

DM 2

À remettre le 15 mars.

1. Soit $P(X) \in \mathbb{Z}[X]$ de degré au moins 1. Montrer que $P(X)$ a des racines modulo p pour une infinité de nombres premiers p (on pourra dans un premier temps supposer que $P(0) = 1$ et examiner les facteurs premiers des entiers $P(n!)$, $n \in \mathbb{N}$, puis dans un second temps, considérer le polynôme $Q(X) = \frac{P(P(0)X)}{P(0)}$ pour se ramener à cette situation).
2. Soit $K = \mathbb{Q}(\theta)$ un corps de nombres, d'anneau des entiers $\mathbb{Z}_K$. On note $P(X)$ le polynôme minimal de θ .
 - (a) Soit p un nombre premier tel que $P(X)$ admette une racine modulo p , autrement dit tel qu'il existe $a \in \mathbb{Z}$ tel que $P(a) \equiv 0 \pmod{p}$.
 - i. Montrer que $I = p\mathbb{Z}[\theta] + (\theta - a)\mathbb{Z}[\theta]$ est un idéal maximal de $\mathbb{Z}[\theta]$ et que $\mathbb{Z}[\theta]/I \simeq \mathbb{F}_p$.
 - ii. Soit $\mathfrak{p}$ un idéal maximal de $\mathbb{Z}_K$ contenant I . Montrer que $\mathfrak{p} \cap \mathbb{Z}[\theta] = I$ et que l'injection canonique de $\mathbb{Z}[\theta]$ dans $\mathbb{Z}_K$ induit un homomorphisme injectif de $\mathbb{Z}[\theta]/I$ dans $\mathbb{Z}_K/\mathfrak{p}$.
 - iii. On suppose que p ne divise pas $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$. Montrer qu'alors $\mathbb{Z}[\theta]/I \simeq \mathbb{Z}_K/\mathfrak{p}$ (montrer que l'homomorphisme de la question précédente est un isomorphisme).
 - (b) Montrer qu'il y a une infinité d'idéaux maximaux $\mathfrak{p}$ de $\mathbb{Z}_K$ de degré résiduel $f(\mathfrak{p}) = 1$.
3. Soit K une extension galoisienne de $\mathbb{Q}$. Montrer qu'il y a une infinité de nombres premiers totalement décomposés dans K .
4. Soit m un entier. Montrer que l'ensemble des nombres premiers $p \equiv 1 \pmod{m}$ est infini (on pourra se placer dans le corps cyclotomique $K = \mathbb{Q}(\zeta_m)$).