal $I \subseteq A$ est dit maximal s'il n'existe pas d'idéal $J \neq A$ tel que $I \subsetneq J$.

<u>Prop</u> Soit A commutatif. Alors, les seuls idéaux de A sont $\{0\}$ et A ssi A est un corps.

<u>Dém</u> Si A corps, $\{0\} \subsetneq I \subsetneq A$, soit $a \in I$, $a \neq 0$. Mais $a^{-1} \in A \Rightarrow a^{-1}a = 1 \in I \Rightarrow I = A$.

Si les idéaux de A sont $\{0\}$, A, soit $a \in A \neq 0$, et $I = (a)$. Alors $I = A \Rightarrow \exists\, b \in A$, $ba = 1 \Rightarrow b = a^{-1}$ #

<u>Déf:</u> Soit $I \subseteq A$ idéal. On dénote par A/I l'ensemble de $a + I = \{a + i \mid i \in I\} \subseteq A$. A/I est dit anneau quotient, parce qu'il est muni des opérations bien définies qui lui donnent une structure d'anneau.

$$(a_1 + I) + (a_2 + I) = (a_1 + a_2) + I$$
$$(a_1 + I)(a_2 + I) = (a_1 a_2) + I$$

On a $\pi : A \longrightarrow A/I$ défini par

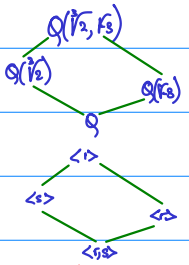
$$a \longrightarrow a + I$$

La projection canonique est un morphisme d'anneaux

Théorie de Galois

M. Lalín

Premier Théorème d'isomorphisme : Si $\varphi : A \longrightarrow B$ est un morphisme d'anneaux, alors, $\ker(\varphi)$ est un idéal de A, $\varphi(A)$ est un sous-anneau de B, et $A/\ker(\varphi) \simeq \varphi(A)$



Dém (Idée) Il est clair que $\varphi(A)$ est un sous-anneau de B et que $\varphi : A \longrightarrow \varphi(A)$ est surjective.

On définit $\tilde{\varphi} : A/\ker(\varphi) \longrightarrow \varphi(A)$

$$\tilde{\varphi}(a+I) = \varphi(a) \quad \text{avec } I = \ker(\varphi)$$

Si $a_1 + I = a_2 + I$, alors $a_1 - a_2 \in I$ et $\varphi(a_1) = \varphi(a_2)$. Le morphisme $\tilde{\varphi}$ est bien défini.

Aussi $\tilde{\varphi}(a+I) = 0 \iff a \in I \iff \varphi(a) = 0 \iff a + I = 0 + I \Rightarrow$ $\tilde{\varphi}$ injective. Il est aussi clair que $\tilde{\varphi}$ surjective

$\Rightarrow \tilde{\varphi}$ bijective #

Ex $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z}$.

Déf Un anneau A commutative, unitaire, non nul est dit **intègre** si $\forall a_1, a_2 \in A$, $a_1 a_2 = 0 \Rightarrow a_1 = 0$ ou $a_2 = 0$

Ex $\mathbb{Z}$ intègre ; F corps $\Rightarrow$ intègre.

$\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre, car $\bar{2} \cdot \bar{3} = \bar{0}$ mais $\bar{2}, \bar{3} \neq \bar{0}$.

Prop ① I est premier ssi A/I est intègre

② I est maximal ssi A/I est un corps

Dém : ① $\Rightarrow$) Soit $a_1 + I, a_2 + I \in A/I$, $a_1 a_2 + I = I \iff a_1 a_2 \in I$

Comme I premier, $a_1 \in I$ ou $a_2 \in I \Rightarrow a_1 + I = I$ ou $a_2 + I = I$

$\Leftarrow$) Exercice.

② Considérons $\pi : A \longrightarrow A/I$

$$a \longrightarrow a + I$$

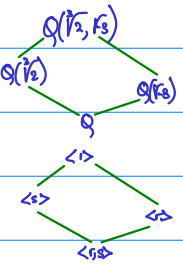
Il y a une correspondence entre idéaux de A qui contiennent I et idéaux de A/I : $J \longleftrightarrow \pi(J) = J + I$ Exercice #

Déf Soit A un anneau intègre.

① $a \in A$ est dit **unité** si $\exists b \in A$ tel que $ab = 1$

② Si $a \in A$ $a \neq 0$ et a n'est pas une unité, on dit que a est **irréductible** si à chaque fois qu'on a $a = bc$, $b, c \in A$, alors on a b ou c unité

③ $a \in A$ $a \neq 0$ est dit **premier** si à chaque fois que $a | bc$, $b, c \in A$ alors on a $a | b$ ou $a | c$



④ $a, b \in A$ sont conjugués si $\exists c \in A$ c unité, tel que $a = bc$

Prop Soit A un anneau intègre. $a \in A$ premier $\Rightarrow a$ irréductible.

Mais $\not\Leftarrow$ Ex: $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ sur $\mathbb{Z}[\sqrt{-5}] \Rightarrow 2 \mid (1+\sqrt{-5})(1-\sqrt{-5})$

mais $2 \nmid (1+\sqrt{-5}), (1-\sqrt{-5})$ et 2 irréductible

Déf: Soit A un anneau intègre. Le corps de fractions $K(A)$ est

$K(A) = \{ (a,b) \mid a, b \in A,\ b \neq 0 \} / \sim$ où

$(a,b) \sim (c,d)$ ssi $ad = bc$ (relation d'équivalence)

On écrit suivant $\frac{a}{b}$ à la place de (a,b)

$K(A)$ est un corps avec les opérations

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{bd}$$

Quelques notions d'anneaux de polynômes

Déf: Soit A un anneau. Les polynômes à une indéterminée x à coefficiens dans A sont

$$A[x] = \{ f(x) = a_0 + a_1 x + \dots + a_n x^n \mid a_i \in A,\ a_n \neq 0 \}.$$

avec les opérations usuelles.

On écrit $n = \deg f(x)$.

L'anneau de polynômes à plusieurs indéterminées est défini par induction

$$A[x_1, \dots, x_{k+1}] := A[x_1, \dots, x_k][x_{k+1}].$$

Si $A = k$ est un corps, $k[x]$ est un corps, $k[x]$ est un anneau euclidien (avec algorithme d'Euclide). On a l'algorithme de division

$f, g \in k[x]$, $g \neq 0$, $\exists q, r \in k[x]$ tels que

$f = q \cdot g + r$, $\deg r < \deg g$ ou $r = 0$.

Ex $f = x^2 + 2x + 5$, $g = 3x + 6 \in \mathbb{Q}[x]$. $f = \frac{x}{3} g + 5$

Mais on ne peut diviser sur $\mathbb{Z}[x]$.

$k[x]$ est aussi un anneau principal (chaque idéal peut être engendré par un seul générateur)

Ex Les idéaux de $\mathbb{Z}$ sont tous de la forme (n), $n \in \mathbb{Z}$

$\mathbb{Z}[x]$ n'est pas principal, $I = (2, x)$

Dans les anneaux principaux, les idéaux premiers sont maximaux

$k[x]$ est aussi un anneau factoriel, avec un équivalent du

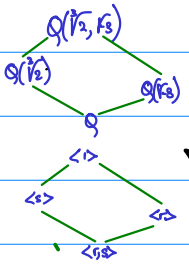
Théorie de Galois

M. Lalín

Théorème fondamental de l'arithmétique : Si $f \in k[x]$, f se décompose en un produit d'un élément du corps k et des polynômes irréductibles unitaires (choisis de façon unique)

(Dans des anneaux factoriels, irréductible $\Leftrightarrow$ premier)

En plus, A anneau factoriel $\Rightarrow$ $A[x]$ anneau factoriel. Donc $A[x_1, \dots, x_k]$ anneau factoriel.



Dans $k[x]$ tout idéal est de la forme $I = (f(x))$. On a que I premier $\Leftrightarrow$ $f(x)$ irréductible.

<u>Dém</u> $\Rightarrow$) Soit $f(x) = a(x)b(x)$. Alors $a(x)b(x) \in I \Rightarrow a(x) \in I$ ou $b(x) \in I$. Mais $a(x) \in I \Leftrightarrow f(x) \mid a(x)$. On a $a(x) = f(x) \cdot a_1(x) \Rightarrow f(x) = f(x) a_1(x) b(x) \Rightarrow a_1(x) b(x) = 1$. $f(x)$ irréductible.

$\Leftarrow$) Soit $g(x)h(x) \in I$. Alors $f(x) \mid g(x)h(x)$. Par unique factorisation, $f(x) \mid g(x)$ ou $f(x) \mid h(x) \Rightarrow g(x) \in I$ ou $h(x) \in I$ #

Alors $k[x]/(f(x))$ est un corps ssi $f(x)$ irréductible

Irréductibilité de polynômes

<u>Prop</u> (Lemme de Gauss) Soit A un anneau factoriel, K son corps de fractions, et $p(x) \in A[x]$. Donc, si $p(x)$ est réductible sur $K[x]$, il est réductible sur $A[x]$.

<u>Coro</u>: Soit A un anneau factoriel, K son corps de fractions, et $p(x) \in A[x]$. Si le pgcd des coefficients de $p(x)$ est 1, alors $p(x)$ est irréductible sur $A[x]$ ssi il est irréductible sur $K[x]$

<u>Ex</u> x^2+5 irréductible sur $\mathbb{Z}[x]$ et $\mathbb{Q}[x]$

$2x^2+10$ irréductible sur $\mathbb{Q}[x]$ mais réductible sur $\mathbb{Z}[x]$

Critères d'irréductibilité de polynômes

<u>Prop</u>: Si $\alpha_1, \dots, \alpha_k \in K$ (pas nécessairement distincts) sont racines du polynôme $p(x) \in K[x]$ ($p(\alpha_i) = 0$), alors

$$(x-\alpha_1) \dots (x-\alpha_k) \mid p(x) \text{ sur } K$$

En particulier, $p(x)$ a un facteur de degré 1 ssi $p(x)$ a une racine sur K. Si $\deg p(x) = 2, 3$, $p(x)$ est réductible ssi $p(x)$ a une racine sur K.

<u>Lemme de la racine</u> Soit $p(x) = a_0 + \dots + a_n x^n \in A[x]$, A anneau

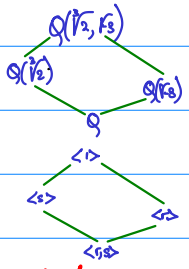
8

Théorie de Galois

M. Larín

FACTORIEL (EX, $A=\mathbb{Z}$) $a_n \neq 0$ SI $\frac{r}{s} \in K(A)$ (EX, $K=\mathbb{Q}$) ET $\frac{r}{s}$ AVEC $\text{pgcd}(r,s)=1$ EST RACINE DE $p(x)$, ALORS $r \mid a_0$ ET $s \mid a_n$

<u>Ex:</u> $p(x)=x^3+10x^2+2x+2 \in \mathbb{Z}[x]$ EST IRRÉDUCTIBLE, CAR LES SEULES RACINES POSSIBLES SONT $\pm 2, \pm 1$, ET $p(1)=15$, $p(-1)=9$, $p(2)=54$, $p(-2)=30$



<u>CRITÈRE D'EISENSTEIN</u> SOIT $p(x)=a_0+\dots+a_n x^n \in A[x]$ ANNEAU FACTORIEL (EX, $A=\mathbb{Z}$) $a_n \neq 0$. SUPPOSONS QU'IL EXISTE UN NOMBRE PREMIER $p \in A$ TEL QUE

1. $p \mid a_i \quad i=0,1,\dots,n-1$
2. $p \nmid a_n$
3. $p^2 \nmid a_0$

ALORS, $p(x) \in K[x]$ EST IRRÉDUCTIBLE. SI $\text{pgcd}(a_0,\dots,a_n)=1$ $p(x) \in A[x]$ IRRÉDUCTIBLE AUSSI.

<u>Ex</u> $x^n+9x+3 \in \mathbb{Z}[x]$, $n \in \mathbb{Z}_{\geq 1}$ EST IRRÉDUCTIBLE. $p=3$

<u>Ex</u> ON NE PEUT UTILISER LE CRITÈRE D'EISENSTEIN SUR $\phi_p(x)=\frac{x^p-1}{x-1}=x^{p-1}+\dots+1$, MAIS ON PEUT LE FAIRE APRÈS UN CHANGEMENT DE VARIABLES, $\phi(x+1)=\frac{(x+1)^p-1}{x}=\sum_{k=1}^{p}\binom{p}{k}x^{k-1}=x^{p-1}+px^{p-2}+\dots+\frac{p(p-1)}{2}x+p \in \mathbb{Z}[x]$. CELA DONNE QUE $\phi_p(x) \in \mathbb{Z}[x]$ EST IRRÉDUCTIBLE

<u>Ex:</u> DANS LE COURS DE THÉORIE DES NOMBRES ON ÉTUDIE LES ENTIERS DE GAUSS $\mathbb{Z}[i]=\{a+bi \mid a,b \in \mathbb{Z}\}$. ON VOIT QUE $\mathbb{Z}[i]$ EST UN ANNEAU EUCLIDIEN ET QUE LES IRRÉDUCTIBLES DE $\mathbb{Z}[i]$ SONT:

(ET CONJUGUÉS)

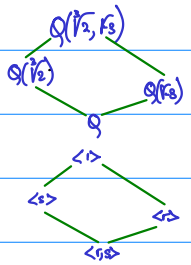
a. $1+i$
b. $p \in \mathbb{Z}$ PREMIER TEL QUE $p \equiv 3 \pmod 4$ $\quad \pm 1, \pm i$
c. $a+bi$, $a-bi$ TELS QUE $a^2+b^2=p$, $p \in \mathbb{Z}$ PREMIER $p \equiv 1 \pmod 4$.

ALORS $x^7+12x^2+18x+6 \in \mathbb{Z}[i][x]$ EST IRRÉDUCTIBLE AVEC $p=3$

ON NE PEUT UTILISER $p=2$ ICI PARCE QUE 2 N'EST PAS PREMIER. DE PLUS, $2=-i(1+i)^2$, ON NE PEUT UTILISER $p=1+i$ PARCE QUE $1+i^2 \mid 2 \mid 6$.

$x^7+10x^2+15x+5 \in \mathbb{Z}[i][x]$ EST IRRÉDUCTIBLE AVEC $p=2+i$ OU $p=2-i$

<u>PROP:</u> SOIT $p(x) \in A[x]$ ANNEAU INTÈGRE, I IDÉAL PROPRE. SI L'IMAGE DE $p(x)$ SUR $A/I[x]$ NE PEUT PAS SE DÉCOMPOSER EN PRODUIT DE POLYNÔMES DE DEGRÉ PLUS PETIT, $p(x)$ EST IRRÉDUCTIBLE SUR $K[x]$



Ex $x^2+1 \in \mathbb{Z}[x]$ irréductible, car il est irréductible sur $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$. Il est réductible sur $\mathbb{Z}/2\mathbb{Z}$, $(x^2+1)=(x+1)^2$

Ex: $x^4+1 \in \mathbb{Z}[x]$ est irréductible, même s'il est réductible sur tous $\mathbb{F}_p$ (on le verra plus tard). Pour voir que x^4+1 est irréductible il faut appliquer le critère d'Eisenstein sur $(x+1)^4+1 = x^4+4x^3+6x^2+4x+2$ avec $p=2$

Prop: Un sous-groupe fini G du groupe multiplicatif d'un corps est cyclique. En particulier, si K est un corps fini, $K^\times$ est cyclique.

Dém: Soit $m \leq |G|$ le plus grand ordre d'un élément de G. Alors l'ordre de chacun des éléments de G est un diviseur de m. Chaque $g \in G$ est solution de l'équation $x^m - 1 = 0$ et cette équation a au moins $|G|$ solutions dans K. Comme chaque racine α donne un diviseur $x-\alpha$ de x^m-1, on a que $|G| \leq m$. Donc $|G| = m$ et il y a un élément $g \in G$ d'ordre $|G| \Rightarrow G$ cyclique #