UPS – Centre d'Orsay
Mathématiques

Arithmétique – Maîtrise
Année 2003–2004

DEVOIR n° 2 (**Correction**)

I (Exemples)

1) Soit $\mathcal{O}$ un ordre de $\mathbb{Q}$. Si $\alpha \in \mathbb{Q} \setminus \mathbb{Z}$, $\mathbb{Z}[\alpha]$ n'est pas de type fini comme $\mathbb{Z}$-module (s'il l'était, il y aurait un dénominateur commun à ses éléments). Donc $\alpha \notin \mathcal{O}$ (sinon $\mathbb{Z}[\alpha] \subset \mathcal{O}$ et $\mathcal{O}$ n'est pas de type fini). Donc $\mathcal{O} \subset \mathbb{Z}$. $\mathcal{O}$ étant un sous-anneau de $\mathbb{Q}$, il contient 1, donc $\mathbb{Z}$. Finalement, $\mathcal{O} = \mathbb{Z}$.

2) $\mathbb{Z}[\alpha]$ est un $\mathbb{Z}$-module libre de base $(1, \alpha, \ldots, \alpha^{n-1})$: c'est une partie génératrice car si $P \in \mathbb{Z}[X]$, le reste de la division euclidienne de P par le polynôme minimal T de α est à coefficient dans $\mathbb{Z}$ (T est unitaire car α est entier) ; elle est libre sur $\mathbb{Z}$ car libre sur $\mathbb{Q}$. C'est un sous-anneau de K par définition.

Si $\alpha \notin \mathcal{O}_K$, $\mathbb{Z}[\alpha]$ n'est pas de type fini. Ce n'est donc pas un ordre.

3) Si $\alpha \in \mathcal{O}$, alors $\mathbb{Z}[\alpha] \subset \mathcal{O}$, donc $\alpha \in \mathcal{O}_K$ sinon $\mathcal{O}$ n'est pas de type fini ($\mathbb{Z}$ étant principal, un sous-module d'un module de type fini est de type fini).

II (Division)

1) $\mathcal{O}$ est un sous-anneau de K : il contient 1 et, par exemple, $\alpha A \subset A$ et $\beta A \subset A$ implique $\alpha\beta A \subset \alpha A \subset A$; la stabilité par addition se montre de même.

Tout $\alpha \in \mathcal{O}$ est entier puisqu'il existe un $\mathbb{Z}$-module de type fini $A \neq (0)$ tel que $\alpha A \subset A$. [*Rappelons l'argument : la multiplication par α dans A est un endomorphisme de $\mathbb{Z}$-module m_α, dont le polynôme caractéristique P est unitaire à coefficient entiers. Par Cayley-Hamilton, $P(m_\alpha) = 0$ comme endomorphisme. On en déduit $P(\alpha) = 0$ en appliquant $P(m_\alpha)$ à un élément non nul de A. Donc α est entier.*]

Donc $\mathcal{O} \subset \mathcal{O}_K$ est de rang $\leqslant n$. Considérons les produits de générateurs de $\mathcal{O}_K$ et A (en nombre fini) ; A étant de rang $\dim_{\mathbb{Q}} K$, on peut les exprimer comme combinaisons linéaires rationnelles d'une base de A. Si d est un dénominateur commun pour tous ces coefficients, on a $(d\mathcal{O}_K)A \subset A$. Donc $\mathcal{O} \supset d\mathcal{O}_K$ contient un module de rang n et il est de rang exactement n.

2) Comme ci-dessus, $\mathcal{O}$ étant de rang n et J de type fini sur $\mathcal{O}$ donc sur $\mathbb{Z}$, il existe $d > 0$ tel que $dJ \subset \mathcal{O}$. Comme dJ est un sous $\mathcal{O}$-module de $\mathcal{O}$, c'est un idéal.. [*Si $\mathcal{O}$ n'est pas principal, J n'a aucune raison d'être un $\mathcal{O}$-module libre. C'est bien un $\mathbb{Z}$-module libre par contre.*]

3) Si $\alpha \in (A : I)$, alors $\alpha I \subset A$ soit $\alpha\mathcal{O} \subset AJ$ et donc $\alpha \in AJ$ (car $1 \in \mathcal{O}$). Réciproquement, si $\alpha\mathcal{O} \subset AJ$, alors $\alpha I \subset AJI = A$ et $\alpha \in (A : I)$.

III (Round 2)

1) $\mathcal{O}/p\mathcal{O}$ est un $\mathbb{F}_p$-espace vectoriel de dimension n (la projection canonique d'une $\mathbb{Z}$-base à n éléments est génératrice, elle est libre puisqu'une relation se relève dans $\mathcal{O}$), c'est aussi une $\mathbb{F}_p$-algèbre. Comme q est une puissance de p et $\mathcal{O}/p\mathcal{O}$ un anneau de caractéristique p, $x \mapsto x^q$ est une application linéaire. Un nilpotent d'un espace vectoriel de dimension n est d'indice au plus n donc si $x \in \mathcal{O}/p\mathcal{O}$ est nilpotent, la multiplication par x est un endomorphisme nilpotent tel que $m_x^n = 0$, soit $x^n = 0$ en appliquant m_x^n à $1 \in \mathcal{O}/p\mathcal{O}$. Comme $q \geqslant n$, on a aussi $x^q = 0$. Réciproquement, un x vérifiant $x^q = 0$ est évidemment nilpotent.

2) Si $x, y \in I_p$, nilpotents d'indice inférieur à n dans $\mathcal{O}/p\mathcal{O}$, λx est aussi nilpotent pour $\lambda \in \mathbb{Z}$, ainsi que $x + y$ car ils commutent : le développement de $(x+y)^{2n}$ ne fait intervenir que des puissances supérieures à n. Donc I_p est un $\mathbb{Z}$-module, de rang au plus n puisqu'il est inclus dans $\mathcal{O}$. De plus $p\mathcal{O} \subset I_p$ (0 est nilpotent !), donc I_p est de rang au moins n.

Tout élément de I_p est donc combinaison linéaire à coefficients entiers d'une base à n éléments $(x_1, \ldots, x_n)$. Le développement de $(\sum \lambda_i x_i)^{n^2}$ fait intervenir des monômes en les (x_i) contenant tous une puissance n-ème. Comme ce sont des nilpotents d'indice inférieur à n dans $\mathcal{O}/p\mathcal{O}$, ce développement est nul dans $\mathcal{O}/p\mathcal{O}$. On peut donc prendre $t = n^2$ (et même $t = n$ une fois que l'on sait que $\sum \lambda_i x_i$ est nilpotent).

3) D'après (II.2), $\mathcal{O}'$ est un ordre. Si $x \in I_p$, $y \in \mathcal{O}$, la projection de xy est nilpotente dans $\mathcal{O}/p\mathcal{O}$, donc $xy \in I_p$, et I_p est bien un idéal (on sait déjà que c'est un $\mathbb{Z}$-module). Donc $\mathcal{O}I_p \subset I_p$ et $\mathcal{O} \subset (I_p : I_p) = \mathcal{O}'$. Soit $x \in \mathcal{O}'$, comme $p \in I_p$ et $xI_p \subset I_p$, on a $xp \in I_p \subset \mathcal{O}$. Soit $p\mathcal{O}' \subset \mathcal{O}$.

4) Comme $p\mathcal{O}' \subset \mathcal{O} \subset \mathcal{O}'$, il y a une surjection canonique de $\mathcal{O}'/p\mathcal{O}'$ sur $\mathcal{O}'/\mathcal{O}$. C'est un morphisme de groupe additifs, et on en déduit que $\#(\mathcal{O}'/\mathcal{O}) \mid \#(\mathcal{O}'/p\mathcal{O}') = p^n$.

Comme $\mathcal{O}'$ est un ordre, on a $\mathcal{O}' \subset \mathcal{O}_K$, soit $\mathcal{O}'/\mathcal{O} \subset \mathcal{O}_K/\mathcal{O}$. C'est l'inclusion d'un sous-groupe donc $[\mathcal{O}' : \mathcal{O}] \mid [\mathcal{O}_K : \mathcal{O}]$. Si ce dernier est premier à p, on a $[\mathcal{O}' : \mathcal{O}] = 1$, soit $\mathcal{O} = \mathcal{O}'$.

5) R, étant un $\mathbb{Z}$-module coincé entre $\mathcal{O}$ et $\mathcal{O}_K$ qui sont de rang n, est de rang n. Comme il est stable par multiplication et contient $1 \in \mathcal{O}$, c'est un sous-anneau de K, donc un ordre. S'il n'était pas p-maximal, il existerait $x \in \mathcal{O}_K \setminus R$ tel que $px \in R$ (il suffit de prendre un relèvement d'un élément d'ordre p du groupe $\mathcal{O}_K/R$). Absurde.

Soit donc $R' \supset \mathcal{O}$ un ordre p-maximal et $x \in R$, tel que $p^k x \in \mathcal{O} \subset R'$. On a donc $p^k x = 0$ dans $\mathcal{O}_K/R'$ et l'ordre de la projection de x dans $\mathcal{O}_K/R'$, qui est un groupe d'ordre premier à p, divise p^k. Donc $x \in R'$, soit $R \subset R'$.

R est de type fini, donc il existe s tel que $p^s R \subset \mathcal{O}$ (on prend le max des k associés aux éléments d'une base de R). D'autre part $I_p^t \subset p\mathcal{O}$, donc on peut prendre $r = st$.

6) $\alpha I_p \subset R I_p^{m+1} \subset \mathcal{O}$ par maximalité de m. Soit $x \in I_p$. On a $R I_p^{m+t+1} \subset I_p^t \mathcal{O} \subset p\mathcal{O}$, donc

$$(\alpha x)^{t+1} \in (R I_p^{m+1})^{t+1} = R^{t+1} I_p^{m+1+t+mt} \subset R I_p^{m+t+1} \subset p\mathcal{O}.$$

En effet, I_p étant un idéal de $\mathcal{O}$, on a $I_p^a \subset I_p^b$ pour tout $a \geqslant b$; R est un anneau, on a $R^k = R$ pour tout $k \geqslant 1$.

Donc la projection de αx est un nilpotent de $\mathcal{O}/p\mathcal{O}$ et $\alpha I_p \subset I_p$. Soit $\alpha \in (I_p : I_p) = \mathcal{O}'$. Contradiction.

7) On sait que $\mathbb{Z}[\alpha]$ est p-maximal pour tous les premiers p dont le carré ne divise pas son discriminant. Les autres sont en nombre fini. Il suffit donc d'initialiser $\mathcal{O} = \mathbb{Z}[\alpha]$, puis pour chaque mauvais premier p, calculer le I_p associé à $\mathcal{O}$, puis remplacer $\mathcal{O}$ par $\mathcal{O}'$ tant que $\mathcal{O} \subsetneq \mathcal{O}'$. Dès qu'on a égalité, $\mathcal{O}$ est maintenant p-maximal, et on passe au mauvais premier suivant. Quand $\mathcal{O}$ est p-maximal pour tout p, on a $\mathcal{O}_K = \mathcal{O}$.

Revenons sur quelques détails : chacun des $\mathcal{O}$ successifs est décrit par une $\mathbb{Z}$-base, la première étant $(1, \alpha, \ldots, \alpha^{n-1})$. À partir d'une $\mathbb{Z}$-base de $\mathcal{O}$, on calcule une $\mathbb{F}_p$ base de $\overline{I_p}$ à l'aide de (III.1). En concaténant une base de $p\mathcal{O}$ (une base de $\mathcal{O}$ dont on multiplie les éléments par p), et un relèvement arbitraire à I_p de la base de $\overline{I_p}$, on obtient une partie génératrices de I_p à $2n$ éléments, dont on extrait une $\mathbb{Z}$-base. Si $(\alpha_i)_{i\leqslant n}$ est une $\mathbb{Z}$-base de I_p, considérons le morphisme de $\mathbb{Z}$-modules $m : \frac{1}{p}\mathcal{O} \to (\frac{1}{p}\mathcal{O})^n$ donné par $m(x) = (x\alpha_1, \ldots, x\alpha_n)$. $\mathcal{O}'$ est l'image inverse $m^{-1}(I_p \times \cdots \times I_p)$.

IV (Dedekind)

1) On a déjà vu que I_p est un idéal et $p \in I_p$. La projection canonique de $f(\alpha)$ dans $\mathcal{O}/p\mathcal{O} = \mathbb{F}_p[X]/(T)$ est $\overline{f}$. Comme $\overline{f}^n = 0$, $f(\alpha) \in I_p$.

2) Si $x^n = 0$ dans $\mathbb{F}_p[X]/(T)$, alors $T \mid x^n$ dans $\mathbb{F}_p[X]$, donc les facteurs irréductibles de T divisent x et $\overline{f} \mid x$. Comme la question précédente donne l'inclusion réciproque, $\overline{I_p}$ est l'idéal engendré par $\overline{f}$. Donc $I_p \subset (p, f(\alpha))$ et l'égalité suit.

3) On a $x \in \mathcal{O}'$ ssi $px \in I_p$ et $pf(\alpha) \in I_p$. La première condition donne $x = \beta/p$, $\beta \in I_p$.

a) $\beta \in I_p$ ssi $\overline{B} \in \overline{I_p}$, soit $\overline{f} \mid \overline{B}$ d'après la question précédente.

b) Dans cette question, la notation A_i désigne un polynôme de $\mathbb{Z}[X]$ pour $i = 1, 2, \ldots$. Comme pI_p est engendré par p^2 et $pf(\alpha)$, $xf(\alpha) \in I_p$ ssi il existe A_1, A_2, A_3 tels que $fB = p^2A_1 + pfA_2 + TA_3$, en utilisant l'identification $\mathbb{Z}[\alpha] = \mathbb{Z}[X]/(T)$. En réduisant modulo p, on obtient $\overline{B} = \overline{gA_3}$, soit $B = gA_3 + pA_4$ et la condition devient

$$fA_4 = pA_1 + fA_2 + hA_3, \quad \text{soit} \quad fA_5 = pA_1 + hA_3.$$

En réduisant modulo p, cette identité est possible ssi $\overline{fA_5} = \overline{hA_3}$ soit $\overline{k} = \overline{f}/(\overline{f}, \overline{h}) \mid \overline{A_3}$. Ou encore $A_3 = kA_6 + pA_7$, soit $B = gkA_6 + pA_8$. Finalement ceci est possible ssi $\overline{gk} \mid \overline{B}$.

4) Dans $\mathbb{F}_p[X]$, on a (on supprime les $\bar{}$ pour alléger la notation)

$$\operatorname{ppcm}(f, gk) = \frac{fgk}{\operatorname{pgcd}(f, gk)} = T\frac{k}{k(f/k, g)} = T/\delta,$$

en écrivant $(f/k, g) = ((f, h), g) = \delta$. Finalement, $\beta/p \in \mathcal{O}'$ ssi T/δ divise $\overline{B}$, soit $B/p = UA_1/p + A_2$ pour deux polynômes $A_i \in \mathbb{Z}[X]$ arbitraires. Donc $\mathcal{O}' = \mathcal{O} + \frac{U(\alpha)}{p}\mathcal{O}$.

Si A_1 parcourt les représentants dans $\mathbb{Z}[X]$ des polynomes de $\mathbb{F}_p[X]$ de degré strictement inférieur à $\deg T - \deg U = \deg \delta$, les $\frac{1}{p}U(\alpha)A_1(\alpha)$ forment un système de représentants de $\mathcal{O}'/\mathcal{O}$, soit $[\mathcal{O}' : \mathcal{O}] = p^{\deg \delta}$. Finalement, $\mathcal{O}' = \mathcal{O}$ ssi $\deg \delta = 0$.

5) On choisit $f = X$, $g = X^{n-1}$, $h = (T - X^n)/p$ dont le coefficient constant n'est pas divisible par p. On en déduit que $(\overline{f}, \overline{h}) = 1$. A fortiori, $\delta = 1$. Donc $\mathbb{Z}[\alpha]$ est p-maximal.

6) Notons que $T = X^3 - \ell$ est d'Eisenstein en p pour tout $p \mid \ell$. Comme il existe un tel p ($\ell \neq \pm 1$), T est donc irréductible sur $\mathbb{Q}$ et K est un corps de nombres de degré 3. Soit

$\alpha = \ell^{1/3}$. Les plongements de K sont les $\alpha \mapsto j^k\alpha$, $k = 0, 1, 2$, pour $j = \exp(2i\pi/3)$. On en déduit que

$$\operatorname{disc} \mathbb{Z}[\alpha] = \begin{vmatrix} 1 & \alpha & \alpha^2 \\ 1 & j\alpha & j^2\alpha^2 \\ 1 & j^2\alpha & j\alpha^2 \end{vmatrix}^2 = (\alpha^3(1-j)^3)^2 = -27\ell^2$$

$\mathcal{O} = \mathbb{Z}[\alpha]$ est donc p-maximal pour tout $p \neq 3$, $p \nmid \ell$, puisque $p^2 \nmid \operatorname{disc} \mathcal{O}$ sinon. Comme $X^3 - \ell$ est d'Eisenstein en $p \mid \ell$, $\mathcal{O}$ est aussi p-maximal pour $p \mid \ell$, y compris si $p = 3 \mid \ell$.

Reste à tester la 3-maximalité si $3 \nmid \ell$. On applique ce qui précède pour calculer $\mathcal{O}'$. On peut prendre $f = X - \ell$, $g = (X - \ell)^2$, soit $h = \ell X^2 - \ell^2 X + \frac{1}{3}(\ell^3 - \ell)$. Donc $\delta \neq 1$ ssi $X = \ell$ est racine de h modulo 3, ssi $\ell^3 - \ell \equiv 0 \pmod 9$, ou encore $\ell \equiv \pm 1 \pmod 9$ puisque $3 \nmid \ell$. Donc pour tout $\ell \not\equiv \pm 1 \pmod 9$, $\mathcal{O}$ est aussi 3-maximal et $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

Sinon, on peut prendre $U = X^2 + \ell X + \ell^2$, et poser $v = U(\alpha)/3$. On obtient $\mathcal{O}' = \mathbb{Z}[\alpha] + v\mathbb{Z}[\alpha]$. Comme $\operatorname{disc} \mathcal{O}' = \operatorname{disc} \mathcal{O}/[\mathcal{O}' : \mathcal{O}]^2 = -3\ell^2$, $\mathcal{O}'$ est 3-maximal (car $3^2 \nmid \operatorname{disc} \mathcal{O}'$). Donc $\mathcal{O}_K = \mathcal{O}'$.

Si on désire donner une $\mathbb{Z}$-base de $\mathcal{O}'$, il faut travailler un peu plus : les $\mathbb{Z}$-générateurs sont $(1, \alpha, \alpha^2, v, \alpha v, \alpha^2 v)$, donnés dans la $\mathbb{Q}$-base $(1/3, \alpha/3, \alpha^2/3)$ par la matrice

$$\begin{pmatrix} 3 & 0 & 0 & \ell^2 & \ell & \ell^2 \\ 0 & 3 & 0 & \ell & \ell^2 & \ell \\ 0 & 0 & 3 & 1 & \ell & \ell^2 \end{pmatrix}$$

Un pivot évident (sans divisions !), dit que le $\mathbb{Z}$-module engendré par ces colonnes est le même que celui donné par

$$\begin{pmatrix} 3 & 0 & \ell^2 \\ 0 & 3 & \ell \\ 0 & 0 & 1 \end{pmatrix}$$

Par exemple si C_i désigne la i-ème colonne, on a $C_5 = \ell C_4 + \frac{1}{3}(\ell - \ell^3)C_1$, où les coefficients sont entiers car $\ell^3 \equiv \ell \pmod 3$. On élimine de même C_3 et C_6. En résumé

$$\mathcal{O}_K = \begin{cases} \langle 1, \alpha, \frac{1}{3}(\alpha^2 + \ell\alpha + \ell^2) \rangle_{\mathbb{Z}} & \text{si } \ell \equiv \pm 1 \pmod 9 \\ \langle 1, \alpha, \alpha^2 \rangle_{\mathbb{Z}} & \text{sinon} \end{cases}$$