Université Paris Diderot
M1 Arithmétique
2010-2011

Feuille d'exercices IX

Soit p un nombre premier. On désigne par $|\cdot|_p$ la valeur absolue p-adique de $\mathbb{Q}$. Soient $\mathbb{Q}_p$ le complété de $\mathbb{Q}$ par rapport à $|\cdot|_p$ et $\mathbb{Z}_p$ la boule unité fermée de $\mathbb{Q}_p$.

Exercice 1 Soit
$$F(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$$
un polynôme unitaire dans $\mathbb{Z}_p[X]$. On suppose que $a_i \in p\mathbb{Z}_p$ pour tout $i \in \{0, \dots, n-1\}$ et que $a_0 \notin p^2\mathbb{Z}_p$.

1) Montrer que le polynôme F est irréductible dans $\mathbb{Z}_p[X]$. On peut prendre la réduction de F modulo p.
2) En déduire que le polynôme F est irréductible dans $\mathbb{Q}_p[X]$.

Exercice 2 Soit p un nombre premier.

1) Montrer que, pour tout entier $n \geqslant 1$, le $(p^n)^{\text{ième}}$ polynôme cyclotomique est
$$\Phi_{p^n}(X) = \sum_{k=0}^{p-1} X^{kp^{n-1}}.$$
2) Montrer que Φ_p est irréductible dans $\mathbb{Q}_p[X]$. (Indication : on peut considérer le polynôme $\Phi_p(X+1)$).
3) Montrer que $(X+1)^{p^{n-1}} - X^{p^{n-1}} - 1 \in p\mathbb{Z}[X]$ pour tout entier $n \geqslant 1$.
4) En déduire que $\Phi_{p^n}(X+1) - X^{p^{n-1}(p-1)} \in p\mathbb{Z}[X]$.
5) Calculer $\Phi_{p^n}(1)$.
6) Montrer que Φ_{p^n} est irréductible dans $\mathbb{Q}_p[X]$.

Exercice 3 Soient p un nombre premier et ζ une racine $p^{\text{ième}}$ de l'unité qui est primitive. On désigne par $\mathbb{Z}[\zeta]$ le plus petit sous-anneau de $\mathbb{Q}(\zeta)$ qui contient $\mathbb{Z} \cup \{\zeta\}$.

1) Soient r et s deux entiers tels que $p \nmid rs$. Montrer que $(\zeta^r - 1)/(\zeta^s - 1)$ est un élément inversible dans $\mathbb{Z}[\zeta]$.
2) Montrer que $(1-\zeta)^{p-1}/p$ est un élément inversible dans $\mathbb{Z}[\zeta]$.
3) En déduire que $N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1-\zeta) = p$.
4) Montrer que le discriminant de la base $(1, \zeta, \dots, \zeta^{p-2})$ de $\mathbb{Q}(\zeta)$ sur $\mathbb{Q}$ est $\pm p^{p-2}$.

Exercice 4 Soit p un nombre premier impair. On note
$$S := \sum_{a \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right) \zeta^a,$$
où ζ est une racine $p^{\text{ième}}$ de l'unité qui est primitive, $\left(\frac{-}{p}\right)$ est le symbole de Legendre modulo p.

1) Montrer que
$$S^2 = \sum_{(a,b)\in(\mathbb{F}_p^\times)^2} \Big(\frac{b}{p}\Big)\zeta^{a(b+1)}$$

2) En déduire que
$$S^2 = \Big(\frac{-1}{p}\Big)p.$$

3) En déduire que $\mathbb{Q}(\sqrt{p})$ est ou bien contenu dans $\mathbb{Q}(\zeta, i)$ ou bien contenu dans $\mathbb{Q}(\zeta)$.

Exercice 5 Soient A un anneau commutatif, R une algèbre sur A, r un élément de R. On dit que r est *entier* sur A s'il est une racine d'un polynôme unitaire dans $A[X]$.

1) Montrer que les propriétés suivantes sont équivalentes :
   (i) r est entier sur A.
   (ii) La sous-algèbre $A[r]$ de R est un A-module de type fini.
   (iii) Il existe une sous-algèbre de R contenant r qui est un A-module de type fini.
   (iv) Il existe un $A[r]$-module M tel que $\operatorname{ann}_{A[r]}(M) = 0$ qui est un A-module de type fini.
2) Supposons que R est engendrée par un nombre fini d'éléments entiers sur A. Montrer que R est un A-module de type fini.
3) Montrer que les éléments de R qui sont entiers sur A forment une sous-A-algèbre de R.

Exercice 6 Soit K une extension finie de $\mathbb{Q}_p$.

1) Montrer que, si
$$F(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n \qquad (a_0 \neq 0)$$
est un polynôme dans $\mathbb{Q}_p[X]$ qui est irréductible, alors pour tout $i \in \{0, \dots, n\}$ on a $|a_i|_p \leqslant \max(|a_0|_p, |a_n|_p)$. En déduire que, si $a_0 = 1$ et si $a_n \in \mathbb{Z}_p$, alors $F \in \mathbb{Z}_p[X]$.
2) Soit $\mathcal{O}_K$ l'ensemble des éléments de K qui sont entiers sur $\mathbb{Z}_p$. Montrer que
$$\mathcal{O}_K = \{\alpha \in K \mid N_{K/\mathbb{Q}_p}(\alpha) \in \mathbb{Z}_p\}.$$
3) Soit $|\cdot| : K \to \mathbb{R}_+$ l'application qui envoie $\alpha \in K$ en
$$|N_{K/\mathbb{Q}_p}(\alpha)|_p^{1/[K:\mathbb{Q}_p]}.$$
   (i) Montrer que l'application $|\cdot|$ prolonge la valeur absolue p-adique.
   (ii) Montrer que $|\cdot|$ est multiplicative : on a $|\alpha\beta| = |\alpha| \cdot |\beta|$ pour tous $\alpha, \beta \in K$.
   (iii) Montrer que $\mathcal{O}_K = \{\alpha \in K \,:\, |\alpha| \leqslant 1\}$.
   (iv) En déduire que $|\cdot|$ est une valeur absolue non-archimédienne sur K.
4) Montrer que $|\cdot|$ est l'unique valeur absolue sur K qui prolonge $|\cdot|_p$.