# I Corps finis, groupes finis

1. **Cours :** Que savez vous sur les corps finis ?

2. Soit $\mathbf{K}$ un corps fini de caractéristique $p$. Montrer que l'application $u$ de $\mathbf{K}$ dans lui-même définie par $u(x) = x^p$ est un automorphisme de corps de $\mathbf{K}$.

3. Soit G un groupe commutatif fini. Prouver que le ppcm $m$ des ordres des éléments de $G$ est l'ordre d'un élément de $G$.
**Indication:** Si $m = \prod p_i^{\alpha_i}$ montrer tout d'abord qu'il existe des éléments d'ordres respectifs les $p_i^{\alpha_i}$.

4. Montrer que tout sous-groupe fini de $(\mathbf{K}^*, \times)$ (où $\mathbf{K}$ est un corps commutatif) est cyclique.

# II Indicatrice d'Euler

1. **Cours :**

   a) Définition de l'indicatrice d'Euler

   b) Expression générale de $\phi(n)$

   c) Théorème de Lagrange

2. déterminer $\sum_{d|n} \phi(d)$
**Indication:** Partitionner $\mathbf{Z}/n\mathbf{Z}$ de manière adaptée

3. Soient $a$ et $n$ premiers entre eux. Montrer que

$$a^{\phi(n)} \equiv 1[n]$$

**Indication:** Traduire les hypothèses dans $\mathbf{Z}/n\mathbf{Z}$

4. Montrer qu'à similitude près, il y a $\phi(n)/2$ polygones réguliers à $n$ côtés

# III Combinatoire dans $\mathrm{GL}_d(\mathbf{Z}/p\mathbf{Z})$

1. Soit p un nombre premier. Montrer que $\mathbf{Z}/p\mathbf{Z}$ est un corps.

2. Montrer que $\mathrm{GL}_d(\mathbf{Z}/p\mathbf{Z})$ est un groupe fini, et calculer son ordre.

3. Vérifier que $d!$ divise $|\mathrm{GL}_d(\mathbf{Z}/p\mathbf{Z})|$
**Indication:** $\mathrm{Card}(S_d) = d!$

**Remarque:** Étant donné un groupe $G$, on peut associer à $g_0 \in G$ la permutation $\sigma_g \in \mathcal{S}(G) : g \mapsto g_0 \cdot g$, et ainsi identifier $G$ à un sous groupe de $\mathcal{S}(G)$, lui-même sous groupe d'un $\mathrm{GL}_d(\mathbf{Z}/p\mathbf{Z})$ (via les matrices de permutations). L'étude des groupes finis se ramène donc à celle des $\mathrm{GL}_d(\mathbf{Z}/p\mathbf{Z})$.

# IV Théorème des noyaux

Soient $E$ un $\mathbf{K}$-e.v. ($\mathbf{K}$=$\mathbf{R}$ ou $\mathbf{C}$), $f \in \mathcal{L}(E)$, $P$ et $Q \in \mathbf{K}[X]$ premiers entre eux.
Démontrer :

$$\mathrm{Ker}((PQ)(f)) = \mathrm{Ker}(P(f)) \oplus \mathrm{Ker}(Q(f))$$

# V Groupe fini

Soit G un groupe fini d'odre $n \geq 2$.

1. Montrer qu'il existe une famille génératrice $\{a_1, \dots, a_k\}$ telle que pour tout $i \geq 2$, $a_i$ n'appartient pas au sous groupe engendré par $(a_1, \dots, a_{i-1})$.

2. Montrer que $n \geq 2^k$.

3. Montrer que $|\mathrm{Aut}(G)| \leq n^{\log n/\log 2}$
**Indication:** Caractériser un Automrphisme de $G$ par l'image des $a_i$.

# VI Anneaux Nœthériens

1. Montrer l'équivalence, pour une anneau $A$ unitaire, entre
   1. Tout idéal de $A$ est engendré par un nombre fini d'éléments
   2. Toute suite croissante d'idéaux de $A$ est stationnaire à partir d'un certain rang.
   3. Tout ensemble non-vide d'idéaux de $A$ possède un élément maximal pour l'inclusion

Un anneau les vérifiant est dit Nœthérien

2. Montrer que dans un anneau Nœthérien, tout élément admet une décomposition (finie) en facteurs irréductibles.

# VII Factorisation dans $\mathbf{F}_p[X]$

On notera dans cet exercice $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$.

Soit $P \in \mathbf{F}_p[X]$ non constant. On suppose que $P$ est séparable c'est-à-dire que $P$ et $P'$ sont premiers entre eux. Notons $R_P$ l'anneau $\mathbf{F}_p[X]/(P)$ des classes d'équivalences pour $Q_1 \sim Q_2 \Leftrightarrow P | Q_1 - Q_2$. Soit $P = \prod_{i=1}^r P_i$ la factorisation de $P$ en polynômes irréductibles de $\mathbf{F}_p[X]$. Notons $n_i = \deg P_i$.

1. Pourquoi $\mathbf{F}_p[X]$ est-il principal ?

2. Montrer que $R_{P_i}$ est un corps fini et donner son cardinal.

3. Pour $A \in R_P$, on désigne par $\rho_i(A)$ le reste de la division euclidienne de $A$ par $P_i$. Montrer que $A \mapsto (\rho_1(A), \rho_2(A), \dots, \rho_r(A))$ définit un isomorphisme d'anneaux $R_P \simeq \prod_{i=1}^r R_{p_i}$.

4. Si $A \in R_P$, posons $t(A) = A^p - A$.Montrer que $t$ est un endomorphisme $\mathbf{F}_p$-linéaire de $R_P$ (vu comme un $\mathbf{F}_p$-espace vectoriel) et qu'il correspond, par les isomorphismes précédents, à l'application

$$\prod_{i=1}^r R_{P_i} \to \prod_{i=1}^r R_{P_i} : (a_1, \dots a_r) \mapsto (a_1^p - a_1, \dots, a_r^p - a_r)$$

5. Montrer que le noyau de $t$ est un sous espace de $R_P$ de dimension $r$.

6. Soit $a$ un élément du noyau de $t$ . Montrer qu'il existe un polynôme unitaire $Q \in \mathbf{F}_p[X]$ de degré minimal tel que $Q(a) = 0$. Montrer que le polynôme $Q$ est scindé et séparable sur $\mathbf{F}_p$.

7. Si $a \notin \mathbf{F_p}$, montrer que $Q$ n'est pas irréductible.
   D'une factorisation partielle $Q = Q_1 Q_2$, montrer comment obtenir une factorisation partielle non triviale de $P$.