Théorie des nombres

CORRIGÉ DU PARTIEL

Exercice 1

On pose $A = \mathbf{Z}[i\sqrt{5}]$ et $N(a+ib\sqrt{5}) = (a+ib\sqrt{5})(a-ib\sqrt{5}) = a^2+5b^2$. Alors pour tout quadruplet d'entiers relatifs (a,b,c,d), on a d'une part la relation :

$$N((a+ib\sqrt{5})(c+id\sqrt{5})) = N(a+ib\sqrt{5})N(c+id\sqrt{5}) = (a^2+5b^2)(c^2+5d^2)$$

et d'autre part la relation :

$$N((a+ib\sqrt{5})(c+id\sqrt{5})) = N(ac-5bd+i\sqrt{5}(ad+cb)) = (ac-5bd)^2+5(ad+cb)^2$$

D'où l'égalité :

$$(a^2+5b^2)(c^2+5d^2) = (ac-5bd)^2+5(ad+cb)^2$$

.

Exercice 2

1. Se donner un polynôme de degré strictement inférieur à m, c'est choisir les m coefficients du polynôme. Etant donné qu'ici il y a p choix pour chacun des coefficients, il y a en tout p^m polynômes de degré strictement inférieur à m. De même que $n = |n|$ est le nombre d'entiers naturels strictement inférieurs à l'entier naturel n, on pose pour tout polynôme unitaire de $k[X]$ de degré m, $\parallel f \parallel = p^m$.
2. Comme on est sur un corps, $\deg(fg) = \deg(f) + \deg(g)$ et $\parallel fg \parallel = \parallel f \parallel \parallel g \parallel$.
3. Comme il y a p^i polynômes unitaires de degré i (autant que de polynômes de degré strictement inférieur à i), nous avons :

   $$\sum_{\substack{f\in k[X] \\ \text{unitaire de degré } \leq m}} \frac{1}{\parallel f \parallel} = \sum_{i=0}^{m} \frac{p^i}{p^i} = m+1$$

   on a bien une série divergente. Et de plus :

   $$\sum_{\substack{f\in k[X] \\ \text{unitaire de degré } \leq m}} \frac{1}{\parallel f \parallel^2} = \sum_{i=0}^{m} \frac{p^i}{(p^i)^2} = \sum_{i=0}^{m} \frac{1}{(p^i)}$$

   qui est la somme partielle d'une série géométrique convergente ;
4. Comme pour tout$n \in \mathbf{N}^*$, $\zeta_n > 0$, on peut considérer $\ln(\zeta_n)$.

   $$\ln(\zeta) = \sum_{f\ \in \mathcal{P}_n} -\ln(1-\frac{1}{\parallel f \parallel})$$

   C'est une série à termes positifs et on a $-\ln(1-\frac{1}{\|f\|}) \sim \frac{1}{\|f\|}$ pour $\parallel f \parallel$ grand, d'où d'après la question précédente c'est une série divergente, et $\lim \zeta_n = +\infty$.

5. Nous avons, comme $\frac{1}{\|f\|} < 1$,

$$ln(\zeta_n) = \sum_{f\ \in\mathcal{P}_n} -ln(1-\frac{1}{\parallel f \parallel}) = \sum_{f\ \in\mathcal{P}_n}\sum_{k=1}^{+\infty}\frac{1}{k \parallel f \parallel} = \sum_{f\in\mathcal{P}_n}\frac{1}{\parallel f \parallel} + \sum_{f\in\mathcal{P}_n}\sum_{k=2}^{+\infty}\frac{1}{k \parallel f \parallel^k}$$

6. Remarquons que

$$\sum_{f\in\mathcal{P}_n}\sum_{k=2}^{+\infty}\frac{1}{k \parallel f \parallel^k} = \sum_{f\in\mathcal{P}_n}\frac{1}{\parallel f \parallel^2}\sum_{k=2}^{+\infty}\frac{1}{k \parallel f \parallel^{k-2}}$$

   Or nous avons :

$$\sum_{k=3}^{+\infty}\frac{1}{k \parallel f \parallel^{k-2}} \leq \sum_{k=1}^{+\infty}\frac{1}{kp^k} = ln(1+\frac{1}{p})$$

   donc comme on a affaire à des sommes de termes tous positifs, il vient de la question 3 que $\sum_{k=2}^{+\infty}\frac{1}{k\|f\|^{k-2}}$ admet une limite qui est finie.

   On en déduit immédiatement que la somme $\sum_{f\in\mathcal{P}}\frac{1}{\parallel f \parallel}$ est infinie et donc que l'ensemble $\mathcal{P}$ des polynômes irréductibles à coefficients dans $\mathbf{F}_p$ est lui-même est infini.

Exercice 3

1. Si p est un tel nombre premier, alors modulo 3, $p = a^2[3]$, or les seuls carrés modulo 3 sont 0 et 1. Comme $p \neq 3$, il vient que p est congru à 1 modulo 3.
2. On a par hypothèse que 3 divise $p-1$: $p-1 = 3k$. Soit x un générateur du groupe cyclique $(\mathbf{F}_p)^*$, alors x^k est par construction d'ordre 3.
3. Soit α un élément d'ordre 3 dans $\mathbf{F}_p$, alors α est une racine du polynôme $X^3-1 = (X-1)(X^2+X+1)$, comme $\alpha \neq 1$, et comme $\mathbf{F}_p$ est intègre, c'est bien une racine de (X^2+X+1).
4. Comme $\sqrt{-3} = 2j+1$ est dans B, $A \subset B$.
   Si $y = 2z$ dans $\mathbf{Z}$, alors $\alpha = x-1+z\sqrt{-3}$ est dans A. Réciproquement si $\alpha = x+jy = \frac{2x-1}{2} + \sqrt{-3}\frac{y}{2}$ s'écrit $a+\sqrt{-3}b$ dans A. Puisque 1 et $\sqrt{-3}$ sont indépendant dans $\mathbf{C}$, $y = 2b$ est pair.
5. Si $\alpha = x+jy$, $j\alpha = jx+(-1-j)y = -y+j(x-y)$ et $j^2\alpha = (-1-j)x+y = -1+y-jx$. Or soit y, soit $-x$, soit $x-y$ est pair.
6. Si p est une norme dans A, alors c'est une norme dans B. Réciproquement si p est la norme de α dans B, c'est aussi la norme de $j\alpha$ ou encore de $j^2\alpha$, donc d'un élément du petit anneau A.
7. $4 = 2\times 2 = (1+\sqrt{-3})(1-\sqrt{-3})$. De plus, comme l'équation $a^2+3b^2 = 2$ n'a pas de solution dans $\mathbf{Z}^2$, les facteurs indiqués, tous de norme $4 = 2\times 2$ sont irréductibles. Comme l'équation $2(a+\sqrt{-3}b) = (1+\sqrt{-3})$ n'a pas de solution dans A les facteurs ne sont pas associés. Donc A n'est pas factoriel.

8. L'anneau B est intègre comme sous-anneau de $\mathbf{C}$. Montrons qu'il est euclidien. Soit $x+jy$ et $r+js$ deux élément de B. Soit z le nombre complexe $z=\frac{x+jy}{r+js}$. Puisque les abscisses de deux éléments proches dans B diffèrent de 1 et les ordonnées de $\sqrt{3}/2$, Il existe un élément de q de B tel que $|q-z|^2 \leq (1/2)^2+(\sqrt{3}/4)^2 = 7/16 < 1$. Alors, soit $(x+jy) = q(r+js)$, soit

$$|(x+jy)-q(r+js)| \leq |r+js||z-q| < |r+js|.$$

La norme complexe fournit donc une jauge euclidienne.

9. Comme le polynôme minimal de j dans $Z[X]$ est X^2+X+1, chacun des deux est isomorphe au quotient $\frac{Z[X]}{(p,X^2+X+1)}$.
10. Comme X^2+X+1 a une racine dans $\mathbf{F}_p$ il est réductible dans $\mathbf{F}_p[X]$. Les anneaux $\mathbf{F}_p[X]/(X^2+X+1)$ et donc $B/(p)$ ne sont donc pas intègres. Comme B est factoriel et que l'idéal (p) n'est pas premier, p est réductible dans B. Noter que ce raisonnement ne vaut pas dans A non factoriel : l'idéal (2) n'est pas premier dans A $(1+\sqrt{-3})(1-\sqrt{-3}) \in (2))$ mais est engendré par un irréductible (2 n'est pas une norme dans A).
11. Il existe donc x et y dans B, non inversibles tels que $p=xy$. On a $p^2 = N(xy) = N(x)N(y)$ et $N(x) \neq 1$, $N(y) \neq 1$. Par conséquent $N(x) = p$.
12. Comme p est une norme dans B, c'est aussi une norme dans A. Il s'écrit donc $p = a^2+3b^2$ avec $(a,b) \in \mathbf{Z}^2$.