UNIVERSITÉ DE BORDEAUX I 2007-2008
MASTER DE MATHÉMATIQUES *1ère année*
Option : Théorie algébrique des nombres.

Corrigé DM 1

Exercice 1.

1. Le nombre $H_{p-1} = \sum_{k=1}^{p-1} \frac{1}{k}$ est une fraction dont le dénominateur n'est pas divisible par p, on peut donc le considérer comme élément de $\mathbb{Z}_{(p)}$. Dire que son numérateur est divisible par p^2 est alors équivalent à dire qu'il appartient à $p^2\mathbb{Z}_{(p)}$.
2. On regroupe 2 par 2 les termes de la somme définissant H_{p-1}, le premier avec le dernier, le deuxième avec l'avant dernier *etc.*, ce qui donne

$$\begin{aligned} H_{p-1} &= \left(1 + \frac{1}{p-1}\right) + \left(\frac{1}{2} + \frac{1}{p-2}\right) + \cdots \\ &= \sum_{i=1}^{\frac{p-1}{2}} \left(\frac{1}{i} + \frac{1}{p-i}\right) \\ &= p \sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i(p-i)} \end{aligned}$$

3. On a $\frac{1}{p-i} + \frac{1}{i} = \frac{p}{i(p-i)} \in p\mathbb{Z}_{(p)}$, donc $\frac{1}{p-i} \equiv \frac{-1}{i} \mod p\mathbb{Z}_{(p)}$, et $\frac{1}{i(p-i)} \equiv \frac{-1}{i^2} \mod p\mathbb{Z}_{(p)}$. Ainsi, $\sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i(p-i)} \equiv -\sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i^2} \mod p\mathbb{Z}_{(p)}$. Par ailleurs, puisque $\frac{1}{p-i} \equiv \frac{1}{-i} \mod p\mathbb{Z}_{(p)}$, on peut écrire

$$\sum_{i=1}^{p-1} \frac{1}{i^2} \equiv \sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i^2} + \sum_{i=1}^{\frac{p-1}{2}} \frac{1}{(-i)^2} \equiv 2 \sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i^2} \mod p\mathbb{Z}_{(p)}$$

soit

$$\sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i^2} \equiv \frac{1}{2} \sum_{i=1}^{p-1} \frac{1}{i^2} \mod p\mathbb{Z}_{(p)}.$$

Il y a $p-1$ classes non nulles dans $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \simeq \mathbb{Z}/p\mathbb{Z}$, représentées par les entiers de 1 à $p-1$. Comme $\frac{1}{i} - \frac{1}{j} \notin p\mathbb{Z}_{(p)}$ pour $1 \leq i \neq j \leq p-1$, les éléments $\frac{1}{i}$, $1 \leq i \leq p-1$ constituent également un système de représentants de ces $p-1$ classes non nulles. Par conséquent

$$\frac{1}{2} \sum_{i=1}^{p-1} \frac{1}{i^2}. \equiv \frac{1}{2} \sum_{i=1}^{p-1} i^2 \mod p\mathbb{Z}_{(p)}.$$

On obtient donc que

$$\sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i(p-i)} \equiv -\frac{1}{2}\sum_{i=1}^{p-1} i^2 \mod p\mathbb{Z}_{(p)}$$

pour tout premier $p \neq 2$.

4. La formule classique $\sum_{i=1}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$ entraîne que $\sum_{i=1}^{p-1} i^2 = \frac{(p-1)p(2p-1)}{6}$, égalité qui vaut dans $\mathbb{Q}$ mais également dans $\mathbb{Z}_{(p)}$ sous réserve que 6 soit inversible dans $\mathbb{Z}_{(p)}$, ce qui est le cas si $p \neq 2$ et $p \neq 3$, soit dès que $p \geq 5$. En rassemblant les résultats précédents, il vient :

$$H_{p-1} = p\sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i(p-i)} \equiv -p^2\frac{(p-1)(2p-1)}{12} \mod p\mathbb{Z}_{(p)}$$

donc $H_{p-1} \in p^2\mathbb{Z}_{(p)}$.

Exercice 2. $k[X,Y]$ n'est pas un anneau de Dedekind : il existe des idéaux premiers non nuls qui ne sont pas maximaux. C'est le cas par exemple de l'idéal $\mathfrak{p} = Xk[X,Y]$: il est premier et non maximal, car le quotient $k[X,Y]/\mathfrak{p} \simeq k[Y]$ est un anneau intègre mais pas un corps (pour établir l'isomorphisme $k[X,Y]/\mathfrak{p} \simeq k[Y]$ on compose l'injection canonique $k[Y] \hookrightarrow k[X,Y]$ et la surjection $k[X,Y] \twoheadrightarrow k[X,Y]/\mathfrak{p}$) .

Exercice 3.

1. Comme racine d'un polynôme unitaire à coefficients entiers, θ est une entier algébrique, ainsi que toutes ses puissances. Par conséquent $\mathbb{Z}[\theta] \subset \mathbb{Z}_K$. Puisque $\theta^n = -a_{n-1} - \cdots - a_1\theta - a_0$, toutes les puissances de θ s'expriment comme combinaison linéaire à coefficients entiers de 1, θ, …, θ^{n-1}. Autrement dit $\mathbb{Z}[\theta] = \mathbb{Z} \oplus \mathbb{Z}\theta \oplus \cdots \oplus \mathbb{Z}\theta^{n-1}$, ce qui implique en particulier que $\mathbb{Z}[\theta]$ et $\mathbb{Z}_K$ ont même rang n ; le quotient $\mathbb{Z}[\theta]/\mathbb{Z}_K$ est donc fini.
2. Soit M_x la matrice de la multiplication par x dans la base $\{1, \theta, \cdots, \theta^{n-1}\}$, dont le déterminant est égal, par définition, à la norme $\mathrm{N}_{K/\mathbb{Q}}(x)$ de x. Puisque x est combinaison linéaire à coefficients entiers de 1, θ, …, θ^{n-1}, et que toutes les puissances de θ s'expriment comme combinaison linéaire à coefficients entiers de 1, θ, …, θ^{n-1} (même argument que précédemment), il est clair que la matrice M_x est à coefficients entiers. Il revient donc au même de calculer le déterminant de M_x modulo p ou de calculer le déterminant de la matrice $\overline{M_x}$ obtenue en réduisant M_x modulo p (coefficient par coefficient). En combinant les relations

$$x\theta^i = \sum_{j=0}^{n-1} c_j\theta^{i+j} \quad (1)$$

$$\theta^{n+j} = -\sum_{k=0}^{n-1} a_k\theta^{k+j} \text{ pour } j \geq 0, \quad (2)$$

et le fait que $a_k \equiv 0 \mod p$ pour $0 \leq k \leq n-1$, on montre facilement que

$$\overline{M_x} = \begin{pmatrix} \overline{c_0} & 0 & \cdots & 0 & 0 \\ \overline{c_1} & c_0 & \ddots & \vdots & \vdots \\ \vdots & \overline{c_1} & \ddots & 0 & \vdots \\ \vdots & \vdots & \ddots & \overline{c_0} & 0 \\ \overline{c_{n-1}} & \overline{c_{n-1}} & \cdots & \overline{c_1} & \overline{c_0} \end{pmatrix}.$$

Par conséquent $\det \overline{M_x} = \overline{c_0}^n$, ce qui signifie que $\mathbb{N}_{K/\mathbb{Q}}(x) \equiv c_o^n \mod p$.

3. (a) On rappelle que si G est groupe fini dont l'ordre est divisible par un nombre premier p, alors G contient un élément d'ordre p (*théorème de Cauchy*). Appliqué au groupe quotient $\mathbb{Z}_K/\mathbb{Z}[\theta]$, ceci garantit l'existence d'un élément $y \in \mathbb{Z}_K \setminus \mathbb{Z}[\theta]$ tel que $py \in \mathbb{Z}[\theta]$. Ceci signifie exactement que $y = \frac{c_0+c_1\theta+\cdots+c_{n-1}\theta^{n-1}}{p}$ où les c_i sont des entiers non tous divisibles par p.

   (b) On a d'une part $\mathbb{N}_{K/\mathbb{Q}}(y) = \frac{\mathbb{N}_{K/\mathbb{Q}}(c_0+c_1\theta+\cdots+c_{n-1}\theta^{n-1})}{p^n} \in \mathbb{Z}$, puique y est entier, et $\mathbb{N}_{K/\mathbb{Q}}(c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1}) \equiv c_o^n \mod p$ d'après la première question. Par conséquent, p divide c_0.

   (c) On peut écrire $y = \frac{c_0}{p} + \theta\frac{c_1+c_2\theta+\cdots+c_{n-1}\theta^{n-2}}{p}$, et puisque $\frac{c_0}{p} \in \mathbb{Z}$, on conclut que l'élément $y' = y - \frac{c_0}{p} = \theta\frac{c_1+c_2\theta+\cdots+c_{n-1}\theta^{n-2}}{p}$ est un entier algébrique. Ceci implique en particulier que $\mathbb{N}_{K/\mathbb{Q}}(y') = \frac{\mathbb{N}_{K/\mathbb{Q}}(\theta)}{p^n}\mathbb{N}_{K/\mathbb{Q}}(c_1 + c_2\theta + \cdots + c_{n-1}\theta^{n-2})$ est un entier. Comme $\mathbb{N}_{K/\mathbb{Q}}(\theta) = \pm a_0$ est divisible par p mais pas par p^2, la valuation p-adique de $\frac{\mathbb{N}_{K/\mathbb{Q}}(\theta)}{p^n}$ vaut $1-n$. Par ailleurs, $\mathbb{N}_{K/\mathbb{Q}}(c_1 + c_2\theta + \cdots + c_{n-1}\theta^{n-2}) \equiv c_1^n \mod p$. Par conséquent, il faut, pour que $\mathbb{N}_{K/\mathbb{Q}}(y')$ soit entier, que c_1 soit divisible par p. En itérant ce procédé, on montre que tous les c_i sont divisibles par p, une contradiction.

4. Le polynôme $P(X) = X^3 - 3$ est d'Eisenstein en 3, donc irréductible. Ainsi, l'extension $K = \mathbb{Q}(\theta)$ est de degré 3, et ce qui précède montre que l'indice $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ n'est pas divisible par 3. Grâce aux formules vues en TD, on calcule $\text{Disc}(\mathbb{Z}[\theta]) = 27 * (-3)^3 = 3^6$. La relation $\text{Disc}(\mathbb{Z}[\theta]) = [\mathbb{Z}_K : \mathbb{Z}[\theta]]^2 \text{Disc}(\mathbb{Z}_K)$ implique alors que $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ est une puissance de 3. Ces deux propriétes pour l'indice $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ ne sont compatibles que si $[\mathbb{Z}_K : \mathbb{Z}[\theta]] = 3^0 = 1$, soit $\mathbb{Z}_K = \mathbb{Z}[\theta]$.