Université Paris 7-Denis Diderot — MT-282
D.E.U.G.- S.M. — Année 1999-00

EXAMEN du 20 janvier 2000

Durée : 3 h

Exercice 1

1. Démontrer que $5.2^7 + 1$ divise $5^4.2^{28} - 1$ et que $5^4 + 2^4$ divise $5^4.2^{28} + 2^{32}$. En déduire que 641 divise $2^{32} + 1$.
2. Trouver un entier $n \geq 0$ tel que $2^{2^n} + 1$ ne soit pas un nombre premier.
3. Quel est l'ordre de $\bar{2}$ dans $(\mathbf{Z}/641\mathbf{Z})^*$?
4. Le groupe $(\mathbf{Z}/641\mathbf{Z})^*$ est-il cyclique ?
5. Démontrer que $\bar{2}$ est une puissance 5-ème dans $(\mathbf{Z}/641\mathbf{Z})^*$.

Exercice 2

Soit G un groupe. Soit l un nombre premier. Soit $x \in G$ d'ordre fini m.
1. Démontrer qu'il existe un unique couple d'entiers $(m', m")$ tels que m' soit une puissance de l et que $m"$ soit premier à l et que $m = m'm"$, puis qu'il existe $(a, b) \in \mathbf{Z}^2$ tel que $am' + bm" = 1$.
2. Quels sont alors les ordres de $x^{am'}$ et $x^{bm"}$?
3. En déduire qu'il existe $x' \in H_x$ d'ordre m' et $x'' \in H_x$ d'ordre $m"$ tels que $x = x'x" = x"x'$, où H_x est le sous-groupe de G engendré par x. Fixons deux tels éléments x' et $x"$.
4. Soient $y' \in G$ d'ordre une puissance de l et $y" \in G$ d'ordre premier à l tels que $x = y'y" = y"y'$. Démontrer que $y'x = xy'$ et que $y"x = xy"$.
5. En déduire que $x'y' = y'x'$ et que $x"y" = y"x"$. Démontrer que $x'y'^{-1}$ est d'ordre une puissance de l et que $x"^{-1}y"$ est d'ordre premier à l. Conclure que $x' = y'$ et $x" = y"$.
6. Lorsque $G = Z/96Z$, $l = 2$, et $x = \bar{2}$, déterminer x' et $x"$ (attention : dans $Z/96Z$ la loi de groupe se note additivement).

Exercice 3

Soit p un nombre premier. Posons $\mathbf{Z}_{(p)} = \{u/v \in Q/u \in Z, v \in Z, p \not| v\}$.
1. Démontrer que $Z_{(p)}$ muni de l'addition et de la multiplication est un anneau.
2. Quels sont les élément inversibles de $Z_{(p)}$? Y a-t-il des éléments d'ordre 3 dans $Z^*_{(p)}$? Y a-t-il des éléments d'ordre infini dans $Z^*_{(p)}$?
3. Posons $p\mathbf{Z}_{(p)} = \{u/v \in Q/u \in pZ, v \in Z, p \not| v\}$. Démontrer que $p\mathbf{Z}_{(p)}$ est un sous-groupe de $\mathbf{Z}_{(p)}$. Est-il distingué ?
4. Considérons l'application $\phi : Z_{(p)} \longrightarrow Z/pZ$ qui à u/v associe $\bar{u}(\bar{v})^{-1}$. Démontrer que ϕ est un homomorphisme d'anneaux. Quel est son noyau ? Est-il surjectif ?
5. En déduire que $\mathbf{Z}_{(p)}/p\mathbf{Z}_{(p)}$ est un groupe isomorphe à Z/pZ.