

Comportement des nombres premiers dans un anneau des entiers monogène

Tilliet Florian

N'hésitez pas à envoyer un mail à prenom.nom@ens-remes.fr si vous trouvez une erreur.

Leçons: 121, 125, 141

Prérequis: Il s'agit d'un développement original mais assez largement hors du programme. Pour présenter ce développement il est nécessaire d'être au point sur les notions de corps de nombre, d'anneaux des entiers, de factorisation en idéaux premiers dans ces anneaux ainsi que de norme d'un idéal.

Cela représente un bagage théorique assez lourd mais qui offre au candidat un développement original, intéressant, d'un très bon niveau et rentrant en 15 min dans soucis.

Motivation: Dans un anneau des entiers d'un corps de nombre, les nombres qui étaient premiers dans \mathbb{Z} peuvent ne plus engendrer un idéal premier comme ils le faisaient dans \mathbb{Z} . Par exemple, dans $\mathbb{Z}[i]$ on a $5 = (1+2i)(1-2i)$ ou bien $2 = -i(1+i)^2$. Certains, comme 3, sont toujours premiers. On se propose de donner une méthode pour déterminer la nouvelle factorisation d'un idéal engendré par un nombre premier dans le cas d'un anneau monogène.

Cette méthode présente des intérêts à la fois théorique et pratique. On pourra par exemple s'intéresser au cas particulier des anneaux quadratiques ou bien au tout algorithmique de factorialité qui en découle.

Résultat préliminaire: On aura besoin du résultat suivant:

Théorème: Soit K un corps de nombre et a, b deux idéaux de l'anneau des entiers \mathcal{O}_K . Alors:

- $a \subset b$ si et seulement s'il existe un idéal c tel que $a = bc$. On note alors $b|a$.
- Il existe des uniques idéaux premiers $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ tels que $a = \mathfrak{p}_1 \dots \mathfrak{p}_n$.

Démonstration: Voir "Algebraic Number Theory and Fermat last Theorem" Stewart & Tall.
↳ = ANT & FLT Th 5.6, Pr 5.7

Le développement: (Ref: ANT & FCT Th 10.1)

Théorème: Soit K un corps de nombre dont l'anneau des entiers est de la forme $\mathbb{Z}[\theta]$ avec un $\theta \in G_K$. Notons $f \in \mathbb{Z}[X]$ le polynôme minimal de θ . Soit p un nombre premier. La réduction \bar{f} de f modulo p admet une factorisation en polynômes irréductibles dans $\mathbb{F}_p[X]$:

$$\bar{f} = \bar{f}_1^{e_1} \dots \bar{f}_r^{e_r}$$

où l'on peut choisir les $f_i \in \mathbb{Z}[X]$ de sorte que $d_i := d^{\circ} f_i = d^{\circ} \bar{f}_i$.

Notons $\mathfrak{p}_i := \langle p \rangle + \langle f_i(\theta) \rangle$ pour $1 \leq i \leq r$.

Alors les \mathfrak{p}_i sont premiers et $\langle p \rangle = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$.

Démonstration: Montrons d'abord que les \mathfrak{p}_i sont premiers. Soit $i \in \{1, \dots, r\}$. \bar{f}_i est irréductible donc $\mathbb{F}_p[X]/\bar{f}_i$ est un corps et il contient une racine θ_i de \bar{f}_i . Considérons:

$$\begin{aligned} \psi: \mathbb{Z}[\theta] &\longrightarrow \mathbb{F}_p[\theta_i] \cong \mathbb{F}_p[X]/\bar{f}_i \\ g(\theta) &\longmapsto \bar{g}(\theta_i) \end{aligned}$$

Alors:

- ψ est bien défini: Si $g(\theta) = h(\theta)$ alors $(g-h)(\theta) = 0$ donc $f \mid g-h$ car f est le polynôme minimal de θ . Puis $\bar{f}_i \mid \bar{f} \mid \bar{g} - \bar{h}$ et $\bar{g}(\theta_i) = \bar{h}(\theta_i)$.

- ψ est un morphisme d'anneau.

- ψ est surjectif.

- $\text{Ker } \psi = \mathfrak{p}_i$: \Rightarrow Si $g(\theta) \in \text{Ker } \psi$ alors \bar{g} annule θ_i donc $\bar{f}_i \mid \bar{g}$ d'où $g(\theta) \in \langle p \rangle + \langle f_i(\theta) \rangle = \mathfrak{p}_i$. L'autre inclusion est claire.

Ainsi, le premier théorème d'isomorphisme donne $\mathbb{Z}[\theta]/\mathfrak{p}_i \cong \mathbb{F}_p[X]/\bar{f}_i$ qui

est un corps donc intègre et cela assure que f est premier.

• On montre maintenant l'égalité entre les idéaux. Pour cela, on montre une divisibilité puis l'on conclut par un argument de norme.

On utilise le fait facile à vérifier suivant:

Fait: Pour tout idéaux a, b, c on a: $(a+b)(a+c) \subset a+bc$.

Alors $\mathfrak{p}_i^2 = (\langle p \rangle + \langle f_i(\theta) \rangle)^2 \subset \langle p \rangle + \langle f_i(\theta)^2 \rangle$.

En itérant:

$$\mathfrak{p}_i^{e_i} \dots \mathfrak{p}_r^{e_r} \subset \langle p \rangle + \langle f_i^{e_i}(\theta) \dots f_r^{e_r}(\theta) \rangle = \langle p \rangle$$

car $(f_i^{e_i} \dots f_r^{e_r})(\theta) = f(\theta) = 0 \pmod{\mathfrak{p}}$

Par le théorème préliminaire, cela assure que $\langle p \rangle \mid \mathfrak{p}_i^{e_i} \dots \mathfrak{p}_r^{e_r}$.

Ainsi, si \mathfrak{q} est un idéal premier de la factorisation de $\langle p \rangle$ alors il est aussi dans celle de $\mathfrak{p}_i^{e_i} \dots \mathfrak{p}_r^{e_r}$ et l'unicité assure que \mathfrak{q} est l'un des \mathfrak{p}_i .

La factorisation en idéaux premiers est de la forme:

$$\langle p \rangle = \mathfrak{p}_1^{k_1} \dots \mathfrak{p}_r^{k_r} \quad \text{avec } 0 \leq k_i \leq e_i.$$

De plus, il est clair que $\langle p \rangle \subset \mathfrak{p}_i$ donc $\mathfrak{p}_i \mid \langle p \rangle$ et $k_i \geq 1$ pour tout i .

Il ne reste plus qu'à conclure:

① d'une part:

$$\begin{aligned} N(\langle p \rangle) &= N(\mathfrak{p}_1^{k_1} \dots \mathfrak{p}_r^{k_r}) = N(\mathfrak{p}_1)^{k_1} \dots N(\mathfrak{p}_r)^{k_r} \\ &= |G_K/\mathfrak{p}_1|^{k_1} \dots |G_K/\mathfrak{p}_r|^{k_r} \\ &= (p^{d_1})^{k_1} \dots (p^{d_r})^{k_r} \\ &= p^{\sum d_i k_i} \end{aligned}$$

Multiplicativité de la norme

car $G_K/\mathfrak{p}_i \cong \mathbb{F}_p(K)/\mathfrak{f}_i$
et $d_i = d^{\circ} \mathfrak{f}_i$

D'autre part :

$$N(\langle p \rangle) = |N(p)| = p^n = p^{\sum d_i e_i}$$

Norme d'un idéal principal

car K est de degré n (génère \mathbb{Q} sur \mathbb{Z} donc K sur \mathbb{Q})

car $\bar{f} = \prod \bar{f}_i^{e_i}$, $d_i = d^\circ f_i$
et $d^\circ \bar{f} = d^\circ f$ puisque f est unitaire
en tant que poly minimal.

Finalement $\sum d_i k_i = \sum d_i e_i$ et les inégalités sur les k_i et e_i conclut à $k_i = e_i$ pour tout $i \in \{1, \dots, r\}$.

Cela termine la preuve.

Remarques : Si l'on présente ce développement, il peut être intéressant de connaître ces quelques remarques :

- Les corps de nombres quadratiques et cyclotomiques donnent des anneaux des entiers monogènes. Mais ce n'est pas le cas pour tous les corps de nb. (ANT & FLT)
- En utilisant ce théorème dans le cas quadratique on peut démontrer le résultat bien connu suivant : Si K est un corps de nb quadratique de discriminant Δ alors pour $p \neq 2$, on a :
$$\left\{ \begin{array}{l} p \text{ inert } \Rightarrow \left(\frac{\Delta}{p}\right) = -1 \\ p \text{ ramifié } \Rightarrow \left(\frac{\Delta}{p}\right) = 0 \\ p \text{ scindé } \Rightarrow \left(\frac{\Delta}{p}\right) = 1 \end{array} \right.$$
- Le théorème permet d'obtenir un algorithme pour trouver la décomposition d'un nombre premier en utilisant un algorithme de factorisation de polynôme sur un corps fini. On peut par exemple trouver des algos de factorisation dans "Cours d'Algèbre" de Demazure.

Pour aller plus loin : Pour terminer, on présente une application un peu plus profonde de ce théorème. Je ne pense pas qu'il soit nécessaire de connaître ce qui suit pour présenter ce développement.

Rappelons qu'un anneau des entiers est factoriel si et seulement s'il est principal. Cela se démontre sans trop de mal une fois la factorisation unique en idéaux premiers acquise. ^(ANT & FLT) Le théorème du développement permet alors un test algorithmique pour savoir si un anneau des entiers monogène est factoriel ou principal. Ce test repose sur le théorème qui suit.

Théorème: Soit K un anneau des entiers de degré $n = r_1 + 2r_2$ et de discriminant Δ . Supposons que tout premier $p \in \mathbb{Z}$ avec $p \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|\Delta|}$ n'admet que des idéaux premiers principaux dans sa décomposition dans \mathcal{O}_K . Alors \mathcal{O}_K est principal.

Démonstration: Il s'agit d'une conséquence assez directe de la borne de Minkowski. Il semble donc important de connaître le théorème de Minkowski si l'on décide de parler de ça. Voir [ANT & FLT, Cor 10.3 et Th 10.4](#).

Combinant ces deux théorèmes, on peut démontrer la principalité de certain anneaux des entiers de degrés petits. Par exemple, les corps $\mathbb{Q}(\sqrt{d})$ avec $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$ donnent des anneaux principaux. Remarquons que certains parmi eux ne sont pas euclidiens, on a l'exemple classique $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$. [ANT & FLT 10.5 pour les détails](#).

Remarque finale, ce sont les seules valeurs de $d < 0$ sans facteurs carrés qui donnent un anneau principal. Pour le coup il s'agit là d'un théorème difficile.

