HAX501X – Groupes et anneaux 1

Examen terminal

Exercice 1 : le critère d'Euler. *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 :*

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

1) *Implication directe "$\Longrightarrow$".*

   a) *Rappeler la preuve vue en TD du petit théorème de Fermat comme application du théorème de Lagrange.*

   Soit p un nombre premier. On applique le théorème de Lagrange (pour l'ordre d'un élément) dans le groupe $(\mathbb{Z}/p\mathbb{Z})^\times = \{\overline{1}, \dots, \overline{p-1}\}$, qui est d'ordre $p-1$. Il dit que pour tout $\overline{x} \in (\mathbb{Z}/p\mathbb{Z})^\times$, on a $\overline{x}^{p-1} = \overline{1}$. En termes de congruences, cela veut dire que pour tout $x \in \mathbb{Z}$ qui n'est pas divisible par p, on a $x^{p-1} \equiv 1 \pmod{p}$.

   b) *Déduire du petit théorème de Fermat l'implication directe "$\Longrightarrow$".*

   Soit a un entier non divisible par p qui est un carré modulo p. Par définition, il existe donc $x \in \mathbb{Z}$ tel que $x^2 \equiv a \pmod{p}$. En mettant cette congruence à la puissance $\frac{p-1}{2}$ (qui est un entier car $p \neq 2$ donc p est impair) on obtient :

   $$x^{p-1} \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

   Or, par le petit théorème de Fermat, on a $x^{p-1} \equiv 1 \pmod{p}$, et donc on obtient bien que :

   $$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

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.*

   Soient $u, v \in (\mathbb{Z}/p\mathbb{Z})^\times$. On a les équivalences :

   $$\begin{aligned} u^2 = v^2 &\iff u^2 - v^2 = \overline{0} \\ &\iff (u-v)(u+v) = \overline{0} \\ &\iff u - v = \overline{0} \text{ ou } u + v = \overline{0} \\ &\iff u = v \text{ ou } u = -v. \end{aligned}$$

   Dans la troisième ligne on a utilisé le fait que $\mathbb{Z}/p\mathbb{Z}$ est un anneau intègre car p est premier.

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 $|E| = \frac{p-1}{2}$.*

Considérons la liste des u^2, pour tous les $u \in (\mathbb{Z}/p\mathbb{Z})^\times$. Cette liste est de longueur $p-1$, mais il y a des répétitions parce que $(-u)^2 = u^2$ pour tout u, et d'après la question précédente, c'est la seule source de répétitions. On note que $-u \neq u$ car $p \geqslant 3$, et donc chaque élément de la liste apparaît exactement 2 fois. Le nombre d'éléments distincts qui apparaissent dans la liste est donc $\frac{p-1}{2}$.
(Concrètement, E est égal à l'ensemble des $\overline{a}^2$, pour $a \in \{1, \dots, \frac{p-1}{2}\}$, et ces éléments sont deux à deux distincts.)

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 $|F| \leqslant \frac{p-1}{2}$.*

Considérons le polynôme $X^{\frac{p-1}{2}} - \overline{1}$ à coefficients dans $\mathbb{Z}/p\mathbb{Z}$, qui est de degré $\frac{p-1}{2}$. Comme p est premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps et donc par le cours, ce polynôme a au plus $\frac{p-1}{2}$ racines.

d) *Déduire des questions 1) et 2)b), 2)c) qu'on a l'égalité $E = F$. En déduire l'implication réciproque $\Longleftarrow$.*

La question 1) montre que $E \subset F$. Or les questions 2)b) et 2)c) impliquent que $|E| \geqslant |F|$. On a donc nécessairement $E = F$. L'inclusion $F \subset E$ est 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.*

Soit un nombre premier $p \neq 2$. Par le critère d'Euler, -1 est un carré modulo p si et seulement si $(-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Comme $(-1)^{\frac{p-1}{2}} = \pm 1$ et que $p \geqslant 3$, c'est équivalent à l'égalité $(-1)^{\frac{p-1}{2}} = 1$.
La valeur de $(-1)^{\frac{p-1}{2}}$ dépend de la parité de $\frac{p-1}{2}$, c'est-à-dire du reste de p dans la division euclidienne par 4. Concrètement :

$$(-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{si } p \equiv 1 \pmod{4}; \\ -1 & \text{si } p \equiv 3 \pmod{4}. \end{cases}$$

On en déduit que :

$$-1 \text{ est un carré modulo } p \iff p \equiv 1 \pmod{4}.$$

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.*

Par le petit théorème de Fermat on a $a^{p-1} \equiv 1 \pmod{p}$, et donc

$$\left(a^{\frac{p-1}{2}}\right)^2 \equiv 1 \pmod{p}.$$

Dans $\mathbb{Z}/p\mathbb{Z}$ cela s'écrit :

$$\left(\overline{a}^{\frac{p-1}{2}}\right)^2 = \overline{1},$$

ou encore :

$$\left(\overline{a}^{\frac{p-1}{2}} - \overline{1}\right)\left(\overline{a}^{\frac{p-1}{2}} + \overline{1}\right) = \overline{0}.$$

Comme p est premier, $\mathbb{Z}/p\mathbb{Z}$ est un anneau intègre, et on en déduit que

$$\overline{a}^{\frac{p-1}{2}} = \overline{1} \quad \text{ou} \quad \overline{a}^{\frac{p-1}{2}} = -\overline{1}.$$

Par hypothèse, a n'est pas un carré modulo p, donc le critère d'Euler implique que $\overline{a}^{\frac{p-1}{2}} \neq \overline{1}$, et donc $\overline{a}^{\frac{p-1}{2}} = -\overline{1}$. On en déduit que si a n'est pas un carré modulo p alors

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Exercice 2 : groupes et sous-groupes d'ordre premier.

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.*

▷ Comme $G \neq \{e\}$, il existe un élément $x \in G$ qui est différent de e. On considère le sous-groupe de G engendré par x, noté $\langle x \rangle$ comme dans le cours. Ce sous-groupe n'est pas $\{e\}$ car il contient x qui est différent de e. Comme les seuls sous-groupes de G sont $\{e\}$ et G, on en déduit que $\langle x \rangle = G$. Donc G est engendré par x, et est donc cyclique.

▷ Notons n l'ordre de G. Comme G est cyclique d'ordre n, on a par le cours que G a exactement un sous-groupe pour chaque diviseur positif de n. Concrètement, pour chaque diviseur positif d de n, on a le sous-groupe $\langle x^d \rangle$, qui est d'ordre $\frac{n}{d}$. Or, par hypothèse, G a exactement deux sous-groupes, et donc n a exactement deux diviseurs positifs. Donc n est 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.*

On prouve l'énoncé par récurrence forte sur n.

- Pour tout $n \in \mathbb{N}^*$, considérons l'assertion $P(n)$: "Tout groupe G d'ordre p^n contient un sous-groupe d'ordre p."
- Initialisation. $P(1)$ est vraie, car un groupe G d'ordre p se contient lui-même comme sous-groupe.
- Hérédité. Soit $n \geqslant 2$ tel que $P(1), \dots, P(n-1)$ sont vraies. Soit G un groupe d'ordre p^n. Comme p^n n'est pas premier car $n \geqslant 2$, la question précédente implique que G a un sous-groupe H qui n'est ni $\{e\}$ ni G. Par le théorème de Lagrange, l'ordre de H divise l'ordre de G. Comme p est premier, il existe donc $k \in \{1, \dots, n-1\}$ tel que $|H| = p^k$. En appliquant l'hypothèse de récurrence $P(k)$ au groupe H, on voit que H contient un sous-groupe K d'ordre p. Alors K est un sous-groupe de G d'ordre p.
- Conclusion : on a montré que $P(n)$ est vraie pour tout $n \in \mathbb{N}^*$.

Exercice 3 : l'anneau des polynômes à valeurs entières.

*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 $\mathbb{Q}[X]$.*

▷ Clairement, le polynôme nul 0 appartient à A.

- ▷ Soient $f, g \in A$. Alors pour tout $n \in \mathbb{Z}$, $f(n) \in \mathbb{Z}$ et $g(n) \in \mathbb{Z}$, et donc $(f+g)(n) = f(n) + g(n) \in \mathbb{Z}$. Donc $f + g \in A$.
- ▷ Soit $f \in A$. Alors pour tout $n \in \mathbb{Z}$, $f(n) \in \mathbb{Z}$, et donc $(-f)(n) = -f(n) \in \mathbb{Z}$. Donc $-f \in A$.
- ▷ Clairement, le polynôme unité 1 appartient à A.
- ▷ Soient $f, g \in A$. Alors pour tout $n \in \mathbb{Z}$, $f(n) \in \mathbb{Z}$ et $g(n) \in \mathbb{Z}$, et donc $(fg)(n) = f(n)g(n) \in \mathbb{Z}$. Donc $fg \in A$.

2) *Déterminer le groupe des inversibles de A.*

Soit $f \in A^\times$. Alors il existe $g \in A$ tel que $fg = 1$. Comme $\mathbb{Q}$ est un corps, on a alors $\deg(f) + \deg(g) = \deg(fg) = 0$, et donc $\deg(f) = \deg(g) = 0$, c'est-à-dire que f et g sont des polynômes constants. On écrit $f = a$ et $g = b$ avec $a, b \in \mathbb{Q}$. Or, $f, g \in A$ et donc notamment $f(0), g(0) \in \mathbb{Z}$, ce qui veut dire que $a, b \in \mathbb{Z}$. Comme $ab = 1$, on en déduit que $a = b = \pm 1$.
Conclusion : les seuls inversibles de A sont les polynômes 1 et -1, c'est-à-dire :

$$A^\times = \{1, -1\}.$$

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.

- ▷ Pour $n \in \mathbb{N}$, on a que $\binom{n}{k}$ est par définition un coefficient binomial, c'est un entier car c'est le nombre de parties à k éléments d'un ensemble à n éléments.
- ▷ Il faut aussi traiter le cas où n est négatif ! Pour $n = -m$ avec $m \in \mathbb{N}^*$, on calcule :

$$\begin{aligned}\binom{-m}{k} &= \frac{(-m)(-m-1)(-m-2)\cdots(-m-k+1)}{k!} \\ &= (-1)^k \frac{(m+k-1)(m+k-2)\cdots(m+1)m}{k!} \\ &= (-1)^k \binom{m+k-1}{k},\end{aligned}$$

qui est aussi un entier.

Conclusion : pour tout $n \in \mathbb{Z}$, $\binom{n}{k} \in \mathbb{Z}$. Donc $\binom{X}{k} \in A$.

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 $\mathbb{Z}$.)

Pour tout $k \in \{0, \ldots, n\}$, le polynôme $\binom{X}{k} \in \mathbb{Q}[X]$ est de degré k. Par le cours d'algèbre linéaire, ces polynômes forment donc une base de l'espace vectoriel des polynômes

de degré $\leqslant n$ à coefficients dans $\mathbb{Q}$. Donc il existe une unique famille de scalaires $a_0, a_1, \ldots, a_n \in \mathbb{Q}$ tels que

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

Il reste maintenant à montrer que les a_i sont dans $\mathbb{Z}$. On utilise le fait que comme $f \in A$, les évaluations $f(0), f(1), \ldots, f(n)$ sont dans $\mathbb{Z}$. Or :

- ▷ $f(0) = a_0$, donc $a_0 \in \mathbb{Z}$.
- ▷ $f(1) = a_0 + a_1$, donc $a_0 + a_1 \in \mathbb{Z}$. Comme $a_0 \in \mathbb{Z}$ par le point précédent, on en déduit que $a_1 \in \mathbb{Z}$.
- ▷ $f(2) = a_0 + 2a_1 + a_2$, donc $a_0 + 2a_1 + a_2 \in \mathbb{Z}$. Comme $a_0, a_1 \in \mathbb{Z}$ par les deux points précédents, on en déduit que $a_2 \in \mathbb{Z}$.
- ▷ Plus généralement, supposons qu'on a montré que $a_0, a_1, \ldots, a_{k-1} \in \mathbb{Z}$ pour un certain $k \in \{1, \ldots, n\}$. Alors en considérant $f(k)$, on voit que

$$a_0 + a_1\binom{k}{1} + a_2\binom{k}{2} + \cdots + a_{k-1}\binom{k}{k-1} + a_k \in \mathbb{Z},$$

et on en déduit que $a_k \in \mathbb{Z}$.

Ce raisonnement (qu'on pourrait écrire de manière plus propre sous la forme d'une récurrence) montre que $a_0, a_1, \ldots, a_n$ 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 : $I_2 \subsetneq I_3 \subsetneq I_5 \subsetneq I_7 \subsetneq I_{11} \subsetneq I_{13} \subsetneq I_{17} \subsetneq \cdots$.)

On procède par l'absurde, en supposant que $\binom{X}{p} \in I_p$. Il existe donc des éléments $f_1, \ldots, f_{p-1} \in A$ tels que

$$\binom{X}{p} = f_1\binom{X}{1} + \cdots + f_{p-1}\binom{X}{p-1}.$$

En évaluant en $X = p$, on obtient alors :

$$1 = f_1(p)\binom{p}{1} + \cdots + f_{p-1}(p)\binom{p}{p-1}.$$

Or, par le cours, $\binom{p}{k}$ est un multiple de p pour tout $k \in \{1, \ldots, p-1\}$. Comme de plus $f_k(p) \in \mathbb{Z}$ pour tout $k \in \{1, \ldots, p-1\}$ car $f_k \in A$, l'égalité précédente implique que 1 est un multiple de p, ce qui est absurde.
On a donc montré que $\binom{X}{p} \notin I_p$.

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

On a l'égalité dans A :

$$2\binom{X}{2} = X(X-1).$$

▷ L'élément $2 \in A$ est irréductible car il n'est pas inversible (par la question 2)) et que ses seuls factorisations sont de la forme $(\pm 1) \times (\pm 2)$. En effet, il est clair que les polynômes constants dans A sont nécessairement des entiers.

▷ Si l'anneau A était factoriel, on aurait existence et unicité de la décomposition en produit d'irréductibles dans A. Donc l'irréductible 2 devrait apparaître dans la décomposition en produit d'irréductibles de X ou de $X-1$, c'est-à-dire qu'on devrait avoir $2|X$ ou $2|X-1$ dans A. Ce n'est pas vrai, car $\frac{X}{2}$ et $\frac{X-1}{2}$ ne sont pas dans A. On en déduit que A n'est pas un anneau factoriel.