HAX501X – Groupes et anneaux 1

Examen terminal

- Durée : 3h.
- Tout matériel électronique est interdit ainsi que les documents de cours.
- Le barème est indicatif. La notation tiendra compte de la clarté de la rédaction ainsi que de la propreté/lisibilité de la copie.

Exercice 1 : le critère d'Euler (8 pts). On fixe un nombre premier $p \neq 2$. On dit qu'un entier a non divisible par p est un carré modulo p s'il existe un entier x tel que $x^2 \equiv a \pmod{p}$. Le *critère d'Euler*, qu'on prouve dans les deux premières questions, est l'équivalence suivante :

$$a \text{ est un carré modulo } p \quad \Longleftrightarrow \quad a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \ .$$

1) Implication directe "$\Longrightarrow$".
   a) Rappeler la preuve vue en TD du petit théorème de Fermat comme application du théorème de Lagrange.
   b) Déduire du petit théorème de Fermat l'implication directe "$\Longrightarrow$".
2) Implication réciproque "$\Longleftarrow$".
   a) À quelle condition sur $u, v \in (\mathbb{Z}/p\mathbb{Z})^\times$ a-t-on $u^2 = v^2$? On justifiera.
   b) On note E l'ensemble des éléments de $(\mathbb{Z}/p\mathbb{Z})^\times$ de la forme u^2, avec $u \in (\mathbb{Z}/p\mathbb{Z})^\times$. Déduire de la question précédente que $|E| = \frac{p-1}{2}$.
   c) On note F l'ensemble des éléments $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$ qui vérifient $\overline{a}^{\frac{p-1}{2}} = \overline{1}$. Montrer que $|F| \leqslant \frac{p-1}{2}$.
   d) Déduire des questions 1) et 2)b), 2)c) qu'on a l'égalité $E = F$. En déduire l'implication réciproque $\Longleftarrow$.
3) En utilisant le critère d'Euler, énoncer et démontrer une condition nécessaire et suffisante sur un nombre premier $p \neq 2$ pour que -1 soit un carré modulo p.
4) Soit un entier a non divisible par p, tel que a n'est pas un carré modulo p. Combien vaut $a^{\frac{p-1}{2}}$ modulo p ? On justifiera.

Exercice 2 : groupes et sous-groupes d'ordre premier (4 pts).

1) Soit G un groupe fini, dont l'élément neutre est noté e. On suppose que $G \neq \{e\}$ et que les seuls sous-groupes de G sont $\{e\}$ et G. Montrer que G est cyclique, puis que G est d'ordre premier.
2) Soit p un nombre premier, soit $n \in \mathbb{N}^*$, et soit G un groupe d'ordre p^n. En utilisant la première question, montrer que G contient un sous-groupe d'ordre p.

Exercice 3 : l'anneau des polynômes à valeurs entières (9 pts). On définit l'*anneau des polynômes à valeurs entières* :

$$A = \{f \in \mathbb{Q}[X] \mid \forall n \in \mathbb{Z}, f(n) \in \mathbb{Z}\}.$$

1) Montrer que A est un sous-anneau de $\mathbb{Q}[X]$.
2) Déterminer le groupe des inversibles de A.
3) Pour tout $k \in \mathbb{N}$ on pose

$$\binom{X}{k} = \frac{X(X-1)(X-2)\cdots(X-k+1)}{k!}.$$

(Par convention, $\binom{X}{0} = 1$.) Montrer que c'est un élément de A.

4) Soit $f \in A$ de degré $\leqslant n$. Montrer que f s'écrit de manière unique sous la forme

$$f = a_0 + a_1\binom{X}{1} + a_2\binom{X}{2} + \cdots + a_n\binom{X}{n}$$

avec $a_0, a_1, \ldots, a_n \in \mathbb{Z}$.
(Indication : montrer cette assertion avec les a_i dans $\mathbb{Q}$, puis montrer que les a_i sont dans $\mathbb{Z}$.)

5) Soit p un nombre premier, et soit I_p l'idéal de A engendré par les éléments $\binom{X}{k}$, pour $k \in \{1, \ldots, p-1\}$. Montrer que :

$$\binom{X}{p} \notin I_p.$$

(Remarque : cela montre que l'anneau A n'est pas noethérien puisqu'on a les inclusions strictes d'idéaux de A : $I_2 \subsetneq I_3 \subsetneq I_5 \subsetneq I_7 \subsetneq I_{11} \subsetneq I_{13} \subsetneq I_{17} \subsetneq \cdots$.)

6) Montrer que l'anneau A n'est pas factoriel.
(Indication : considérer les factorisations de l'élément $X(X-1)$.)