Université Saclay-Paris-Sud **Feuille de TD 7** **M303**

Exercice 1 Soient a et b deux entiers tels que $a \geq b \geq 1$ et $a \wedge b = 1$.

1. Montrer que $a + b \wedge a - b = 1$ ou 2.
2. Montrer que $a + b \wedge ab = 1$.
3. Montrer que $a + b \wedge a^2 + b^2 = 1$ ou 2.

Exercice 2 Soit p un nombre premier et n un entier positif. On note $\binom{p}{k}$ le nombre de parties à k éléments dans un ensemble à p éléments.

1. Si $1 \leq k \leq p$, montrer que p divise $\binom{p}{k}$.
2. En déduire que
$$\forall a, b \in \mathbb{Z} \text{ on a } (a+b)^p = a^p + b^p \mod p.$$

Exercice 3 Trouver tous les points dans $\mathbb{Z}^3$ du plan d'équation $6x + 10y + 15z = 1997$. Combien y a-t-il de solutions dans $\mathbb{N}^3$?

Exercice 4 Trouver la décomposition selon le théorème de structure des groupes abéliens finis du groupe
$$\mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}.$$

Exercice 5 Montrer qu'un groupe abélien fini non cyclique possède un sous-groupe isomorphe à $(\mathbb{Z}/p\mathbb{Z})^2$ pour un certain nombre premier p.

Exercice 6

1. On rappelle que si p est un nombre premier impair et $n \geq 1$, le groupe $(\mathbb{Z}/p^n\mathbb{Z})^\times$ des éléments inversibles de $\mathbb{Z}/p^n\mathbb{Z}$ est cyclique. Donner son cardinal.
2. Soit $G = (\mathbb{Z}/6615\mathbb{Z})^\times$. Ecrire G sous la forme $G \cong \prod_{i=1}^s \mathbb{Z}/d_i\mathbb{Z}$ avec s un entier positif et d_i des entiers strictement positifs et $d_{i+1}|d_i$ pour $1 \leq i \leq s-1$.

Exercice 7 On considère dans $A := \mathbb{Z}^3$ le sous-groupe B engendré par $v = (6, -12, 0)$ et $w = (0, 8, 4)$. On note $A^* := \mathrm{Hom}(A, \mathbb{Z})$ l'ensemble des morphismes de groupes de A à valeurs dans $\mathbb{Z}$, également appelé ensemble des *formes linéaires entières* sur A.

1. Le groupe A^* est-il de type fini ? libre ? (On peut parfaitement résoudre la fin de l'exercice sans répondre à cette question.)
2. Montrer que l'application $A^* \to \mathbb{Z}$ donnée par $f \mapsto f(v)$ (respectivement $A^* \to \mathbb{Z}$, donnée par $f \mapsto f(w)$ est un morphisme de groupes dont l'image est le sous-groupe $6\mathbb{Z}$ $\mathbb{Z}$ (respectivement le sous-groupe $4\mathbb{Z}$ de $\mathbb{Z}$).
3. En déduire que
$$\forall f \in A^*,\ f(B) \subset 2\mathbb{Z}.$$
4. Soit $f \in A^*$ la forme linéaire définie par $x \mapsto x_1 - x_2$. Trouver $v_1 \in B$ tel que $f(v_1) = 2$ puis montrer que $v_1 = 2u_1$ pour un certain $u_1 \in A$.
5. Montrer que
$$A = \mathbb{Z}u_1 \oplus \mathrm{Ker} f,$$
puis que
$$B = 2u_1\mathbb{Z} \oplus (\mathrm{Ker} f \cap B).$$

6. Écrire les coordonnées d'un vecteur $\lambda v + \mu w$, pour $(\lambda, \mu \in \mathbb{Z})$. En déduire que $\mathrm{Ker} f \cap B$ est l'ensemble des vecteurs de la forme $(12t, 0, 12t)$ où t décrit $\mathbb{Z}$.
7. En déduire une base de B, et une base (u_1, u_2, u_3) de A telles que

$$B = 2u_1\mathbb{Z} \oplus \ \mathbb{Z} \cdot 12u_2\mathbb{Z}.$$

Exercice 8 On considère

$$H := \{(a, b) \in \mathbb{Z}^2 \mid a - b \text{ est divisible par } 10\}.$$

1. Montrer que H est un sous-groupe abélien libre de $\mathbb{Z}^2$.
2. Calculer son rang, en donner une base.
3. Décrire le quotient $\mathbb{Z}^2/H$.

Exercice 9 1. Soit $A = \mathbb{Z}^2$ et B le sous-groupe de A engendré par $b_1 = (14, 2)$ et $b_2 = (2, 4)$. Calculer une base de A adaptée à B (on en rappellera la définition). Donner la structure du quotient A/B.

2. Soit G un groupe abélien (noté additivement) et possédant deux générateurs a et b tels que $14a + 2b = 0_G$ et $2a + 4b = 0_G$. Montrer que G est isomorphe à un quotient du groupe A/B précédent.

Exercice 10 Soit A un groupe aélien.

1. Montrer que $\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, A) = A[m] := \{a \in A \mid ma = 0\}$ (on donnera explicitement un isomorphisme).
2. Montrer que $\mathrm{Hom}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/q\mathbb{Z}) \simeq \mathbb{Z}/p \wedge q\mathbb{Z}$.
3. Montrer que $\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}) = \{0\}$.
4. Montrer que $\mathrm{Hom}(\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \simeq \mathbb{Z}/m\mathbb{Z}$.

Exercice 11 Soit G un groupe abélien engendré par trois éléments x, y, z vérifiant les deux relations suivantes :

$$5x - 2y + 12z = 0 \quad \text{et} \quad 3x + 4z = 0.$$

Donner la structure du groupe G.

Exercice 12 Soit K un corps fini de cardinal q. Montrer en utilisant le théorème de structure que le groupe K^* est cyclique. (question annexe : montrer que q est une puissance d'un nombre premier p et donner la structure du groupe $(K, +)$).

Exercice 13 Soit G un groupe abélien fini. Un caractère de G est un morphisme de G dans $\mathbb{C}^*$.

1. Montrer qu'un caractère de G est à valeur dans le groupe μ_∞ des racines de l'unité.
2. Soit G un groupe abélien fini et H un sous groupe tel qu'il existe x dans G tel $G =< H, x >$. Soit r le plus petit entier non nul tel que x^r est dans H (justifier son existence). Montrer que tout élément de G s'écrit de manière unique sous la forme hx^k avec h dans H et k entre 0 et $r - 1$.

3. Soit χ un caractère de H. Posons ζ une racine r-ieme de l'unité de $\chi(x^r)$ ie telle que $\zeta^r = \chi(x^r)$. Montrer que l'on peut prolonger χ à G en utilisant la décomposition de la question précédente et la racine ζ

4. Utiliser ce qui précède pour prouver que si G est un groupe abélien fini et H un sous groupe de G alors tout caractère de H s'étend en un caractère de G.

5. Soit G un groupe abélien fini et n_1 l'ordre maximal d'un élément x de G. Justifier que $< x >$ est isomorphe (via un morphisme χ_1) au groupe μ_{n_1} des racines n_1-eme de l'unités. En déduire qu'il existe un isomorphisme entre G et $G/ < x > \times < x >$.

6. En déduire une démonstration de l'existence dans le théorème de structure des groupes abéliens finis.