Université Bordeaux 1 — **MHT633 – Arithmétique et Cryptologie**
Mathématiques — Année 2008–2009

DEVOIR n° 1 (pour la semaine du lundi 9 mars)

Le principal résultat établi dans ce devoir est le théorème suivant :

Théorème 1. *Soit K un corps commutatif. Tout sous-groupe fini du groupe multiplicatif K^* est* cyclique.

A. Généralités sur les groupes cycliques

Dans cette partie on établit quelques propriétés des groupes cycliques. Soit donc G un groupe cyclique d'ordre n ; on note multiplicativement sa loi de composition interne et 1 son élément neutre.

On rappelle la définition de la fonction φ d'Euler : pour $n \geqslant 1$, on pose

$$\varphi(n) = \operatorname{card}\{a, 1 \leqslant a \leqslant n : (a, n) = 1\}.$$

1) Soit g un générateur de G. Montrez que l'ordre d'un élément $x = g^r$ de G est $n \,/\, \operatorname{pgcd}(r, n)$.

2) Soit d un diviseur de n. Montrez que G contient exactement $\varphi(d)$ éléments d'ordre d.

3) En déduire la formule :

$$n = \sum_{d|n} \varphi(d),$$

valable pour tout entier $n \geqslant 1$.

4) Soit d un diviseur de n. Montrez que $H := \{x \in G \colon x^d = 1\}$ est un sous-groupe de G d'ordre d.

5) Montrez que, pour tout d divisant n, G contient un unique sous-groupe d'ordre d et que celui-ci est cyclique. On en précisera un générateur.

6) Donnez un contre exemple aux propriétés (2) et (5) lorsque G n'est pas cyclique.

7) Soit G un groupe d'ordre n, tel que, pour tout diviseur d de n, G possède un unique sous-groupe d'ordre d. Montrez que G est cyclique.

B. Démonstration du théorème

Soit G un sous-groupe fini de K^*, de cardinal n ; a priori, on ne suppose *plus* que G est cyclique. On fixe $a, b \in G$, d'ordres respectifs α et β.

1) Montrer que si α et β sont premiers entre eux, alors ab a pour ordre $\alpha\beta$.

2) Soit $H = \langle a, b \rangle$ le sous-groupe de G engendré par a et b. Montrer qu'il existe $g \in H$ d'ordre $\mathrm{ppcm}(\alpha, \beta)$.

[*Indication : soit* $\prod p_i^{e_i}$ *la décomposition en produit de facteur premiers du ppcm en question ; pour chaque* i*, déterminer un* $g_i \in H$ *d'ordre* $p_i^{e_i}$.]

3) Soit ω le ppcm des ordres des éléments de G. Déduire de la question précédente qu'il existe $g \in G$ d'ordre ω et que ω divise n.

4) En remarquant que tout $x \in G$ est racine de $X^\omega - 1$, montrer que $\omega = n$. En déduire que tout sous-groupe multiplicatif fini G d'un corps commutatif K est cyclique.

C. Exemple

Soit $\mathbb{F}_3 := \mathbb{Z}/3\mathbb{Z}$ et $\mathbb{F}_9 := \mathbb{F}_3[X]/(X^2+1)\mathbb{F}_3[X]$. On note $x := X \pmod{X^2+1}$.

1) Montrez que $\mathbb{F}_9$ est un corps à 9 éléments. Exprimez tous ses éléments comme combinaisons linéaires de 1 et x.

2) Déduire de la partie B que $\mathbb{F}_9^*$ est un groupe cyclique à 8 éléments et de la partie A son nombre de générateurs.

3) Calculez l'ordre de chacun des éléments de $\mathbb{F}_9^*$; en particulier vous identifierez ses générateurs.