UNIVERSITÉ DE BORDEAUX
M1, Théorie des Nombres
2020-2021

Feuille 5. Exercices de révision

Exercice 1. L'équation $y^2 = x^3 - 1$. On cherche les solutions de l'équation $y^2 = x^3 - 1$ dans $\mathbf{Z}$. Supposons que $(x, y) \in \mathbf{Z}^2$ est une solution. Alors $x^3 = (y + i)(y - i)$ dans $\mathbf{Z}[i]$.

1) Soit $d = PGCD(y + i, y - i)$. Montrer que $d \mid 2$.

2) On veut prouver par l'absurde que $d = 1$. Montrer que si $d \neq 1$, alors $y^2 \equiv -1 \pmod 8$, et expliquer pourquoi cette congruence n'a pas de solution dans $\mathbf{Z}$.

3) Montrer qu'il existe $u, v \in \mathbf{Z}[i]$ tels que $y + i = u^3$ et $y - i = v^3$. En déduire qu'il existe $a, b \in \mathbf{Z}$ tels que $3a^2b - b^3 = 1$.

4) En déduire que $x = 1$, $y = 0$ est l'unique solution de l'équation diophantienne $y^2 = x^3 - 1$.

Exercice 2. Soit p un nombre premier et soit $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbf{Z}[X]$ un polynôme d'Eisenstein en p. On note α une racine de $f(X)$ et on pose $K = \mathbf{Q}[\alpha]$. Soit O_K l'anneau des entiers de K. On veut montrer par l'absurde que $p \nmid [O_K : \mathbf{Z}[\alpha]]$. On note $N : K \to \mathbf{Q}$ l'application norme.

1) Montrer que $p \mid N(\alpha)$ et que $p^2 \nmid N(\alpha)$.

2) Montrer que $\alpha^n/p \in O_K$.

Supposons que $p \mid [O_K : \mathbf{Z}[\alpha]]$.

3) Montrer qu'il existe $x \in O_K \setminus \mathbf{Z}[\alpha]$ tel que $px \in \mathbf{Z}[\alpha]$. En déduire qu'il existe $b_0, \ldots, b_{n-1} \in \mathbf{Z}$ tels que :

a) $\dfrac{b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}}{p} \in O_K$;

b) Il existe i tel que $p \nmid b_i$.

4) Soit i le plus petit entier pour lequel $p \nmid b_i$. Montrer que

$$\frac{b_i\alpha^i + \cdots + b_{n-1}\alpha^{n-1}}{p} \in O_K.$$

5) Montrer que $b_i\alpha^{n-1}/p \in O_K$ et aboutir à une contradiction.

Exercice 3. Soit p un nombre premier et soit $K = \mathbf{Q}[\sqrt[p]{p}]$.

1) Calculer le discriminant de $\mathbf{Z}[\sqrt[p]{p}]$.

2) Montrer que $O_K = \mathbf{Z}[\sqrt[p]{p}]$.

Exercice 4. Soit A un anneau de Dedekind. Pour tous idéaux I_1, I_2 et I_3 de A montrer que

$$I_1 \cap (I_2 + I_3) = (I_1 \cap I_2) + (I_1 \cap I_3); \qquad I_1 + (I_2 \cap I_3) = (I_1 + I_2) \cap (I_1 + I_3).$$

Exercice 5. Un anneau est local s'il admet un unique idéal maximal. Montrer que tout anneau de Dedekind local est principal.