116: Polynômes irréductibles. Corps de rupture. Exemples et applications.

Pierre Lissy

January 4, 2010

1 Définitions et premières propriétés

1.1 Polynômes irréductibles sur un anneau factoriel

Définition 1. *Soit A un anneau factoriel. On considère l'anneau $A[X]$. Un polynôme de $A[X]$ est dit irréductible ssi P n'est pas un élémént inversible de $A[X]$ et si les seuls diviseurs de P sont les inversibles et les associés.*

Exemple 1. *Si A est un corps, tout polynôme de degré 1 est irréductible. Dans $\mathbb{C}$ les irréductibles de degré 1 sont exactement les polynômes de dergré 1(D'alembert-Gauss). Les irréductibles de $\mathbb{R}$ sonr les polynômes de degré 1 et ceux de degré 2 de discriminant strictement négatif. X est irréductible sur $\mathbb{Z}$.*

Remarque 1. *Si un polynôme P est irréductible sur une extension d'anneau B de A et à coefficient dans A alors P est irréductible sur A. Ceci est vrai par exemple pour $B = Fr(A)$.*

Réciproque évidemment fausse.

Exemple 2. *$2X$ n'est pas irréductible dans $\mathbb{Z}$ (car 2 est un diviseur non inversible non associé), mais il l'est dans $\mathbb{Q}$ (car 2 devient alors un élément inversible). $X^2 - 2$ est irréductible dans $\mathbb{Q}$ mais pas dans $\mathbb{R}((X^2 - 2 = (X - \sqrt{2})(X + sqrt2))$. $X^2 + 1$ est irréductible dans $\mathbb{R}$ mais pas dans $\mathbb{C}$.*

En fait, si on se donne un polynôme irréductible, on pourra toujours trouver une extension dans lequel il sera réductible, et même scindé. cf suite.

Proposition 1. *Un polynôme de degré 2 ou 3 sur un corps est irréductible ssi il n'admet aucune racine.*

1.2 Corps de rupture d'un polynôme irréductible

Définition 2. *Soit K un corps et $P \in K[X]$ irréductible. On appelle corps de rupture de P sur K tout extension de corps L de K monogène (ie $L = K(\alpha)$ avec $P(\alpha) = 0$.*

Lemme 1. *Soit P un polynôme irréductible sur un corps K. Alors l'idéal (P) est maximal, donc $K[X]/(P)$ est un corps.*

Théorème 1. *Il y a toujours existence du corps de rupture: on peut par exemple prendre l'anneau quotient K[X]/(P) (une racine est alors l'image de X). De plus, un corps de rupture est unique à isomorphisme près. Enfin, le degré de l'extension est celui du polynôme minimal.*

Exemple 3. *On considère le polynôme $X^2 + 1$ sur $\mathbb{R}$. Il est irréductible. Son corps de rupture est $\mathbb{R}[X]/(X^2 + 1) = \mathbb{R}[i] = \mathbb{C}$*

Exemple 4. *On considère le polynômeX$^3 - 2$ sur $\mathbb{Q}$. Il est irréductible. Son corps de rupture est $Q[X]/X^3 - 2 = Q[\sqrt[3]{2}]$, c'est une extension de degré 3 de $\mathbb{Q}$.*

Ce n'est pas parce qu'un corps de rupture contient une racine qu'il contient tous les autres.

Exemple 5. *$Q[X]/X^3-2 = Q[\sqrt[3]{2}]$ ne contient pas les racines complexes de X^3-2 qui sont $\sqrt[3]{2}j$ et $\sqrt[3]{2}j^2$.*

C'est pourquoi on introduit la notion de corps de décomposition.

2 Corps de décomposition

Définition 3. *Soit P un polynôme (non nécessairement irréductible). On appelle corps de décomposition de P sur K toute extension L de K dans laquelle P est scindé (ie qui contient toutes les racines de P) et qui soit minimale pour cette propriété.*

Théorème 2. *Il existe toujours un corps de décomposition. De plus, ce corps est unique à isomorphisme près. Enfin, le degré du corps de décomposition est inférieur à $n!$.*

Remarque 2. *Si le polynôme est déjà scindé dans le corps, alors son corps de décomposition est lui-même: cette remarque montre que contrairement au cas du corps de rupture, on atteint pas forcément le degré maximal qu'est $n!$.*

Exemple 6. *Le corps de décomposition de X^3-2 sur $\mathbb{Q}$ est $Q[\sqrt[3]{2}, j]$. C'est trivialement une extension de degré 6 (elle contient $Q[\sqrt[3]{2}]$ de degré 2 et $Q[j]$ de degré 3, donc elle est au moins de degré 6 car 2 et 3 sont premiers entre eux)*

En général le corps de décomposition est strictement plus grand que le corps de rupture comme l'a montré les exemples ci-dessus.

Exemple 7. *Le corps de décomposition de X^4-2 sur $\mathbb{Q}$ est $Q[\sqrt[4]{2}, i]$.*

On a pas forcément que le degré de l'extension est n! même si le polynôem est irréductible.

Exemple 8. *X^4+1 est irréductible sur $\mathbb{R}$. Son corps de rupture est $\mathbb{C}$, et c'est aussi son corps de décomposition car $\mathbb{C}$ contient toutes les racines de X^4+1 (qui sont des racindes doubles i et -i).*

Cet exemple est un peu artificiel car $\mathbb{C}$ est algébriquement clos. Donnons-en un autre.

Exemple 9. *Le corps de décomposition de X^4-1 sur $\mathbb{Q}$ est $Q[1, i]$ de degré 2.*

3 Critères d'irréductibilité de polynômes

3.1 Irréductibilité et contenu

Définition 4. *On appelle contenu d'un polynôme P, sur un anneau factoriel A le pgcd des coefficients de A, noté $C(P)$. Un polynôme est dit primitif ssi son contenu est 1.*

Proposition 2. $C(PQ) = C(P)C(Q)$.

Théorème 3. *Les polynômes irréductibles sur $A[X]$ sont soit les constantes irréductibles de A, soit les polynômes de degré au moins 1 irréductibles sur $K[X]$ et primitifs. Notamment si l'on se donne un polynôme P irréd sur $K[X]$ alors $P/C(P)$ est irréductible sur A.*

On en déduit notamment

Application 1 (Théorème de transfert de Hilbert)**.** *Si A est factoriel alors $A[X]$ l'est aussi.*

3.2 Critère D'Eisenstein

Théorème 4 (Critère d'Eisenstein)**.** *Soit $P \in \mathbb{Z}[X]$, $P = a_nX^n + \ldots + a_0$. Soit p un nombre premier. On suppose:*

1. *$p \not| a_n$,*
2. *$p|a_i$, pour $i \leqslant n-1$,*

3. $p^2 \not| a_0$.

Alors P est irréductible sur $\mathbb{Q}$.(et donc dans $\mathbb{Z}$ pourvu que P soit primitif)

Exemple 10. *Si p est un nombre premier, $X^{p-1} + \ldots + X + 1$ est irréductible sur $\mathbb{Z}$. (appliquer Eisenstein à $P(X+1)$)*

3.3 Réduction modulo un idéal premier

Théorème 5 (Réduction modulo un idéal premier)**.** *Soit I un idéal premier (ie. A/I intègre) et soit $P \in \mathbb{A}[X]$, $P = a_n X^n + \ldots + a_0$. On pose $\bar{P} = C_I(a_n)X^n + \ldots + C_I(a_0)$. Si $\bar{P}$ est irréductible dans A/I ou dans $Fr(A/I)$, alors P est irréductible dans $Fr(A)[X]$ (et donc dans $A[X]$ si P est primitif).*

Exemple 11. *Soit p un nombre premier. $X^p - X - 1$ est irréductible sur $\mathbb{Z}$ (car il l'est sur $\mathbb{Z}/p\mathbb{Z}$).*

Rappelons les lemmes suivants, bien utiles.

Lemme 2. *Un polynôme de degré 2 ou 3 est irréductible ssi il admet une racine*

Exemple 12. *En application directe du théorème et du lemme précédent on a aussi l'irréductibilité des polynômes suivants:*

1. $X^3 + 462X^2 + 2433X - 67691$ *est irréductible sur $\mathbb{Z}$ (car il l'est sur $\mathbb{Z}/2\mathbb{Z}[X]$)*
2. $X^3 + 4X^2 - 5X + 7$ *est irréductible sur $\mathbb{Z}$ (car il l'est sur $\mathbb{Z}/2\mathbb{Z}[X]$)*
3. $X^3 - 6X^2 - 4X - 13$ *est irréductible sur $\mathbb{Z}$ (car il l'est sur $\mathbb{Z}/3\mathbb{Z}[X]$)*
4. $X^3 + 30X^2 + 6X + 1$ *est irréductible sur $\mathbb{Z}$ (car il l'est sur $\mathbb{Z}/5\mathbb{Z}[X]$)*

Signalons le lemme suivant, qui est aussi utile.

Lemme 3. *$X^2 + X + 1$ est l'unique polynôme irréductible de degré 2 sur $\mathbb{F}_2$. Donc tout polynôme n'admettant pas de racines dans $\mathbb{F}_2$ et distinct de $(X^2 + X + 1)^2 = 1 + X^2 + X^4$ est irréductible.*

Exemple 13. 1. $5X^4 + 17X^3 - X^2 - 6X + 23$ *est irréductible sur $\mathbb{Z}$ (car il l'est sur $\mathbb{Z}/2\mathbb{Z}[X]$)*
2. $X^4 + 5X^3 - 3X^2 - X + 7$ *est irréductible sur $\mathbb{Z}$ (car il l'est sur $\mathbb{Z}/2\mathbb{Z}[X]$)*

dans $\mathbb{F}_3$ on a

Lemme 4. *Les polynômes irréductibles unitaires de degré 2 sont X^2+1, X^2-X-1 et X^2+X-1. Donc tout polynôme de degré 4 sans racines dans $\mathbb{F}_3$ et non divisible par un de ces polynômes est irréductible.*

Exemple 14.
$X^4 + 7X^2 4X + 1$ *est irréductible sur $\mathbb{Z}$ (car il l'est sur $\mathbb{Z}/3\mathbb{Z}[X]$, alors qu'i lest réductible sur $\mathbb{Z}/2\mathbb{Z}[X]$)*

On peut généraliser cette méthode à des polynôems de degré plus grands. On a aussi une application plus subtile du théorème.

Exemple 15. *$X^4 + 4X^3 + 3X^2 + 7X - 4$ est réductible modulo $2, 3, 5, 7et11$, on n'arrive donc pas à conclure directement. Mais on montre en utilisant la forme factorisée modulo 3 que P ne peut admettre de racines dans $\mathbb{Z}$ et on montre en utilisant la forme factorisée modulo 2 qu'il ne peut pas non plus se mettre sous forme de produits de polynômes de degré 2 irréductibles. Il est donc bien irréductible.*

Réciproque du théorème de réduction fausse.

Exemple 16. *$X^4 + 1$ irréductible sur $\mathbb{F}_p$ mais réductible sur tous les $\mathbb{F}_p$.*

3.4 Irréductibilité et extensions de corps

Théorème 6. *Soit k un corps; Alors $p \in k(X]$ est irréductible ssi il n'admet pas de racines dans toute extension de degré inférieure $(degP)/2$.*

Exemple 17. *$X^4 + X + 1$irréductible sur $\mathbb{F}_2$, donc $X^4 + 8X^2 + 17X - 1$ irréductible sur $\mathbb{Z}$*

Théorème 7. *Soit k un corps et K une extension de degré m premier avec le degré d'un polynôme P. Si P est irréductible sur k il l'est encore sur K.*

Exemple 18. *$X^3 + X + 1$ irréductible sur $\mathbb{Q}$ donc sur $\mathbb{Q}[i]$.*

Faux si pas premiers entre eux.

Exemple 19. *$X^4 + 1$ irréductible sur $\mathbb{Q}$ mais pas sur $\mathbb{Q}[i]$.*

4 Applications à la théorie des corps

4.1 Construction des corps finis

Théorème 8. *Soit $q = p^n$. Alors il existe un corps de cardinal q et de caractéristique p, on peut prendre par exemple le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p$. De plus, K est unique à isomorphisme près. Ce corps est noté $\mathbb{F}_q$.*

Remarque 3. *Dans le cas des corps finis, le corps de rupture d'un polynôme irréductible est nécessairement le corps de décomposition de ce polynôme irréductible. En pratique, on préfère écrire les corps finis comme des corps de rupture d'un poynôme irréductible grâce au théorème suivant.*

Théorème 9. *$\mathbb{F}_{p^n}$ est le corps de rupture de tout polynôme irréductible de degré n sur $\mathbb{Z}/p\mathbb{Z}$.*

Exemple 20. $\mathbb{F}_4 \simeq \mathbb{Z}/2\mathbb{Z}[X]/(1+X+X^2)$ $\mathbb{F}_8 \simeq \mathbb{Z}/2\mathbb{Z}[X]/(1+X+X^3)$, $\mathbb{F}_9 \simeq \mathbb{Z}/3\mathbb{Z}[X]/(X^2+1)$, $\mathbb{F}_16 \simeq \mathbb{Z}/2\mathbb{Z}[X]/(1+X+X^4)$.

4.2 Extensions quadratiques de $\mathbb{Q}$

5 Autres applications

5.1 Polynôme minimal d'un élément d'un corps. Théorème de l'élément primitif

On se donne une extension de corps $k \subset K$.

Définition 5. *Un élément $\alpha \in K$ est dit algébrique sur k ssi il existe un polynôme non nul à coefficient dans k qui annule α. Sinon α est dit transcendant.*

Proposition 3. *Si α est un élément algébrique alors L'ensemble des annulateurs de α est un idéal de $k[X]$ qui est principal. On appelle $\mu(\alpha)$ le polynôme engendrant cet idéal, il est appelé polynôme annulateur.*

Théorème 10. *On a les équivalences suivantes:*

1. *α algébrique*
2. *$K[\alpha] = K(\alpha)$*
3. *$K[\alpha]$ de dimension finie*

De plus, dans ce cas, le polynôme minimal est irréductible et la dimension de $K[\alpha]$ est le degré du polynôme minimal. De plus, $K[\alpha] \simeq K[X]/(\mu(\alpha))$.

Proposition 4. *L'ensemble des éléments de K algébriques sur k forment un sous-corps de k.*

Signalons le théorème suivant.

Théorème 11 (élément primitif)**.** *On considère une extension finie L d'un corps K (fini ou infini). Alors $\exists \alpha | K[\alpha] = L$.*

Exemple 21. *Le corps de décomposition du polynôme $X^4 - 2$ est $Q[^4 sqrt(2), i] = Q[i +^4 \sqrt(2)]$.*

5.2 Polynômes cyclotomiques

Dans toute la suite on prend n premier à la caractéristique de k.

Proposition 5. *Soit k un corps. On appelle $\mu_n(k)$ l'ensemble des racines n-ièmes de l'unité. C'est un sous-groupe de k^* fini, il est donc cyclique. On appelle racine n-ième primitive une racine qui engendre ce groupe. Il y en a exactement $\varphi(n)$. On note $\mu_n(k)^*$ cette ensemble de générateurs.*

Définition 6. *n-ième polynôme cyclotomique: $\Phi_n(X) = \prod_{x \in \mu_n(k)^*} (X - x)$. C'est un polynôme unitaire de degré $\varphi(n)$.*

Proposition 6. $X^n - 1 = \prod_{d|n} \varphi(d)$.

Proposition 7. *On considère les polynômes cyclotomiques dans $\mathbb{Q}$. Alors leurs coefficients son entiers. De plus, si on se donne un morphisme d'anneaux $\sigma : \mathbb{Z} \to k$ on obtient le polynôme cyclotomique sur k en réduisant les coefficients par σ.*

Théorème 12. *Les polynômes cyclotomiques sont irréductibles sur $\mathbb{Z}$ (donc sur $\mathbb{Q}$).*

Remarque 4. *L'écriture de $X^n - 1$ est donc la décomposition en irréductibles de ce polynôme sur $\mathbb{Q}[X]$!*

Corollaire 1. *Le polynôme minmal d'une racine n-ième primitive est donc $Phi_n(X)$ et $[Q(\alpha) : Q] = \varphi(n)$.*

Corollaire 2. *On se donne deux racines n-ièmes et m-ièmes de l'unité primitives α et β. Alors $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}$.*

Citons une application des polynôems cyclotomiques.

Application 2. *[1][petit théorème de Dirichlet page 272] Il existe une infinité de nombres premiers de la forme $an + 1$.*

Application 3 (Théorème de Wedderburn)**.** *La commutativité est une conséquence des autres axiomes de la structure de corps fini.*

References

[1] Combes

[2] Gourdon algèbre

[3] Objectif agrégation

[4] Perrin

[5] Ortiz

[6] Lang