Université Paris Sud **Année 2008-2009**

M1 **Arithmétique**

Corrigé de quelques exercices

Correction du TD V, exercice C

Une racine primitive $p^{\text{ième}}$ de l'unité ζ étant fixée, on note

$$P \ := \ \frac{X^p-1}{X-1} \ = \ \sum_{i=0}^{p-1} X^i \ \in \ \mathbb{Z}[X]$$

son polynôme minimal. Il est commode de remarquer que le polynôme minimal de $\zeta-1$ est

$$P_1 \ = \ \frac{(X+1)^p-1}{X} \ = \ \sum_{i=1}^{p} C_p^i X^{i-1} \ .$$

On note

$$K \ := \ \mathbb{Q}[\zeta] \ = \ \mathbb{Q}[X]/P \ = \ \mathbb{Q}[X]/P_1 \ .$$

le $p^{\text{ième}}$ corps cyclotomique et $\mathcal{O}_K$ son anneau d'entiers.

1) Le polynôme P_1 est un polynôme d'Eisenstein en p (cf. II.3.2.6.) Il en résulte grâce au théorème II.3.2.8, que l'extension

$$(K \otimes_{\mathbb{Q}} \mathbb{Q}_p)/\mathbb{Q}_p \ = \ (\mathbb{Q}_p[X]/P/\mathbb{Q}_p \ = \ (\mathbb{Q}_p[X]/P_1)/\mathbb{Q}_p$$

est totalement ramifiée et que l'image de $\zeta-1$ dans $K \otimes_{\mathbb{Q}} \mathbb{Q}_p$ est une uniformisante. Il résulte ensuite du corollaire II.3.2.9 que l'anneau des entiers de $K \otimes_{\mathbb{Q}} \mathbb{Q}_p$ est

$$\mathbb{Z}_p[\zeta-1] \ \cong \ \mathbb{Z}_p[\zeta] \ \cong \ \mathbb{Z}[\zeta] \otimes_{\mathbb{Z}} \mathbb{Z}_p$$

ce qui signifie exactement que $\mathbb{Z}[\zeta]$ est p-clos (cf. III.3.1.2.)

Pour tout nombre premier $\ell \neq p$, le polynôme $R \ := \ X^p-1$ vérifie

$$-R + \frac{A}{P} X R' \ = \ 1 \ \in \ \mathbb{F}_\ell[X]$$

c'est-à-dire qu'il est séparable dans $\mathbb{F}_\ell[X]$. Il en va donc de même de P qui est un facteur de R si bien que $\mathbb{Z}[\zeta]$ est ℓ-clos en vertu du théorème III.3.1.8.

On en déduit donc que, pour tout nombre premier ℓ (p y compris,)

$$\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \;=\; \mathbb{Z}[\zeta] \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$$

ce qui assure, en appliquant les résultats des paragraphes III.3.0 et III.3.1, que

$$\mathcal{O}_K \;=\; \mathbb{Z}[\zeta]\;.$$

On pourrait alors facilement en déduire des résultats concernant la ramification dont nous n'aurons pas besoin dans la suite de l'exercice : En effet, on a alors

$$\begin{aligned}
\mathfrak{d}_{\mathcal{O}_K/\mathbb{Z}} &= \mathfrak{d}^{\mathbb{Z}}_{K/\mathbb{Q}}(\mathbb{Z}[\zeta]) \\
&= \delta_{K/\mathbb{Q}}(P) \\
&= \mathfrak{d}^{\mathbb{Z}}_{K/\mathbb{Q}}(\mathbb{Z}[\zeta-1]) \\
&= \delta_{K/\mathbb{Q}}(P_1) \\
&= \mathrm{N}_{K/K}(P_1'(\zeta-1)) \\
&= \mathrm{N}_{K/\mathbb{Q}}(\frac{(\zeta-1)p\zeta^{p-1}\zeta^p}{\zeta^2}) \\
&= \frac{\mathrm{N}_{K/\mathbb{Q}}(-p\zeta^{p-1})}{\mathrm{N}_{K/\mathbb{Q}}(\zeta)^2} \\
&= \epsilon\frac{p^p}{p^2} \\
&= \epsilon p^{p-2}
\end{aligned}$$

où ϵ vaut ± 1 qu'on pourrait calculer avec plus de soin. On savait déjà que le nombre premier p était ramifié dans $\mathcal{O}_K$, mais il résulte du calcul ci-dessus et du théorème III.3.2.30.iv que c'est le seul. Néanmoins, dans ce cas particulier, il était encore plus économique de déduire ce dernier résultat du fait que P est séparable dans

$$\mathbb{F}_\ell \;\forall\; \ell \neq p$$

et du théorème III.3.1.8.

2 ***Racines de l'unité*** **a)** On remarque d'abord que, pour tout $0 \leq k \leq p-1$, ζ^k, et $-\zeta^k$ sont bien des racines $2p^{\text{ième}}$ de l'unité appartenant à K.

Réciproquement, s'il existe $\zeta_q \in K$ racine primitive $q^{\text{ième}}$ de l'unité avec $p \nmid q$, alors il existe $(u,v) \in \mathbb{Z}^2$ tel que $up + vq = 1$. Si l'on note ζ_{pq} une racine primitive $pq^{\text{ième}}$ de l'unité,

$$\zeta_{pq} \;=\; \zeta_{pq}^{up+vq} \;\in\; K\;.$$

Il s'ensuit que

$$\mathbb{Q}[\zeta_{pq}] \subset K \;=\; \mathbb{Q}[\zeta]$$

d'où

$$[Rat[\zeta_{pq}] : \mathbb{Q}] \mid [K : \mathbb{Q}]$$

c'est-à-dire $\phi(pq)|\phi(p)$ c'est-à-dire $\phi(q)\phi(p)|\phi(p)$ c'est-à-dire $\phi(q) = 1$ ce qui entraîne que $q = 2$.

b) Soit $x \in \mathcal{O}_K$. Si on note

$$\sigma_i : K \to \mathbb{C}, 1 \leq i \leq p-1,$$

les $p-1$ plongements deux à deux distincts de K dans $\mathbb{C}$, le polynôme

$$P_x := \prod_{i=1}^{p-1} X - \sigma_i(x) \in \mathbb{Z}[X],$$

annule x. Si l'on suppose que, pour tout $1 \leq i \leq p-1$, $|\sigma_i(x)| = 1$, les coefficients de P_x sont bornés indépendamments de x, si bien que les polynômes P_x sont en nombre fini ainsi que leurs racines.

Il est clair que M est un sous-groupe de K^*, si bien que tout $x \in M$ est d'ordre fini ou encore est une racine de l'unité c'est-à-dire que $M \subset \mu(K)$. L'inclusion réciproque est immédiate.

3 .a) Pour tout $\epsilon \in \mathcal{O}_K^\times$, et tout $1 \leq i \leq p-1$, il est fastidieux, mais sans difficulté de montrer que $\sigma_i(\overline{\epsilon}) = \overline{\sigma_i(\epsilon)}$. Il en résulte que

$$\frac{\epsilon}{\overline{\epsilon}} \in M$$

c'est-à-dire d'après la question précédente, que

$$\frac{\epsilon}{\overline{\epsilon}} \in \mu(K)$$

ce qui prouve le résultat.

b) On sait, puisque l'extension $(\mathbb{Q}_p[X]/P)/\mathbb{Q}_p$ est totalement ramifiée et grâce au théorème III.2.2.7, qu'il n'y a qu'un seul idéal maximal $\mathfrak{q}$ de $\mathcal{O}_K$ au-dessus du nombre premier p et que

$$p\mathcal{O}_K = \mathfrak{q}^{p-1} .$$

De plus, $\mathbb{Z}[\zeta]$ étant p-clos, on peut appliquer le résultat de l'exercice TD V, exercice B pour déterminer $\mathfrak{q}$. Puisque $P = (X-1)^p \in \mathbb{F}_p[X]$,

$$\mathfrak{q} = (\zeta - 1)\mathcal{O}_K + p\mathcal{O}_K .$$

Or $P_1(\zeta - 1) = 0$, ce qui permet d'écrire

$$p = -\sum_{i=2}^{p} C_p^i (\zeta - 1)^{i-1}$$

ce qui entraîne que

$$\mathfrak{q} = (\zeta - 1)\mathcal{O}_K .$$

Il résulte toujours du théorème III.2.2.7, que

$$[\mathcal{O}_K/\mathfrak{q} : \mathbb{F}_p] = f_{\mathfrak{q}/p} = f_{(\mathbb{Q}_p[X]/P)/\mathbb{Q}_p} = 1 .$$

Il s'ensuit que

$$\mathcal{O}_K/\mathfrak{q} \;\cong\; \mathbb{F}_p\,.$$

Or la restriction à K de la conjugaison complexe étant un élément du groupe de Galois $\mathrm{Gal}_{K/\mathbb{Q}}$ elle induit un élément $\gamma \in \mathrm{Gal}_{\mathcal{O}_K/\mathfrak{q}/\mathbb{F}_p}$ caractérisé par le fait que, pour tout $x \in \mathcal{O}_K$,

$$\gamma(x[\mathfrak{q}]) \;\equiv\; \overline{x}[\mathfrak{q}]\,.$$

Or $\mathrm{Gal}_{\mathcal{O}_K/\mathfrak{q}/\mathbb{F}_p} \;=\; \{1\}$ c'est-à-dire que $\gamma \;=\; \mathrm{Id}$ ce qui entraîne que, pour tout $\epsilon \in \mathcal{O}_K^\times$,

$$\epsilon \;\equiv\; \overline{\epsilon}\,[\mathfrak{q}]\,.$$

c) Il découle des deux points précédents, que

$$\pm\zeta^b \;\equiv\; 1\,[\mathfrak{q}]$$

c'est-à-dire que

$$\pm 1 \;\equiv\; 1\,[\mathfrak{q}]$$

ce qui entraîne, puisque $p \neq 2, \pm 1 \;=\; 1$. Il s'ensuit que, pour tout $\epsilon \in \mathcal{O}_K^\times$, il existe $b \in \mathbb{Z}$, tel que

$$\epsilon \;=\; \zeta^b\overline{\epsilon}\,.$$

Il en résulte que

$$\epsilon^2 \;=\; \zeta^b|\epsilon|^2\,.$$

Or pour tous entiers b et c tels que $b \;\equiv\; c\,[p]$, $\zeta^b \;=\; \zeta^c$. Puisque p est impair, on peut donc supposer $b \;=\; 2a$ pair. On a alors $\epsilon \;=\; \zeta^{2a}\overline{\epsilon}$ entraîne

$$\zeta^a\overline{\epsilon} \;=\; \zeta^{-a}\epsilon \;=\; \overline{\zeta^a\overline{\epsilon}}$$

si bien que

$$\epsilon_1 \;:=\; \zeta^a\overline{\epsilon} \;\in\; \mathbb{R}\,\text{et}\,\epsilon \;=\; \zeta^a\epsilon_1\,.$$

4 .a) S'il existe $d \in \mathbb{N}$ tel que d divise deux des trois entiers x, y, z l'équation $x^P + y^P \;=\; z^p$ entraîne qu'il divise le troisième. On a alors encore $\frac{x}{d}^p + \frac{y}{d}^p \;=\; \frac{z}{d}^p$ si bien qu'on peut se ramener à l'étude des solutions où les entiers x, y, z sont deux à deux premiers entre eux.

Si $x \;\equiv\; y\,[p]$, dans $\mathbb{F}_p$ on a

$$\begin{array}{rrcl} & x^p + y^p & = & z^p \\ \Leftrightarrow & (x+y)^p & = & z^p \\ \Leftrightarrow & x+y & = & z \\ \Leftrightarrow & 2x & = & z \end{array}$$

si bien que $x \;\not\equiv\; z\,[p]$ et qu'on peut permuter y et z.

b) On a

$$\prod_{j=1}^{p-1}(1-\zeta^j) \;=\; \mathrm{N}_{K/\mathbb{Q}}(1-\zeta) \;=\; (-1)^{p-1}\mathrm{N}_{K/\mathbb{Q}}(\zeta-1) \;=\; \mathrm{N}_{K/\mathbb{Q}}(\zeta-1)$$

puisque $p-1$ est pair. Or le polynôme minimal de $\zeta - 1$ est P_1 (qui est de degré pair) et dont le terme constant vaut p. Il en résulte que

$$p \;=\; \prod_{j=1}^{p-1} 1-\zeta^j \;.$$

D'autre part notons

$$R \;:=\; X^p - 1 \;=\; (X-1)P \;\in\; \mathbb{Z}[X] \;.$$

On a alors

$$\begin{aligned}
\prod_{j=0}^{p-1} x+\zeta^j y \;&=\; (-y)^p \prod_{j=0}^{p-1} -\frac{x}{y} - \zeta^j \\
&=\; -y^p R(-\frac{x}{y}) \\
&=\; -y^p(-\frac{x^p}{y^p} - 1) \\
&=\; x^p + y^p \\
&=\; z^p \;.
\end{aligned}$$

c) Soient $i \not\equiv j\ [p]$. Si $\mathfrak{p} \in \mathrm{Spm}(\mathcal{O}_K)$ divise $((x+y\zeta^i),(x+y\zeta^j))$,

$$\mathfrak{p} \;\mid\; y(\zeta^i - \zeta^j) \text{ et } \mathfrak{p} \;\mid\; z^p \;.$$

Or $\zeta^i - \zeta^j \;=\; \zeta^i(1-\zeta^{j-i}) \;\mid\; p$ d'où $\mathfrak{p} \;\mid\; py$. Or $y \wedge z^p \;=\; 1$ et $p \wedge z^p \;=\; 1$ d'où $\mathfrak{p} \;\mid\; 1$ ce qui n'est pas possible.

d) L'identité

$$z^p \;=\; \prod_{j=0}^{p-1} x+\zeta^j y$$

se décompose de manière unique dans l'anneau de Dedekind $\mathcal{O}_K$ en

$$\prod_{\mathfrak{p}\in\mathrm{Spm}(\mathcal{O}_K)} \mathfrak{p}^{pv_\mathfrak{p}(z)} \;=\; \prod_{j=0}^{p-1} \Big(\prod_{\mathfrak{p}\in\mathrm{Spm}(\mathcal{O}_K)} \mathfrak{p}^{v_\mathfrak{p}(x+\zeta^j y)} \Big) \;.$$

Pour tout $i \not\equiv j\ [p]$, et tout $\mathfrak{p} \in \mathrm{Spm}(\mathcal{O}_K)$,

$$v_\mathfrak{p}(x+\zeta^i y) v_\mathfrak{p}(x+\zeta^j y) \;=\; 0$$

puisque $(x+\zeta^i y)$ et $(x+\zeta^j y)$ sont premiers entre eux. Il découle de l'unicité de la décomposition que, pour tout $\mathfrak{p} \in \mathrm{Spm}(\mathcal{O}_K)$, $p | v_\mathfrak{p}(x+\zeta y)$. Posons alors

$$\mathfrak{I} \;:=\; \prod_{\mathfrak{p}\in\mathrm{Spm}(\mathcal{O}_K)} \mathfrak{p}^{\frac{v_\mathfrak{p}(x+\zeta y)}{p}}$$

qui est bien un idéal de $\mathcal{O}_K$ et vérifie

$$\mathfrak{I}^p \ = \ (x+\zeta y)\ .$$

Or $(x+\zeta y)$ est un idéal principal de $\mathcal{O}_K$ c'est-à-dire que sa classe dans le groupe de Picard (cf. III.1.1.14,) est triviale. Or p ne divisant pas le cardinal du groupe de Picard, si $\mathfrak{I}^p$ est trivial dans le groupe de Picard c'est que $\mathfrak{I}$ est déjà trivial c'est-à-dire principal. Il existe donc $\alpha \in \mathcal{O}_K$ tel que $\mathfrak{I} \ = \ \alpha\mathcal{O}_K$. Puisque $\mathfrak{I}^p \ = \ (x+\zeta y)$ les générateurs de ces idéaux sont associés c'est-à-dire qu'il existe $\epsilon \in \mathcal{O}_K^\times$ tel que

$$(x+\zeta y) \ = \ \epsilon\alpha^p\ .$$

e) Pour tout $\alpha \in \mathcal{O}_K$, il existe $a_{i\ ,1\leq i\leq p-2} \in \mathbb{Z}$ tels que $\alpha \ = \ \sum_{i=0}^{p-2} a_i\zeta^i$. Il en résulte que

$$\begin{aligned}\alpha^p \ &= \ (\sum_{i=0}^{p-2} a_i\zeta^i)^p \\ &\equiv \ \sum_{i=0}^{p-2} a_i^p\zeta^{pi} \pmod{p}\end{aligned}$$

Or $\zeta^p \ = \ 1$ et par conséquent

$$\alpha^p \ \equiv \ \sum_{i=0}^{p-2} a_i^p \ [p]\ .$$

Remarquons qu'on peut même prendre $\beta \ = \ \sum_{i=0}^{p-2} a_i$ puisque

$$a_i^p \ \equiv \ a_i \ [p] \ \forall \ 0 \leq i \leq p-2\ .$$

f) Il faut tout d'abord remarquer que $\zeta^{-1} \ = \ \overline{\zeta}$ et que, par conséquent, comme x et y sont dans $\mathbb{Z}$, $x+y\zeta^{-1} \ = \ \overline{x+y\zeta}$. Or $x+y\zeta \ = \ \epsilon\alpha^p$ d'où $x+y\zeta^{-1} \ = \ \overline{\epsilon\alpha^p}$. Or il existe $k \in \mathbb{Z}$ tel que $\overline{\epsilon} \ = \ \zeta^k\epsilon$. Il en résulte que

$$x+y\zeta-(x+y\zeta^{-1})\zeta^{-k} \ = \ \epsilon(\alpha^p-\overline{\alpha}^p)\ .$$

Il est clair d'abord, que d'après la question précédente, $\alpha^p-\overline{\alpha}^p \ \equiv \ 0 \ [p]$ et ensuite, que seule la classe modulo p de k étant bien définie, on peut choisir $-k \in \mathbb{N}$.

g) Pour tout $a \in \mathbb{Z}$ (resp. $x \in \mathcal{O}_K$,) notons $1\otimes a$ (resp. $1\otimes x$) son image dans $\mathbb{F}_p \ = \ \mathbb{F}_p \otimes_{\mathbb{Z}} \mathbb{Z}$ (resp. $\mathcal{O}_K/p\mathcal{O}_K \ = \ \mathbb{F}_p \otimes_{\mathbb{Z}} \mathcal{O}_K$.) Puisque $\zeta^{i\ ,0\leq i\leq p-2}$ est une $\mathbb{Z}$-base de $\mathcal{O}_K$, $(1\otimes\zeta^i)_{\ ,0\leq i\leq p-2}$ est

une $\mathbb{F}_p$-base de $\mathcal{O}_K/p\mathcal{O}_K$. Pour tout $a_{i\ ,0\leq i\leq p-2}\in\mathbb{Z}$ on a alors

$$\begin{aligned} & \sum_{i=0}^{p-2} a_i\zeta^i &\equiv\ & 0[p] \\ \Leftrightarrow\ & \sum_{i=0}^{p-2}(1\otimes a_i)(1\otimes\zeta^i) &=\ & 0 \\ \Leftrightarrow\ & (1\otimes a_i) &=\ & 0\ \forall 0\leq i\leq p-2 \\ \Leftrightarrow\ & a_i &\equiv\ & 0[p]\ \forall 0\leq i\leq p-2\ . \end{aligned}$$

Pour $a_{i\ ,0\leq i\leq p-1}\in\mathbb{Z}$ si

$$(*)\ :\ \sum_{i=0}^{p-} a_i\zeta^i\ \equiv\ 0\ [p]$$

et il existe $0\leq i\leq p-1$ tel que $p|a_i$, on peut, quitte à multiplier l'identité $(*)$ par une puissance convenable de ζ, supposer que $a_{p-1}\ \equiv\ 0\ [p]$. On est alors ramené à appliquer le résultat précédent.

h) On a montré qu'il existe $k\in\mathbb{N}$ tel que

$$\begin{aligned} & x+\zeta y-(x+\zeta^{-1}y)\zeta^k &\equiv\ & 0 \pmod{p\mathcal{O}_K} \\ \Leftrightarrow\ & x+y\zeta-y\zeta^{k-1}-x\zeta^k &\equiv\ & 0 \pmod{p\mathcal{O}_K}\ . \end{aligned}$$

On applique la question précédente :

$$\{1,\zeta,\zeta^{k-1},\zeta^k\}$$

a 4 éléments et $p\geq 5$; comme les coefficients de l'équation obtenue sont non nuls mod p, ces éléments ne sont pas distincts. Il y a 3 possibilités : $\zeta^k\ =\ 1, \zeta^{k-1}\ =\ 1$ ou $\zeta\ =\ \zeta^{k-1}$ (car $\zeta\neq 1$, donc aussi $\zeta^{k-1}\neq\zeta^k$.) On rappelle que $(p)\ =\ \mathfrak{q}^{p-1}$, avec $\mathfrak{q}\ =\ (1-\zeta)$, et que $\mathfrak{q}\cap\mathbb{Z}\ =\ p\mathbb{Z}$.

- $\zeta^k\ =\ 1$: soit $y(\zeta-\zeta^{-1})\equiv 0\pmod{p}$ on en déduit $y\equiv 0\pmod{\mathfrak{q}^{p-2}}$ car $(\zeta-\zeta^{-1})\ =\ \mathfrak{q}$, puis $y\in\mathfrak{q}$ ($p>2$) et $p\mid y$. Absurde.
- $\zeta^{k-1}\ =\ \zeta$: soit $x(1-\zeta^2)\equiv 0\pmod{p}$ et $p\mid x$. Absurde.
- $\zeta^{k-1}\ =\ 1$: soit $(x-y)(1-\zeta)\equiv 0\pmod{p}$ et $p\mid x-y$. Absurde.

Remarque [16] **Les mêmes techniques (en plus ardu, il faut étudier les unités en détail) permettent d'écarter le cas $p\mid xyz$, toujours sous l'hypothèse que p est *régulier*. Il existe un critère élémentaire, mais dont la preuve est non élémentaire, pour savoir si p est régulier : on appelle nombres de Bernoulli les uniques rationnels (B_k) satisfaisant l'équation**

$$\frac{t}{e^t-1}\ =\ \sum_k B_k\frac{t^k}{k!},\quad |t|<1\ .$$

On les calcule par récurrence : $B_0\ =\ 1$, $B_1\ =\ -1/2$, $B_2\ =\ 1/6$, $B_3\ =\ 0$ **et en fait** $B_{2i+1}\ =\ 0$ **pour tout** $i>0$, $B_4\ =\ -1/30$, **...,** $B_{12}\ =\ -\frac{691}{2730}$.

[16] On doit cette remarque à K. Belabas

Théorème Kummer p ***est régulier si et seulement si pour tous les nombres de Bernoulli*** B_{2k}, $2 \leq 2k \leq p-3$, ***on a*** $v_p(B_{2k}) \ = \ 0$.

Par exemple 691 **est irrégulier et** 691 **divise le nombre de classes de** $\mathbb{Q}(\zeta_{691})$ **car**

$$v_{691}(B_{12}) \ = \ 1 \ .$$

Il y a une infinité de nombres premiers irréguliers (Adleman, Heath-Brown, puis Fouvry 1985). On ne sait toujours pas s'il existe une infinité de nombres premiers réguliers.