Examen – 6 mai 2021 – 13h45-16h45

Tous les documents sont autorisés, mais l'utilisation d'internet est interdite. La clarté et la précision de la rédaction seront prises en compte très significativement. En particulier, les calculs faits avec `sage` doivent être justifiés, commentés et vérifiés. Les notations de l'énoncé doivent être suivies scrupuleusement.

Au début de l'examen :

- créer une nouvelle feuille de calcul `sage` en lui donnant comme nom le numéro d'anonymat figurant sur la copie d'examen.

À la fin de l'examen :

- créer un nouveau dossier dans le dossier personnel et donner à ce dossier comme nom le numéro d'anonymat figurant sur la copie d'examen,
- mettre dans ce dossier votre feuille de calcul (au format .ipynb),
- lancer un terminal (différent de celui avec lequel vous avez lancé `sage`) et taper la commande :

  `copieexam` votre numéro d'anonymat

  Le script affiche alors soit un message d'erreur soit le nouveau contenu déposé.

Exercice 1. QUOTIENTS.

Soit k un corps fini commutatif de cardinal q et $P \in k[X]$. Soit $\pi_P : k[X] \to k[X]/(P)$ la projection canonique.

1. Quel est le noyau de π_P ?
2. Soit Q un autre polynôme, et $\pi_Q : k[X] \to k[X]/(Q)$ la projection canonique. À quelle condition sur $Q \in k[X]$ l'application π_P passe-t-elle au quotient en un morphisme d'anneaux $\phi : k[X]/(Q) \to k[X]/(P)$ (autrement dit, à quelle condition peut on écrire une factorisation $\pi_P = \phi \circ \pi_Q$ avec ϕ morphisme d'anneaux ?)
   On suppose dans la suite que cette condition est vérifiée pour $Q \in k[X]$ fixé.
3. Avec `sage`, dans le cas particulier $k = \mathbb{Z}/3\mathbb{Z}$, $P = X^2 + X$ et $Q = X^4 + X^2$:
   (a) définir les quotients $k[X]/(P)$ et $k[X]/(Q)$;
   (b) déterminer le noyau de ϕ ainsi que le nombre d'éléments de ce noyau.
4. Montrer que, pour $B \in k[X]$, $\pi_Q(B) \in \ker(\phi)$ si et seulement si $B \in \ker(\pi_P)$.
5. Décrire des représentants de $\ker(\phi)$ puis calculer le cardinal de cet ensemble en fonction de q et des degrés de P et Q. Vérifier que vos résultats sont bien cohérents avec vos calculs en `sage`.

Exercice 2. UNE ÉQUATION DANS $\mathbb{Z}/65\mathbb{Z}$.

1. Soit
$$\begin{array}{rccc} \psi : & \mathbb{Z}/65\mathbb{Z} & \longrightarrow & \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z} \\ & a \mod 65 & \longmapsto & (a \mod 5,\ a \mod 13)\,. \end{array}$$
   Justifier à l'aide du cours que ψ est un isomorphisme puis donner une formule explicite pour ψ^{-1} (on pourra utiliser `sage` pour effectuer d'éventuels calculs).

2. L'objectif de cette question est de résoudre l'équation $x^2 + 4x + 8 = 0$ dans $\mathbb{Z}/65\mathbb{Z}$.
   (a) Trouver toutes les solutions (modulo 65) avec `sage`.
   (b) Peut-on utiliser les formules usuelles ($x = \frac{-b\pm\sqrt{b^2-4ac}}{2a}$ sont les racines de $aX^2 + bX + c$ lorsque $b^2 - 4ac$ est un carré et que a et 2 sont inversibles) pour résoudre l'équation ?
   (c) Montrer que l'équation initiale est équivalente à un système de deux équations polynomiales de degré 2 dans des corps finis k_1 et k_2 que l'on précisera.
   (d) Expliquer comment retrouver les solutions données par `sage`.

Exercice 3. CORPS FINIS.

Soit p un nombre premier impair. On note $\mathbb{F}_p$ le corps à p éléments et $\mathbb{F}_{p^2}$ un corps à p^2 éléments. On note $\mathbb{F}_{p^2}^\times$ le groupe des inversibles de $\mathbb{F}_{p^2}$. On rappelle que tous les corps à p^2 éléments sont isomorphes.

Cet exercice étudie $G = \{x \in \mathbb{F}_{p^2}^\times \mid x^{p+1} = 1\}$.

1. (a) Soit $P \in \mathbb{F}_p[X]$ un polynôme de degré 2 n'admettant pas de racine sur $\mathbb{F}_p$. Montrer que $\mathbb{F}_p[X]/(P)$ est isomorphe à $\mathbb{F}_{p^2}$.
   (b) Avec `sage`, choisir aléatoirement (et afficher) un nombre premier p impair inférieur à 50 puis définir un corps K à p^2 éléments, en appelant u le générateur.
   (c) Toujours sur `sage`, générer (sans l'afficher) la liste de tous les polynômes de degré 2 sur $\mathbb{F}_p$ et vérifier qu'ils sont tous scindés sur K.
2. On rappelle que $G = \{x \in \mathbb{F}_{p^2}^\times \mid x^{p+1} = 1\}$.
   (a) Montrer que G est un sous-groupe de $(\mathbb{F}_{p^2}^\times, \times)$.
   (b) Montrer que $G \cap \mathbb{F}_p = \{1, -1\}$.
   (c) Vérifier le résultat précédent avec `sage` pour le nombre premier p choisi dans la question 1, puis déterminer (toujours avec `sage`) le cardinal de G.
3. On considère l'application $\psi : \mathbb{F}_{p^2}^\times \to \mathbb{F}_{p^2}$ définie par $\psi(x) = x + x^{-1}$.
   (a) Toujours pour le premier p choisi dans la question 1, déterminer avec `sage` l'image réciproque $\psi^{-1}(a)$ pour $a \in \{-2, -1, 0, 1, 2\}$, et donner le cardinal de $\psi^{-1}(a)$ dans chaque cas.
   (b) Soit $a \in \mathbb{F}_{p^2}$ et $x \in \mathbb{F}_{p^2}^\times$. Montrer que $\psi(x) = a$ si et seulement si x est racine de $X^2-aX+1 \in \mathbb{F}_{p^2}[X]$.
   (c) Montrer que $\mathbb{F}_p \subset \mathrm{Im}(\psi)$.
   (d) Soient $x, y \in \mathbb{F}_{p^2}^\times$. Montrer que $\psi(x) = \psi(y)$ si et seulement si $x = y$ ou $x = y^{-1}$.
   (e) Déterminer, en fonction de $a \in \mathrm{Im}(\psi)$, le cardinal de $\psi^{-1}(a)$.
   (f) En déduire le cardinal l'image $\mathrm{Im}(\psi)$ de ψ. Vérifier votre résultat avec `sage`, toujours pour le premier p de la question 1.
4. (a) Soit $Q \in \mathbb{F}_p[X]$ un polynôme de degré 2. Si $x \in \mathbb{F}_{p^2}$ est racine de Q, et $x \notin \mathbb{F}_p$, quelle est l'autre racine de Q ?
   (b) Montrer que si $x \in G$ alors $\psi(x) \in \mathbb{F}_p$.
   (c) Soit $a \in \mathbb{F}_p$. On écrit $a = \psi(x)$. Montrer que $x \in G$ ou $x \in \mathbb{F}_p^\times$.
   Si $x \notin \mathbb{F}_p$, on pourra déterminer les autres antécédents de a par ψ à l'aide des questions précédentes.
5. Déduire des questions précédentes que G est de cardinal $p + 1$.