

## ALGEBRE L3

Automne 2015

### Exercices

#### Feuille 7

##### *Colliers*

Un collier  $c$  est un anneau de  $n$  perles; supposons que chaque perle peut avoir  $m$  couleurs.

Pour chaque  $e \in \mathbb{N}^*$  on définit le collier  $ec$  à  $en$  perles et  $em$  couleurs par concaténation.

Un collier de la forme  $c = dc'$  pour  $d|n$ ,  $d > 1$ , est appelé décomposable. Un collier qui n'est pas décomposable est appelé *primitif*.

1. Prouver le *théorème de Moreau* (1872, cf. [M]) : le nombre de colliers primitifs à  $n$  perles et à  $\leq m$  couleurs est égal à  $M_n(m)$ .

Faire d'abord le cas  $n = p$  un nombre premier.

Ici

$$M_n(x) = \frac{1}{n} \sum_{d|n} \mu(d) x^{n/d}$$

C. Moreau était un capitaine d'artillerie français.

[M] C. Moreau, Sur les permutations circulaires distinctes, *Nouv. Ann. Math.*, **11** (1872), 309 - 314.

##### *Fonction d'Euler $\phi(n)$*

Notation:  $[1, n] := \{a \in \mathbb{Z}, 1 \leq a \leq n\}$ .

On définit

$$\Phi(n) = \{a \in \mathbb{Z}, 1 \leq a \leq n \mid (a, n) = 1\};$$

Ici  $(a, n)$  désigne le pgcd de  $a$  et  $n$ .

$$\phi(n) := \text{Card}(\Phi(n))$$

**2.** Définissons une bijection

$$\alpha : [1, n] \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z}$$

en posant

$$\alpha(i) = i \pmod n.$$

Montrez que  $i \in [1, n]$  appartient à  $\Phi(n)$  si et seulement si  $\alpha(i)$  est un générateur du groupe  $\mathbb{Z}/n\mathbb{Z}$ .

Donc,  $\alpha$  induit une bijection de  $\Phi(n)$  avec l'ensemble  $\Psi(n)$  des générateurs de  $\mathbb{Z}/n\mathbb{Z}$ .

**3.** Soit  $G = \mathbb{Z}/n\mathbb{Z}$ .

(a) Soit  $d|n$ . Montrez qu'il existe  $x \in G$  d'ordre  $d$ .

(b) Montrez que  $G$  contient un seul sous-groupe  $G_d \subset G$  d'ordre  $d$ ;  $G_d$  est le sous-groupe engendré par  $x$ .

(c) Montrez que l'ensemble  $\Phi_d$  des éléments d'ordre  $d$  dans  $G$  coïncide avec l'ensemble de générateurs de  $G_d$ .

(d) Montrez que

$$G = \coprod_{d|n} \Phi_d$$

et en conclure que

$$n = \sum_{d|n} \phi(n).$$

**4.** (a) Montrez que

$$\phi(n) = \sum_{d|n} d\mu(n/d)$$

(b) Montrer, en employant (a), que si  $n = \prod_{i=1}^r p_i^{a_i}$  est la décomposition en facteurs premiers (tous  $p_i$  étant distincts), alors

$$\phi(n)/n = \prod_{i=1}^r (1 - p_i^{-1})$$

*Corps fini  $\mathbb{F}_p$*

Soient  $p$  un nombre premier;  $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ . On va noter par  $\mathbb{F}_p^*$  son groupe multiplicatif, i.e.

$$\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\},$$

avec la multiplication comme la loi de composition.

6. (a) Montrez que le polynôme

$$f(x) = x^{p-1} - 1$$

admèt  $p - 1$  racines dans  $\mathbb{F}_p$ .

(b) Montrez que si  $m|n$ , alors le polynôme

$$f_m(x) = x^m - 1$$

divise  $f_n(x)$  dans l'anneau de polynômes  $k[x]$ ,  $k$  étant un corps.

(c) Montrez, en utilisant (b), que si  $d|(p - 1)$  alors le polynôme

$$f_d(x) = x^d - 1$$

admèt  $d$  racines dans  $\mathbb{F}_p$ .

(d) Soit  $\psi(d)$  le nombre d'éléments d'ordre  $d$  dans  $\mathbb{F}_p^*$ . Montrez que

$$d = \sum_{c|d} \psi(c).$$

(Utilisez (c).)

(e) En déduire que

$$\psi(d) = \sum_{c|d} c\mu(d/c) = \phi(d).$$

(f) En conclure que  $\psi(p - 1) > 0$  et que le groupe  $\mathbb{F}_p^*$  est cyclique.