PRES Sorbonne-Paris Cité.
Université Paris 13
Institut Galilée
Licence Informatique Semestre 4 **feuille TD n° 5**

Groupes, $\mathbb{Z}/n\mathbb{Z}$ et $(\mathbb{Z}/n\mathbb{Z})^*$

Exercice 1. Etudier l'ensemble des groupes d'ordre (c'est-à-dire de cardinal) 1, 2, 3, 4.

Exercice 2. Trouver l'ensemble des sous-groupes de $\mathbb{Z}/6\mathbb{Z}$

Exercice 3. (*i*) Dans $\mathbb{Z}/15\mathbb{Z}$, résoudre les équations suivantes
- (*i*) $\dot{4}x = \dot{12}$
- (*ii*) $\dot{12}x = \dot{4}$

(*ii*) Combien existe-t-il d'homomorphismes de groupes f de $(\mathbb{Z}, +, 0)$ dans $(\mathbb{Z}/15\mathbb{Z})^*$ tels que $f(1) = 7$? Calculer l'image de 8 par un tel homomorphisme.

Exercice 4.

(*i*) Rappelez les propriétés que vous connaissez sur le nombre de racines dans $\mathbb{K}$ d'un polynôme dans $\mathbb{K}[X]$, pour $\mathbb{K}$ étant respectivement $\mathbb{C}, \mathbb{R}, \mathbb{Z}$.

(*ii*) Dans $\mathbb{Z}/6\mathbb{Z}$, trouver les racines du polynôme $P(X) = X^2 - X$.

(*iii*) Trouver dans $\mathbb{Z}/6\mathbb{Z}[X]$ deux factorisations distinctes de $X^2 - X$ sous la forme $(X - \dot{a})(X - \dot{b})$.

(*iv*) Trouver dans $\mathbb{Z}/2\mathbb{Z}[X]$ tous les polynômes de degré au plus 3. Quels sont ceux qui sont irréductibles ? Factoriser en produit d'irréductibles les autres.

(*v*) On suppose $n \in \mathbb{P}$. Montrer que
- (*i*) tout polynôme de $\mathbb{Z}/n\mathbb{Z}[X]$ de degré k supérieur ou égal à 1 peut être mis sous la forme d'un produit d'une constante et d'un polynôme unitaire (coefficient de plus haut degré = 1).
- (*ii*) que les polynômes de degré 1 ont au plus une racine dans $\mathbb{Z}/n\mathbb{Z}$
- (*iii*) que si $\dot{a}$ est une racine de P, alors $(X - \dot{a})|P$. On pourra se ramener à P unitaire et raisonner par récurrence forte en utilisant $Q = P - X^{k-1}(X - \dot{a})$.
- (*iv*) En déduire par récurrence sur k que si $n \in \mathbb{P}$, alors tout polynôme de degré k supérieur ou égal à 1, à coefficient dans $\mathbb{Z}/n\mathbb{Z}[X]$, admet au plus k racines.

(*vi*) Qu'en concluez-vous ?

Exercice 5. Soit $(G, \times, 1)$ un groupe commutatif fini de n éléments. On appelle ordre d'un élément $x \in G$ le plus petit entier naturel non nul k tel que $x^k = 1$.

(*i*) Quel est le cardinal de $(\mathbb{Z}/15\mathbb{Z})^*$, ensemble des éléments inversibles de $\mathbb{Z}/15\mathbb{Z}$?

(*ii*) Expliquer pourquoi tout élément d'un groupe fini possède un ordre ?

(*iii*) Soit $x \in G$, d'ordre k. Montrer que $< x >= \{1, x, x^2, \cdots x^{k-1}\}$ est un sous-groupe de G.

(*iv*) En déduire que k est un diviseur de n et que $x^n = 1$.

(*v*) Quel est l'ordre des éléments de $(\mathbb{Z}/15\mathbb{Z})^*$?

(*vi*) Le groupe $(\mathbb{Z}/15\mathbb{Z})^*$ est-il cyclique (y-a-t-il un élément d'ordre le cardinal de $(\mathbb{Z}/15\mathbb{Z})^*$?

Application : soit $p \in P$ et $a \in \mathbb{N} - p\mathbb{N}$, montrer que $a^{p-1} - 1$ est divisible par p.