Université Paris Sud — Année 2007-2008

M1 — Arithmétique

Examen partiel du 26 mars 2008

Durée 3 heures

La qualité de la rédaction entrera pour une grande part dans la notation. Les calculatrices, téléphones mobiles et documents ne sont pas autorisés.

Les trois problèmes sont indépendants. Notes de cours autorisées. On choisit une fois pour toutes une clôture algébrique $\overline{\mathbb{Q}}$ de $\mathbb{Q}$ et, pour tout nombre premier p, une clôture algébrique $\overline{\mathbb{Q}_p}$ de $\mathbb{Q}_p$.

Exercice A

1) Un anneau de valuation est un anneau commutatif intègre A qui est tel que, si un élément b de son corps des fractions n'est pas dans A, alors $1/b \in A$. Montrer qu'un anneau de valuation est un anneau local.

2) On munit le groupe $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$ de l'ordre lexicographique (on a $(m,n) \leq (m',n')$ si ou bien $m < m'$ ou bien $m = m'$ et $n \leq n'$. Soit K un corps. On suppose K muni d'une *valuation à valeurs dans* $\mathbb{Z}^2$, c'est-à-dire d'un homomorphisme du groupe multiplicatif K^* de K dans $\mathbb{Z}^2$ vérifiant $v(a+b) \geq \min\{v(a), v(b)\}$ si a, b et $a+b$ sont non nuls. Montrer que $A = \{a \in K^* \mid v(a) \geq 0 = (0,0)\} \cup \{0\}$ est un anneau de valuation de corps des fractions K (on l'appelle *l'anneau de la valuation* v).

Dans toute la suite, p est un nombre premier, v_p est l'unique valuation de $\mathbb{Q}$ telle que $v_p(p) = 1$ et $\mathbb{Q}(X)$ est le corps des fractions rationnelles en une indéterminée X à coefficients dans $\mathbb{Q}$.

3) Montrer qu'il existe une unique valuation v sur $\mathbb{Q}(X)$ à valeurs dans $\mathbb{Z}^2$ telle que $v(X) = (1,0)$ et $v(a) = (0, v_p(a))$ pour tout nombre rationnel a non nul [On pourra commencer par vérifier que, si une telle valuation existe, pour tout $P \in \mathbb{Q}[X]$ tel que $P(0) \neq 0$, on doit avoir $v(P) = (0, v_p(P(0)))$. Puis que tout $\alpha \in \mathbb{Q}(X)$ non nul peut s'écrire sous la forme $X^r P/Q$, avec $r \in \mathbb{Z}$, $P, Q \in \mathbb{Q}[X]$, $P(0) \neq 0$ et $Q(0) = 1$].

4) Montrer que l'anneau A de la valuation v est l'ensemble des $\alpha \in \mathbb{Q}(X)$ qui peuvent s'écrire sous la forme P/Q avec $P, Q \in \mathbb{Q}[X]$, $P(0) \in \mathbb{Z}_{(p)}$ et $Q(0) = 1$. Déterminer l'idéal maximal $\mathfrak{m}$ de A et le corps $A/\mathfrak{m}$.

5) Montrer que l'idéal I de A engendré par X est premier et que A/I est isomorphe à $\mathbb{Z}_{(p)}$.

Exercice B

Soient N un entier ≥ 2 et S_N l'ensemble des nombres premiers qui divisent N.

1) Soit q un nombre premier. Soit $\alpha \in \overline{\mathbb{Q}}$ une racine de $X^N - q$. Soient $E = \mathbb{Q}[\alpha]$ et $\mathcal{O}_E$ l'anneau des entiers de E.

a) Montrer que le polynôme $X^N - q$ est irréductible sur $\mathbb{Q}_q$ et sur $\mathbb{Q}$.

b) Montrer qu'il existe un et un seul idéal $\mathfrak{q}$ de $\mathcal{O}_E$ au-dessus de l'idéal de $\mathbb{Z}$ engendré par q. Calculer l'indice de ramification $e(\mathfrak{q}/(q))$ et le degré résiduel $f(\mathfrak{q}/(q))$.

c) Montrer que l'ensemble S des nombres premiers p tels que l'image de $X^N - q$ dans $\mathbb{F}_p[X]$ est un polynôme non séparable est un ensemble fini et déterminer cet ensemble.

d) Soit p un nombre premier qui n'appartient pas à S. Montrer que, si β est une racine de $X^N - p$ dans $\overline{\mathbb{Q}_p}$, l'extension $\mathbb{Q}_p(\beta)/\mathbb{Q}_p$ est non ramifiée.

e) On suppose encore que p est un nombre premier qui n'appartient pas à S. Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_E$ au-dessus de l'idéal de $\mathbb{Z}$ engendré par p. Montrer que $e(\mathfrak{p}/(p)) = 1$.

2) Déduire de la question précédente qu'il existe une infinité d'extensions de degré N de $\mathbb{Q}$ contenues dans $\overline{\mathbb{Q}}$.

Exercice C

Dans tout le problème, p est un nombre premier fixé et d est un entier ≥ 1 (on suppose $d = p$ à partir de la troisième question). On note v l'unique valuation de $\overline{\mathbb{Q}_p}$ telle que $v(p) = 1$ et $\|$ l'unique valeur absolue sur $\overline{\mathbb{Q}_p}$ telle que $|p| = p^{-1}$ (on a donc $|a| = p^{-v_p(a)}$ pour tout a non nul dans $\overline{\mathbb{Q}_p}$).

1) Combien y-a-t'il d'extensions non ramifiées de degré d de $\mathbb{Q}_p$ contenues dans $\overline{\mathbb{Q}_p}$?

2) Soit $P \in \mathbb{Q}_p[X]$ un polynôme irréductible de degré $d \geq 1$ et soient $\lambda_1, \lambda_2, \ldots, \lambda_d$ les racines de P dans $\overline{\mathbb{Q}_p}$. Soit $\mu \in \overline{\mathbb{Q}_p}$ tel que $|\mu - \lambda_1| < |\mu - \lambda_i|$ pour $i = 2, 3, \ldots, d$.

a) On pose $K = \mathbb{Q}_p(\mu)$ et $L = K(\lambda_1)$. Soit σ un K-plongement de L dans $\overline{\mathbb{Q}_p}$. Montrer qu'il existe $i \in \{1, 2, \ldots, d\}$ tel que $\sigma(\mu - \lambda_1) = \mu - \lambda_i$. L'entier i peut-il être différent de 1 ?

b) Montrer que $L = K(\lambda_1)$. Montrer que le polynôme minimal de μ sur $\mathbb{Q}_p$ est de degré $\geq d$ et que, s'il est de degré d, alors $\mathbb{Q}_p(\mu) = \mathbb{Q}_p(\lambda_1)$.

3) On suppose désormais que $d = p$ et que P est un polynôme d'Eisenstein. On pose $P = \sum_{i=0}^{p-1} a_i X^i + X^p$. Si $v(a_i) \geq 2$ pour $i = 1, 2, \ldots, p-1$, on pose $r = p - 1$. Sinon on note r le plus petit entier ≥ 0 tel que $v(a_{r+1}) = 1$.

a) Calculer $v(\lambda_1)$, montrer que $v(P'(\lambda_1)) = 1 + r/p$ et que, pour tout $r \in \mathbb{N}$, $v(P^{(r)}(\lambda_1)) \geq 1 + r/p$.

b) Utiliser la formule de Taylor pour calculer les coefficients du polynôme $Q = \prod_{i=2}^{p}(X - (\lambda_i - \lambda_1))$.

c) On pose $s = \frac{p+r}{p(p-1)}$. Montrer que, pour $i = 2, 3, \ldots, p$, on a $v(\lambda_i - \lambda_1) = s$.

4) Soit $\mu \in \overline{\mathbb{Q}_p}$. On pose $t = max_{1 \leq i \leq p} v(\mu - \lambda_i)$. Calculer $v(P(\mu))$ en fonction de t [On distinguera suivant que $t \leq s$ ou $t > s$. On pourra d'abord supposer que le maximum est atteint pour $i = 1$].

5) Montrer que si $\mu \in \overline{\mathbb{Q}_p}$ est tel que $v(P(\mu)) > ps$, alors il existe i tel que $\lambda_i \in \mathbb{Q}_p(\mu)$.

6) On suppose $r \neq p-1$. Soient R_1, R_2 des polynômes à coefficients dans $\mathbb{Z}_p$ vérifiant $\deg R_1 < p$ et $\deg R_2 < p - 2 - r$ (on a donc $R_2 = 0$ si $r = p - 2$). Soit $P_1 = P - p^2 R_1 - pX^{r+2} R_2$. Montrer qu'il existe une racine μ de P_1 dans $\overline{\mathbb{Q}_p}$ telle que $\mathbb{Q}_p(\mu) = \mathbb{Q}_p(\lambda_1)$.

7) On suppose $r = p-1$. Donner une condition nécessaire et suffisante, analogue à la précédente, pour qu'un polynôme $P_1 \in \mathbb{Q}_p[X]$, unitaire de degré p, admette une racine μ dans $\overline{\mathbb{Q}_p}$ telle que $v(\mu - \lambda_1) > v(\mu - \lambda_i)$ pour $i = 2, 3, \ldots, p$.

8) Montrer qu'il n'y a qu'un nombre fini d'extensions de degré p de $\mathbb{Q}_p$ contenues dans $\overline{\mathbb{Q}_p}$.