Comportement des nombres premiers dans un anneau des entiers monogène

Tilliet Florian

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

Leçons : 121, 125, 141

Prérequis : Il s'agit d'un développement que j'aime beaucoup 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 celle 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 sans soucis.

Motivation : Dans un anneau des entiers d'un corps de nombre, les nombres qui étaient premiers dans $\mathbb{Z}$ peuvent ne plus engendré 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 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 test 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 $b \mid a$.
- Il existe des uniques idéaux premier $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ tels que $a = \mathfrak{p}_1 \cdots \mathfrak{p}_n$.

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

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

Théorème : Soit K un corps de nombre dont l'anneau des entiers est de la forme $\mathbb{Z}[\theta]$ avec un $\theta \in \mathcal{O}_K$. 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 polynôme irréductible dans $\mathbb{F}_p[X]$:

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

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 $\langle p \rangle = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$.

Démonstration : • Montrons d'abord que les $\mathfrak{p}_i$ sont premiers. Soit $i \in [\![1, r]\!]$.
$\bar{f}_i$ 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 :

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

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.

- $\ker \psi = \mathfrak{p}_i$: ⊃ Si $g(\theta) \in \ker \psi$ 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 $\mathfrak{p}_i$ est premier.

• On montre maintenant l'égalité entre les idéaux. Pour cela, on montre une divisibilité puis l'on conclura 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 :

$$\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} \subset \langle p \rangle + \langle f_1^{e_1}(\theta) \cdots f_r^{e_r}(\theta) \rangle = \langle p \rangle$$

car $(f_1^{e_1} \cdots f_r^{e_r})(\theta) \equiv f(\theta) \equiv 0 \ (\mathfrak{p})$

Par le théorème préliminaire, cela assure que $\langle p \rangle \mid \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$.
Ainsi, si $\mathfrak{q}$ est un idéal premier de la factorisation de $\langle p \rangle$ alors il est aussi dans celle de $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ et l'unicité assure que $\mathfrak{q}$ est l'un des $\mathfrak{p}_i$.
La factorisation en idéaux premier est de la forme :

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

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 que à conclure :

D'une part :

$$N(\langle p \rangle) = N(\mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_r^{k_r}) = N(\mathfrak{p}_1)^{k_1} \cdots N(\mathfrak{p}_r)^{k_r}$$

(multiplicativité de la norme)

$$= |\mathcal{O}_K/\mathfrak{p}_1|^{k_1} \cdots |\mathcal{O}_K/\mathfrak{p}_r|^{k_r}$$

$$= (p^{d_1})^{k_1} \cdots (p^{d_r})^{k_r}$$

car $\mathcal{O}_K/\mathfrak{p}_i \simeq \mathbb{F}_p(K)/\overline{f_i}$ et $d_i = d^\circ \overline{f_i}$

$$= p^{\sum d_i k_i}$$

D'autre part :

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

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

($N(\langle p \rangle)$: Norme d'un idéal principal)

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 concluent à $k_i = e_i$ pour tout $i \in [\![1, r]\!]$.

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 :

$$\begin{cases} p \text{ inert si } \left(\frac{\Delta}{p}\right) = -1 \\ p \text{ ramifié si } \left(\frac{\Delta}{p}\right) = 0 \\ p \text{ scindé si } \left(\frac{\Delta}{p}\right) = 1 \end{cases}$$

- 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 en trouver 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 qu'il soit nécessaire de connaître ce qu'il 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 G_K.
Alors G_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 euclidien, 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 pour $d < 0$ sans facteurs carrés qui donnent ce résultat. Pour le coup il s'agit là d'un théorème difficile.