

L3 (S6) – Méthodes analytiques dans l'arithmétique.

Contrôle continu.

4 mars 2026

Durée 1 heure. Utilisation des documents autorisée, mais pas encouragée.

Exercice 1.

Trouver le nombre de solutions de l'équation

$$x^6 + 2x + n = 0$$

dans l'anneau $\mathbb{Z}/81\mathbb{Z}$ en fonction de n .

Exercice 2.

Le groupe abélien est donné par trois générateurs a, b, c et trois relations

$$\begin{cases} a + 5b + c = 0 \\ 2a + 4b + 6c = 0 \\ 3a + b + c = 0 \end{cases}$$

Trouver la présentation standard de ce groupe, i.e., de la forme $\oplus_i \mathbb{Z}/d_i\mathbb{Z}$ où $d_i | d_{i+1}$.

Exercice 3.

Trouver le nombre de groupes abéliens de l'ordre $8640 = 2^6 \cdot 3^3 \cdot 5$.

Exercice 4.

Pour le groupe $(\mathbb{Z}/7\mathbb{Z})^\times$

- Explicitez un caractère χ d'ordre maximal.
- Trouver les coefficients a_i tels que

$$\sum_k a_k \chi^k(x) = \begin{cases} 1 & \text{si } x \equiv 4 \pmod{7} \\ 0 & \text{sinon} \end{cases}$$

Correction :

1a : Soit $p(x) = x^6 + 2x + n$. $p(0) \equiv n \pmod{3}$, $p(1) \equiv n \pmod{3}$, $p(2) \equiv n + 2 \pmod{3}$ donc l'équation $p(x) = 0$ une solution modulo 3 si $n \equiv 1 \pmod{3}$, deux solution si $n \equiv 0 \pmod{3}$ et pas de solution $n \equiv 2 \pmod{3}$. $p'(x) \equiv 2 \not\equiv 0 \pmod{3}$ et alors cette équation le même nombre de solution modulo 81.

2a : Soit $A = \begin{pmatrix} 1 & 5 & 1 \\ 2 & 4 & 6 \\ 3 & 1 & 1 \end{pmatrix}$ dont le pgcd est 1, La comatrice de A est $\begin{pmatrix} -2 & -4 & 26 \\ 16 & -2 & -4 \\ -10 & 14 & 6 \end{pmatrix}$, dont le pgcd est

2. $\det(A) = 68$ et donc le groupe est isomorphe à $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/34\mathbb{Z}$.

3 : Tout groupe d'ordre 8000 est un produit de groupes cyclique d'ordre d_i avec $d_i | d_{i+1}$ et $\prod d_i = 8640$. Donc $d_i = 2^{a_i} 3^{b_i} 5^{c_i}$ avec $\sum a_i = 6$, $\sum b_i = 3$, $\sum c_i = 1$. et $a_i \geq a_{i+1}$, $b_i \geq b_{i+1}$ et $c_i \geq c_{i+1}$. Alors il y a 3 possibilités pour b_i : (3), (2,1) et (1,1,1) et 11 possibilités pour a_i : (6), (5,1), (4,2), (4,1,1), (3,3), (3,2,1), (3,1,1,1), (2,2,2), (2,2,1,1), (2,1,1,1,1), (1,1,1,1,1,1) et une seule possibilité pour c . Donc il y a 33 groupes d'ordre 8000.

4a : Le groupe $(\mathbb{Z}/7\mathbb{Z})^\times$ est cyclique donc le caractère est déterminé par sa valeur sur un générateur. Pour le générateur on peu choisir par exemple 3 car modulo 7 on a $3^1 = 3$, $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$, $3^6 = 1$. L'ordre du groupe est 6 donc l'ordre maximal du générateur est 6. Le caractère à l'ordre 6 si $\chi(3)$ a l'ordre 6. Par exemple on peut prendre $\chi(3) = e^{\pi i/3}$. Donc $(\chi(1), \dots, \chi(6)) = (1, e^{2\pi i/3}, e^{\pi i/3}, e^{-2\pi i/3}, e^{-\pi i/3}, -1)$.

4b : Par la formule de la transformation de Fourier inverse $a_k = \frac{1}{6} e^{-2\pi i k}$.