Université de Nice - Sophia Antipolis
Préparation à l'agrégation de mathématiques
Semaine du 13 au 19 novembre 2006

Exercice 1.

a) Soit G un groupe abélien noté additivement et soient a et b deux éléments de G d'ordres finis et premiers entre eux ; montrez que l'ordre de $a+b$ est le produit des ordres de a et de b.

b) Soit G un groupe abélien fini et soit e le plus petit commun multiple des ordres des éléments de G. Montrez que e est l'ordre d'un élément de G.

c) Soit k un corps commutatif et soit G un sous-groupe fini de k^*. Soit n le cardinal de G et soit e le plus petit commun multiple des ordres des éléments de G. Montrez que e ne peut être strictement inférieur à n (ici intervient le corps k), et conclure que G est cyclique.

Exercice 2. Soit k un corps fini de caractéristique différente de 2, soit q son cardinal et soit $\phi : k^* \to k^*$ l'élévation au carré.

a) Quel est le cardinal de Im ϕ ? En déduire que si a est un élément de k^* qui est un carré dans k, alors $a^{(q-1)/2}$ est égal à 1.

b) Réciproquement, montrez que si a est un élément de k^* et si $a^{(q-1)/2} = 1$, alors a est un carré dans k^*.

c) En déduire que (-1) est un carré dans k si et seulement si $q-1$ est multiple de 4.

d) Montrez qu'il existe un corps fini L contenant k et possédant un élément ω tel que $\omega^4 = -1$. On pose $y = \omega + \omega^{-1}$; vérifez que $y^2 = 2$. En déduire que 2 est un carré dans k si et seulement si $y^q = y$, et que ceci se produit si et seulement si q est congru à 1 ou -1 modulo 8.

e) Dans un corps fini de caractéristique 2, quels sont les carrés ?

Exercice 3. On rappelle que 641 est premier. À l'aide de la loi de réciprocité quadratique, déterminez pour chacun des entiers suivants s'il est un carré modulo 641 : 111, 320, 29.

Exercice 4. Soient a, b, c trois entiers relatifs dont aucun n'est un carré dans $\mathbb{Z}$, et tels que le produit soit le carré d'un élément de $\mathbb{Z}$ (donnez des exmples de tels triplets). Soit P le polynôme $(X^2-a)(X^2-b)(X^2-c)$. Montrez que P n'a pas de racine dans $\mathbb{Q}$, mais qu'il en a une modulo p pour tout p. Montrez la même assertion au sujet du polynôme $(X^2+3)(X^3+2)$.