Colles de Maths - semaine 20 - MP*1

Julien Allasia - ENS de Lyon

Exercice 1 Soit p un nombre premier.

1. Montrer que, pour tout $n \in \mathbb{N} \setminus \{0\}$,
$$\nu_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor .$$
2. Déterminer le nombre de 0 à la fin de l'écriture décimale de l'entier 100!.

Exercice 2 Soit A un anneau intègre fini. Montrer que A est un corps.

Exercice 3 Soit $p \geqslant 3$ un nombre premier.
Déterminer le nombre de carrés dans $\mathbb{Z}/p\mathbb{Z}$ et montrer que si $x \neq 0$,
$$\begin{cases} x \text{ est un carré} & \iff \quad x^{\frac{p-1}{2}} = 1; \\ x \text{ n'est pas un carré} & \iff \quad x^{\frac{p-1}{2}} = -1. \end{cases}$$

Exercice 4 Soit $d \in \mathbb{N}^*$. On pose
$$\Phi_d = \prod_{1 \leqslant k \leqslant d,\ k \wedge d = 1} \left(X - e^{\frac{2ik\pi}{d}} \right).$$
Montrer que pour tout $d \in \mathbb{N}^*$, $\Phi_d \in \mathbb{Z}[X]$.

Exercice 5

1. Soit $P, Q \in \mathbb{Z}[X]$ non nuls. On note $c(P), c(Q)$ les PGCD des coefficients de P et Q. Montrer que
$$c(PQ) = c(P)c(Q).$$
2. Soit $P \in \mathbb{Z}[X]$ un polynôme non constant. Montrer que P est irréductible dans $\mathbb{Z}[X]$ si et seulement s'il est irréductible dans $\mathbb{Q}[X]$ et tel que $c(P) = 1$.

Exercice 6 *On admet le lemme de Gauss (exercice précédent) et on admet que les propriétés générales de $K[X]$ (intégrité, existence et unicité de la décomposition en facteurs irréductibles...) sont vraies avec n'importe quel corps K, même non inclus dans $\mathbb{C}$.*
Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$ et p un nombre premier, tels que

(i) p ne divise pas a_n ;
(ii) p divise $a_0, \dots, a_{n-1}$;
(iii) p^2 ne divise pas a_0.

Montrer que P est irréductible dans $\mathbb{Q}[X]$

Exercice 7 On admet le critère d'Eisenstein (exercice précédent). Soit p un nombre premier. Montrer que
$$\mathbb{Q}[e^{\frac{2i\pi}{p}}] = \{Q(e^{\frac{2i\pi}{p}}),\ Q \in \mathbb{Q}[X]\}$$
est un corps, et déterminer sa dimension comme $\mathbb{Q}$-espace vectoriel.

Exercice 8 Soit K un corps et G un sous-groupe fini de K^*. Dénombrer l'ensemble des éléments de G d'ordre d pour tout d diviseur de $|G|$, et en déduire que G est cyclique.