# FEUILLE nº 2 : GROUPES FINIS, ACTIONS DE GROUPE

## Exercice 1

La fonction $\varphi$ d'Euler est définie par $\varphi(n) = \#\{k \in [\![1, n]\!]$ tels que pgcd(k, n) = 1$\}$.

**1.** ***a.*** Démontrer que pour tout entier premier $p$ et tout entier $n$, $\varphi(p^n) = p^n - p^{n-1}$.

***b.*** Démontrer que $\varphi$ est multiplicative, c'est-à-dire que si $a$ et $b$ sont premiers entre eux, $\varphi(ab) = \varphi(a)\varphi(b)$.

***c.*** En déduire que si $n = \Pi p_k^{r_k}$, $\varphi(n) = \Pi p_k^{r_k-1}(p_k - 1)$.

**2.** ***a.*** Démontrer que pour tout entiers $a$ et $n$ premiers entre eux, $a^{\varphi(n)} \equiv 1 \ (n)$.

***b.*** En déduire les deux derniers chiffres de $12^{42}$.

***c.*** Soit $p$ un nombre premier congru à $-1$ modulo 4 et supposons que $p$ divise $x^2 + y^2$. Montrer que $p$ divise $x$ et $y$.

**3.** ***a.*** Résoudre les équations $\varphi(n) = i$ pour $i = 1, 2, 3, 4$.

***b.*** Montrer que pour tout entier $d$, l'équation $\varphi(n) = d$ n'a qu'un nombre fini de solutions.

***c.*** En déduire que $\varphi(n)$ tend vers l'infini quand $n$ tend vers l'infini.

## Exercice 2

**1.** Soit $G$ un groupe fini d'ordre $n$.

***a.*** En faisant agir $G$ par translation sur lui-même (à gauche ou à droite), démontrer que $G$ est un sous-groupe du groupe $\mathfrak{S}_n$.

***b.*** Dans le cas $G = \mathbb{Z}/n\mathbb{Z}$, expliciter le sous-groupe cyclique de $\mathfrak{S}_n$ obtenu.

***c.*** Déduire de a. que pour tout corps $\mathbf{k}$, $G$ est un sous-groupe de $\mathrm{GL}_n(\mathbf{k})$.

**2.** Si $G$ est un sous-groupe fini de $\mathrm{GL}_n(\mathbb{Z})$, démontrer que pour tout nombre premier $p \geq 3$, la composition $G \hookrightarrow \mathrm{GL}_n(\mathbb{Z}) \to \mathrm{GL}_n(\mathbb{F}_p)$ est injective.

## Exercice 3

**1.** Soit $G$ un groupe fini agissant sur un espace fini $X$.

***a.*** Rappeler l'énoncé du lemme de Burnside attaché à la paire $(X, G)$, et expliquer brièvement quel est son intérêt.

***b.*** Montrer que pour tout $g$ dans $G$, $\#X^g$ ne dépend que de la classe de conjugaison de $G$.

***c.*** Reformuler le lemme de Burnside à l'aide des classes de conjugaisons de $G$.

**2.** On cherche à compter combien de colliers de perles on peut former avec 3 perles rouges, 2 perle bleues et 1 perle verte.

***a.*** Dénombrer le nombre de colliers possibles manuellement.

***b.*** Retouver le résultat de 2.a à l'aide du lemme de Burnside.

## Exercice 4

Soit $\mathbf{k}$ un corps.

1. *a.* Calculer les éléments inversibles de l'anneau $\mathbf{k}[[t]]$.

   *b.* En déduire que $\mathbf{k}[[t]]$ est principal.

2. Les anneaux $\mathbf{k}[x, y]$ et $\mathbf{k}[[x, y]]$ sont-ils principaux ?

## Exercice 5

1. Soit $A$ un anneau euclidien. À tout couple d'éléments $(x, y)$ où $y$ est non nul, on associe le couple $(y, r)$, où $x = by + r$ est la division euclidienne de $x$ par $y$.

   *a.* Démontrer que les idéaux $(x, y)$ et $(y, r)$ coïncident.

   *b.* Établir que l'algorithme $(x, y) \mapsto (y, r)$ aboutit en un nombre fini d'étapes à couple de la forme $(d, 0)$.

   *c.* Que vaut $d$ ?

2. Calculer le pgcd de 243 et 198 dans $\mathbb{Z}$.

3. Calculer le pgcd de $22 + \mathbf{i}$ et 97 dans $\mathbb{Z}[i]$.

4. Pour tout entier $r \geq 1$, on définit le r-ème nombre de Mesrenne $M_r$ par $M_r = 2^r - 1$. Démontrer que $\mathrm{pgcd}(M_r, M_s) = M_{\mathrm{pgcd}(r,s)}$.

## Exercice 6

Le but de cet exercice (facultatif) est de présenter un cadre conceptuel général généralisant celui de la question 1 de l'exercice 4.

Soit $K$ un corps. Une valuation sur $K$ est une application $v\colon K \longrightarrow \mathbb{Z} \cup \{+\infty\}$ telle que :

- $v(x) = +\infty \Leftrightarrow x = 0$.
- $v(xy) = v(x) + v(y)$
- $v(x + y) \geq \min(v(x), v(y))$ avec égalité si $v(x) \neq v(y)$.

Un anneau commutatif $A$ est dit anneau de valuation discrète si $A$ se réalise comme sous-anneau d'un corps $K$ muni d'une valuation $v$ telle que $A = \{x \in K, v(x) \geq 0\}$.

1. Soit $A$ un anneau de valuation discrète.

   *a.* Démontrer que les éléments inversibles de $A$ sont les éléments de valuation nulle.

   *b.* Soit $t$ un élément non nul de $A$ de valuation minimale. Démontrer que $(t)$ est un idéal qui contient tous les autres idéaux de $A$.

   *c.* En utilisant la même méthode qu'à la question précédente, montrer que $A$ est principal.

   *d.* Préciser le résultat précédent en démontrant que les seuls idéaux de $A$ sont les $(t^s)$ pour $s \in \mathbb{N}$.

2. *a.* Montrer que pour tout corps $\mathbf{k}$ l'anneau des séries formelles à coefficients dans $\mathbf{k}$ est un anneau de valuation discrète.

   *b.* Même question pour les séries entières à coefficients réels ou complexe de rayon de convergence $> 0$.