Partiel d'Algèbre, Semestre 2, 2013.

Durée 2 heures. 5 Mars 2013, 13h30-15h30
Notes de cours autorisées.

Exercice 1

1. Soient $\begin{array}{c} M \\ | \\ K \end{array}$ une extension finie de K, et L_1, L_2 deux sous-corps de M contenant K.

   On suppose que $M = K(L_1 \cup L_2)$. Montrer que $[M; L_1] \leq [L_2; K]$.

2. Soit α et β des racines primitives respectivement n-ième et m-ième de l'unité dans $\overline{\mathbb{Q}}$. On suppose que $pgcd(n, m) = 1$.

   Verifier que $[\mathbb{Q}(\alpha\beta); \mathbb{Q}] = \varphi(nm) = \varphi(n)\varphi(m)$, où φ est l'indicatrice d'Euler.

3. Montrer que $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}$.

Exercice 2

1. Soit $r \geq 1$ un entier. Justifier que tout élément de $\mathbb{F}_{2^r}$ est un carré.

Dans toute la suite p est un nombre premier impair, $r \in \mathbb{N}^*$, et $q = p^r$.

2. Déterminer le noyau du morphisme de groupe $\phi : \left\{ \begin{array}{ccc} \mathbb{F}_q^* & \to & \mathbb{F}_q^* \\ x & \mapsto & x^2 \end{array} \right.$

   En déduire le cardinal de l'ensemble $C \subset \mathbb{F}_q^*$ des carrés de $\mathbb{F}_q^*$.

3. Identifier l'image du morphisme $\psi : \left\{ \begin{array}{ccc} \mathbb{F}_q^* & \to & \mathbb{F}_q^* \\ x & \mapsto & x^{\frac{q-1}{2}} \end{array} \right.$ et montrer que son noyau vaut C.

4. A quelle condition sur q, l'élément -1 est-il un carré dans $\mathbb{F}_q$?

5. En considérant un entier n (grand) et un diviseur premier de $(n!)^2 + 1$, montrer qu'il existe une infinité de nombres premiers de la forme $4m + 1$.

La suite ne dépend pas des questions 4 et 5.

Tournez S.V.P.

6. On se place dans le cas $r = 1$. On note le *symbole de Legendre sur* $\mathbb{F}_p$ comme suit : $\mathrm{Leg}_p(x) = 1 \in \mathbb{Z}$ si x est un carré de $\mathbb{F}_p^*$ et $= -1 \in \mathbb{Z}$ sinon. Comparez Leg_p et ψ (dans le cas $q = p$).

7. Soit ζ une racine primitive p-ième de l'unité dans $\overline{\mathbb{Q}}$. Si $x \in \mathbb{F}_p^*$, on note ζ^x l'élément de $\overline{\mathbb{Q}}$ donné par $\zeta^{\tilde{x}}$ pour $\tilde{x}$ un relevé (arbitraire) de x dans $\mathbb{Z}$. Après avoir verifié que cela a un sens, montrer que si l'on note

$$s = \sum_{x \in \mathbb{F}_p^*} \mathrm{Leg}_p(x) \zeta^x \in \overline{\mathbb{Q}}$$

alors

$$s^2 = \sum_{x \in \mathbb{F}_p^*, y \in \mathbb{F}_p^*} \mathrm{Leg}_p(y) \zeta^{x(y+1)}$$

8. Justifier que l'on a

$$\sum_{x \in \mathbb{F}_p^*} \mathrm{Leg}_p(x) = 0$$

9. Montrer que $s^2 = p$ si -1 est un carré de $\mathbb{F}_p$ et $= -p$ sinon.

10. Soit $d \in \mathbb{Z}$, et $\omega \in \overline{\mathbb{Q}}$ tel que $\omega^2 = d$. Montrer qu'il existe ξ une racine de l'unité telle que $\mathbb{Q}(\omega) \subset \mathbb{Q}(\xi)$.

Fin.