UPS – Centre d'Orsay **Arithmétique – Maîtrise**
Mathématiques Année 2003–2004

DEVOIR n° 2 (pour la semaine du 10/05)

Dans tout le devoir, K désigne un corps de nombres de degré $n = \dim_{\mathbb{Q}} K$. On appelle *ordre*[1] de K un sous-anneau $\mathcal{O} \subset K$, qui est un $\mathbb{Z}$-module de rang n. Par exemple, l'anneau des entiers $\mathcal{O}_K$ de K est un ordre. On écrira $K = \mathbb{Q}(\alpha)$, où $\alpha \in \mathcal{O}_K$ a pour polynôme minimal (unitaire) $T \in \mathbb{Z}[X]$.

Soit p un nombre premier. Un ordre est dit *p-maximal* si p ne divise pas l'indice $[\mathcal{O}_K : \mathcal{O}]$. Ce problème présente l'algorithme « Round 2 » (Zassenhaus, 1965), qui permet de calculer $\mathcal{O}_K$ à partir de T. Une version simplifiée permet de décider si un ordre $\mathcal{O}$ est p-maximal. Celle-ci est particulièrement simple quand $\mathcal{O}$ est de la forme $\mathbb{Z}[\alpha]$:

Théorème 1 (Dedekind)**.** *Soit $T \in \mathbb{Z}[X]$ le polynôme minimal de α. Soit $\overline{T} = \prod_i \overline{t_i}^{e_i}$ la factorisation de T dans $\mathbb{F}_p[X]$, où les $\overline{t_i}$ sont irréductibles, unitaires et distincts. On note*

- *f un relèvement dans $\mathbb{Z}[X]$ de $\prod_i \overline{t_i}$,*
- *g un relèvement dans $\mathbb{Z}[X]$ de $\overline{T}/\overline{f}$,*
- *$h := (T - fg)/p \in \mathbb{Z}[X]$.*

Soit finalement $\delta := \operatorname{pgcd}(\overline{f}, \overline{g}, \overline{h})$ dans $\mathbb{F}_p[X]$. Alors $\mathbb{Z}[\alpha]$ est p-maximal ssi $\delta = 1$.

I (Exemples)

1) Quels sont les ordres de $\mathbb{Q}$?

2) Si $K = \mathbb{Q}(\alpha)$, où $\alpha \in \mathcal{O}_K$, montrer que $\mathbb{Z}[\alpha]$ est un ordre. Qu'en est-il si $\alpha \notin \mathcal{O}_K$?

3) Montrer que tout ordre de K est inclus dans $\mathcal{O}_K$. [*C'est pourquoi on appelle aussi l'anneau des entiers l'*ordre maximal *de K.*]

II (Division)

Si A et B sont deux sous-$\mathbb{Z}$-modules de K, on note $(A : B) = \{\alpha \in K, \alpha B \subset A\}$, qui se lit « A divisé par B ». Si A et B sont deux parties de K, on note AB le $\mathbb{Z}$-module engendré par les ab, $a \in A$, $b \in B$. La loi $(A, B) \to AB$ est associative et commutative.

1) Montrer que si $\operatorname{rg}_{\mathbb{Z}} A = n$, alors $\mathcal{O} := (A : A)$ est un ordre [*montrer que $d\mathcal{O}_K \subset \mathcal{O}$ pour $d \in \mathbb{Z}$ assez grand*].

2) Soit $\mathcal{O}$ un ordre. Un sous $\mathcal{O}$-module de type fini de K est appelé *idéal fractionnaire* de $\mathcal{O}$. Montrer que si J est un idéal fractionnaire de K, il existe un entier $d > 0$ tel que dJ soit un idéal de $\mathcal{O}$.

3) Un idéal I d'un ordre $\mathcal{O}$ est dit *inversible* s'il existe un idéal fractionnaire J tel que $IJ = \mathcal{O}$. Montrer que si $I \subset \mathcal{O}$ est un idéal inversible d'inverse J, alors $(A : I) = AJ$ pour tout sous-$\mathbb{Z}$-module A de K. [*Ce qui explique notre terminologie :* $(A : I) = AI^{-1}$.]

Note : Un ordre non maximal n'est pas de Dedekind. En particulier il existe des idéaux non inversibles ; dans $\mathbb{Z}[\sqrt{5}]$, par exemple, l'idéal $(2, 1+\sqrt{5})$ est maximal, mais non inversible [*calcul explicite assez long en partant d'une $\mathbb{Z}$-base d'un inverse*]. On démontre que les idéaux de $\mathcal{O}$ qui sont premiers à l'indice $[\mathcal{O}_K : \mathcal{O}]$ sont inversibles, ainsi que tous les idéaux principaux. Si $\mathcal{O} = \mathcal{O}_K$, tous les idéaux non nuls sont inversibles.

[1] De *ordo,-inis* : rangée, file. Cf. les trois Ordres de l'Ancien Régime.

III (Round 2)

Soit p un nombre premier et $\mathcal{O}$ un ordre de K. On note $\overline{I_p}$ l'ensemble des nilpotents de $\mathcal{O}/p\mathcal{O}$, et $I_p := \left\{x \in \mathcal{O}, \overline{x} \in \overline{I_p}\right\}$, où $\overline{x}$ est la projection canonique. On posera $\mathcal{O}' := (I_p : I_p)$. On désire montrer que $\mathcal{O} = \mathcal{O}'$ ssi $\mathcal{O}$ est p-maximal.

1) Si $q \geqslant n$ est une puissance de p, montrer que $\overline{I_p}$ est le noyau de l'endomorphisme $x \mapsto x^q$ de $\mathcal{O}/p\mathcal{O}$, qui est un $\mathbb{F}_p$-espace vectoriel de dimension n. [*Il est donc facile de calculer I_p à partir d'une $\mathbb{Z}$-base de $\mathcal{O}$.*]

2) Montrer que I_p est un $\mathbb{Z}$-module de rang n, puis que $\exists t \geqslant 0, I_p^t \subset p\mathcal{O}$.

3) Montrer que $\mathcal{O}'$ est un ordre, que I_p est un idéal de $\mathcal{O}$, puis que $p\mathcal{O}' \subset \mathcal{O} \subset \mathcal{O}'$.

4) Montrer que l'indice $[\mathcal{O}' : \mathcal{O}]$ divise p^n. En déduire que $\mathcal{O}' = \mathcal{O}$ si $\mathcal{O}$ est p-maximal.

5) Soit $R = \left\{x \in \mathcal{O}_K : \exists k, p^k x \in \mathcal{O}\right\}$, montrer que R est le plus petit ordre p-maximal contenant $\mathcal{O}$. Montrer qu'il existe $r \geqslant 0$ tel que $RI_p^r \subset \mathcal{O}$.

6) On suppose maintenant que $\mathcal{O} = \mathcal{O}'$. Supposons par l'absurde qu'il existe $m \geqslant 0$ tel que $RI_p^m \not\subset \mathcal{O}$ et choisissons $m < r$ maximal, puis $\alpha \in RI_p^m \setminus \mathcal{O}$. Montrer que $\alpha I_p \subset \mathcal{O}$, puis $\alpha I_p \subset I_p$ [*montrer que $(\alpha x)^{t+1} \in p\mathcal{O}$ si $x \in I_p$*]. Conclure.

7) Décrire un algorithme permettant de calculer $\mathcal{O}_K$ à partir d'un élément primitif α entier. [*Considérer les premiers p dont le carré divise le discriminant de $\mathbb{Z}[\alpha]$.*] On admettra que, si A, B, C sont des $\mathbb{Z}$-modules libres de rang fini, $\varphi : A \to B$ un morphisme, $C \subset B$, il est facile d'extraire une $\mathbb{Z}$-base d'une partie génératrice finie de A, ainsi que de calculer une base de l'image inverse $\varphi^{-1}(C) = \{a \in A, \varphi(a) \in C\}$. [*Généralisations du pivot de Gauss fondée sur l'algorithme d'Euclide étendu*].

Note : On démontre que I_p est le produit des idéaux maximaux de $\mathcal{O}$ contenant p. L'idée du test $\mathcal{O} = \mathcal{O}'$ est de vérifier si ces idéaux sont inversibles (ce qui est équivalent à ce que leur produit I_p le soit). Dans ce cas, la note précédente implique que p ne divise pas l'indice $[\mathcal{O}_K : \mathcal{O}]$.

IV (Dedekind)

On s'intéresse maintenant au cas particulier $\mathcal{O} = \mathbb{Z}[\alpha] = \mathbb{Z}[X]/(T)$, dont on représentera les éléments par des relèvements dans $\mathbb{Z}[X]$. On désire simplement savoir si $\mathcal{O}$ est p-maximal.

1) Montrer que l'idéal engendré par p et $f(\alpha)$ est inclus dans I_p.

2) Montrer que $\overline{I_p}$ est l'idéal de $\mathbb{F}_p[X]/(T)$ engendré par $\overline{f}$. En déduire $I_p = (p, f(\alpha))$.

3) Montrer qu'un élément de $\mathcal{O}'$ s'écrit $x = \beta/p$, où $\beta \in I_p$. On représente β par le polynôme $B \in \mathbb{Z}[X]$, i.e. $\beta = B(\alpha)$.

a) Montrer que $xp \in I_p$ ssi $\overline{f} \mid \overline{B}$.

★ b) Montrer que $xf(\alpha) \in I_p$ ssi $\overline{gk} \mid \overline{B}$, où $\overline{k} := \overline{f}/(\overline{h}, \overline{f})$.[*Écrire $Bf = p^2A_1 + pfA_2 + TA_3$, $A_i \in \mathbb{Z}[X]$.*]

★ **4)** Montrer que $\mathrm{ppcm}(\overline{f}, \overline{gk}) = \overline{T}/\delta$. Si $U \in \mathbb{Z}[X]$ est un relèvement de $\overline{T}/\delta$, en déduire que $\mathcal{O}' = \mathcal{O} + \frac{U(\alpha)}{p}\mathcal{O}$, puis que $[\mathcal{O}' : \mathcal{O}] = p^{\deg \delta}$. Démontrer le Théorème 1.

5) Appliquer le théorème de Dedekind à un polynôme T d'Eisenstein.

★★ **6)** Soit $\ell \neq \pm 1$ un entier sans facteur carrés. Montrer que $K = \mathbb{Q}(\ell^{1/3})$ est un corps de nombres de degré 3 et calculer $\mathcal{O}_K$. [$\mathcal{O} := \mathbb{Z}[\ell^{1/3}] = \mathcal{O}_K$ *ssi* $\ell \not\equiv \pm 1 \pmod 9$. *Calculer $\mathcal{O}'$ sinon.*]