D.M. 9 : petit Fermat, versant théorie des groupes : solutions

1) Un théorème, dû à Lagrange, sur les sous-groupes d'un groupe fini :

a) *Méthode :*

Pour montrer que deux ensembles ont le même cardinal, on exhibe une bijection entre eux.

Soit $a \in G$. On considère l'application multiplication par a, $m_a : H \to G$, $x \mapsto ax$.

Pour chaque $a \in G$, par déf. de l'ensemble aH, l'ensemble image $m_a(H)$ est exactement aH.

Donc $m_a : H \to aH$ est surjective.

Montrons que m_a est injective : soit $(h, h') \in H^2$ tels que $a.h = a.h'$. Comme $(G, \cdot)$ est un groupe, on peut multiplier à gauche par a^{-1} dans cette égalité, ce qui donne : $h = h'$.

Ainsi $m_a : H \to aH$ est bijective et donc $\boxed{\mathrm{Card}(aH) = \mathrm{Card}(H).}$

b) Soient a et b deux éléments de G.

Méthode pour montrer une alternative A ou B :
on se place dans le cas où A n'est pas réalisée et on montre que B l'est.

Supposons que $aH \cap bH \neq \varnothing$. Soit $x \in aH \cap bH$.

Alors on a un couple $(h_1, h_2) \in H^2$ tel que $x = ah_1 = bh_2$.

Alors $a = bh_2h_1^{-1}$ et $h = h_2h_1^{-1} \in H$ car H est un sous-groupe de G, donc $a = bh \in bH$.

Comme $a = bh$ alors pour tout $h' \in H$, $ah' = bhh' \in bH$, ce qui entraine que $aH \subset bH$.

En échangeant les rôles de a et b dans ce qui précède, on obtient $bH \subset aH$. On conclut que $aH = bH$.

Ainsi si $aH \cap bH \neq \varnothing \Rightarrow aH = bH$.

Ce qui montre l'alternative $\begin{cases} aH \cap bH = \varnothing \text{ ou} \\ aH = bH. \end{cases}$

N.B. 1 si $aH \neq H$, alors aH n'est pas un sous-groupe de $(G, \cdot)$: par exemple, il ne contient pas le neutre. A fortiori, ce n'est pas le sous-groupe de G engendré par a !

N.B. 2 Le résultat qu'on vient de montrer est très général pour les *relations d'équivalences* : ici pour un sous-groupe H de $(G, \cdot)$ fixé, la relation $a\tilde{b} \overset{\text{def}}{\Leftrightarrow} \exists\, h \in H,\ a = bh$ est une *relation d'équivalence* appelée *relation d'équivalence à droite modulo* H. Les ensembles aH sont appelées les classes à droite modulo H.

Un exemple connu est le cas où $(G, \cdot) = (\mathbb{Z}, +)$ et H est le sous-groupe $n\mathbb{Z}$. La relation précédente est alors simplement la congruence modulo n et ici il n'est pas besoin de distinguer la droite de la gauche. Les classes modulo $n\mathbb{Z}$ sont : $n\mathbb{Z}$, $n\mathbb{Z} + 1$, $n\mathbb{Z} + 2$, jusqu'à $n\mathbb{Z} + (n - 1)$.

Le fait général est alors le suivant : pour toute relation d'équivalence sur un ensemble E, deux classes d'équivalences quelconques pour cette relation sont *disjointes ou confondues.* Ceci entraîne alors ce qu'on va expliquer au c) : on peut faire une *partition* de E (écriture de E comme une union disjointe de parties toutes non vides) à l'aide des ces classes d'équivalences. Nous rencontrerons d'autres exemples du même phénomène au chapitre sur les déterminants.

c) Comme pour tout $x \in G$, $x \in xH$ alors $G \subset \bigcup_{x \in G} xH$.

Mais comme tous les xH sont inclus dans G, on a l'égalité $G = \bigcup_{x \in G} xH$.

Par le b), les sous-ensembles xH sont deux à deux ou bien disjoints ou bien égaux.

En regroupant entre eux tous les xH qui sont égaux, on obtient que G peut s'écrire comme la réunion disjointe $G = a_1H \cup a_2H \cup \cdots \cup a_kH$.

d) La réunion disjointe du c) donne que $\mathrm{Card}(G) = \sum_{i=1}^{k} \mathrm{Card}(a_iH)$.

Mais par a), pour tout i, $\mathrm{Card}(a_iH) = \mathrm{Card}(H)$ donc $\mathrm{Card}(G) = \sum_{i=1}^{k} \mathrm{Card}(H) = k\,\mathrm{Card}(H)$.

On a obtenu le « théorème de Lagrange » :

$$\boxed{\text{si } H \text{ est un sous-groupe d'un groupe fini } (G,\cdot),\ \mathrm{Card}(H) \text{ divise toujours } \mathrm{Card}(G).}$$

N.B. Historiquement le résultat de Lagrange (1771) ne parlait pas de groupes (cette notion ne s'est dégagée pleinement que bien plus tard). Mais seulement du cas particulier des « groupes de permutations » qui pendant presque un siècle seront les groupes suscitant le plus d'intérêt. Lagrange faisait cette étude dans un mémoire sur la résolution des équations polynomiales de degré $3, 4$, et *plus de 5*.

2) Ordre d'un élément dans un groupe :

Soit $(G, .)$ un groupe fini, dont la loi est notée multiplicativement.

a) Comme $< a > \subset G$, en particulier, $< a >$ est fini comme sous-ensemble d'un ensemble fini.
On est donc sûr qu'il existe deux entiers $k_1 < k_2$ tels que $a^{k_1} = a^{k_2}$.
Alors $a^{k_2 - k_1} = e$, où e est le neutre de G.
Donc il existe bien un entier $k = k_2 - k_1 > 0$ tel que $a^k = e$. On peut donc définir k_0 comme le plus petit de ces entiers strictement positifs.

b) On fait un tableau des a^k pour $a \in \mathbb{Z}/7\mathbb{Z} \smallsetminus \{\bar{0}\}$:

k	$\bar{1}^k$	$\bar{2}^k$	$\bar{3}^k$	$\bar{4}^k$	$\bar{5}^k$	$\bar{6}^k$
1	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
2	$\bar{1}$	$\bar{4}$	$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{1}$
3	$\bar{1}$	$\bar{1}$	$\bar{6}$	$\bar{1}$	$\bar{6}$	$\bar{6}$
4	$\bar{1}$	$\bar{2}$	$\bar{4}$	$\bar{4}$	$\bar{2}$	$\bar{1}$
5	$\bar{1}$	$\bar{4}$	$\bar{5}$	$\bar{2}$	$\bar{3}$	$\bar{6}$
6	$\bar{1}$	$\bar{1}$	$\bar{1}$	$\bar{1}$	$\bar{1}$	$\bar{1}$

Le tableau montre que les ordres respectifs de $\bar{1}, \dots, \bar{6}$ sont $1, 3, 6, 3, 6, 2$.

c) Par prop. de k_0 =ord(a), la suite des (a^k) est périodique de période k_0, ce qui donne l'inclusion $< a > \subset \{a^k, k \in [\![0, k_0 - 1]\!]\}$. Ainsi $\mathrm{Card}(< a >) \leq k_0$ =ord(a).
Montrons l'inégalité inverse : si par l'absurde il existe $(k_1, k_2) \in \mathbb{N}^2$ vérifiant $0 \leq k_1 < k_2 < k_0$ vérifiant $a^{k_1} = a^{k_2}$ alors par le raisonnement du a), $a^{k_2 - k_1} = e$ avec $0 < k_2 - k_1 < k_0$ ce qui est en contradiction avec la déf. de k_0.
Donc $\{a^k, k \in [\![0, k_0 - 1]\!]\}$ est exactement de cardinal $k_0 = \mathrm{ord}(a)$.
N.B. Cette partie réciproque a été assez négligée sur les copies.

d) Soit $a \in G$, on considère $H =< a >$. Par le c), $\mathrm{Card}(H) = \mathrm{ord}(a)$.
Par le théorème de Lagrange du 1) d), on sait que $\mathrm{Card}(H) | \mathrm{Card}(G)$.
Ainsi $\mathrm{ord}(a) | \mathrm{Card}(G)$.

e) Soit $x \in G$ et $n = \mathrm{Card}(G)$. Alors par le d), on a un $k \in \mathbb{N}$ tel que $n = k.\mathrm{ord}(x)$.
Alors $x^n = (x^{\mathrm{ord}(x)})^k = e^k = e$.
On vient de montrer la propriété :

$$\boxed{\text{si } (G, .) \text{ est un groupe fini de cardinal } n, \text{ alors pour tout } x \in G, \text{ on a } x^n = e.}$$

3) Application : petit Fermat devient évident :

Soit p un nombre premier. Soit $G = \mathbb{Z}/p\mathbb{Z} \smallsetminus \{\bar{0}\}$ qu'on note aussi $\mathbb{Z}/p\mathbb{Z}^*$. Comme p est premier, $(G, \cdot)$ est un groupe. Par le résultat du 2) e), pour tout $x \in \mathbb{Z}/p\mathbb{Z}^*$, $x^{p-1} = \bar{1}$.

Donc en multipliant par x, pour tout $x \in \mathbb{Z}/p\mathbb{Z}^*$, $x^p = x$. Cette dernière égalité est aussi valable pour $x = \bar{0}$ trivialement, ce qui donne le petit théorème de Fermat.

Remarque : Avec celle du cours par récurrence à l'aide de la formule du binôme, cela nous fait deux démonstrations de ce théorème bien différentes. En fait, il en existe encore beaucoup d'autres et notamment des démonstrations purement *combinatoires* autrement dit *en comptant*, nous y reviendrons avec le chapitre de dénombrement.

4) Fonction φ d'Euler

Pour tout $n \in \mathbb{N}^*$, on note $\varphi(n)$ le nombre d'entiers $k \in [\![1,n]\!]$ tels que $k \wedge n = 1$.

a) Si p est premier, pour tout $k \in [\![1,p-1]\!]$, on a $k \wedge p = 1$, donc $\varphi(p) = p-1$.

b) **QdC :** Soit $k \in [\![1,n]\!]$. Alors :

$$\begin{aligned} k \wedge n = 1 &\Leftrightarrow \exists\,(u,v) \in \mathbb{Z}^2,\ ku + nv = 1,\\ &\Leftrightarrow \exists\, u \in \mathbb{Z},\ ku \equiv 1\,[n]\\ &\Leftrightarrow \exists\, \bar{u} \in \mathbb{Z}/n\mathbb{Z},\ \bar{k}\bar{u} = \bar{1},\\ &\Leftrightarrow \bar{k} \text{ est inversible dans } \mathbb{Z}/n\mathbb{Z}. \end{aligned}$$

Donc $\varphi(n)$ est aussi le nombre d'éléments inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z},+,\cdot)$.

c)

Prop. générale : Si $(A,+,\times)$ est un anneau alors l'ensemble $I(A)$ des éléments inversibles de A est toujours un groupe pour la multiplication.

Application de cette propriété ici :
Ici on considère $A = \mathbb{Z}/n\mathbb{Z}$ et $I(A)$ l'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$. Par la prop. précédente, $(I(A),\cdot)$ est un groupe de cardinal $\varphi(n)$.
Par la prop. du 2) e), pour tout $\bar{a} \in I(\mathbb{Z}/n\mathbb{Z})$ on a $\bar{a}^{\varphi(n)} = \bar{1}$.
Autrement dit (par b)), pour tout $a \in \mathbb{Z}$ tel que $a \wedge n = 1$, $a^{\varphi(n)} \equiv 1\,[n]$.

Preuve de la propriété : • La multiplication est une l.c.i. de $I(A)$ car si a et b sont inversibles, on sait que ab est inversible d'inverse $b^{-1}a^{-1}$.
• La multiplication est associative dans A, en part. dans $I(A)$.
• Le neutre 1 est inversible donc dans $I(A)$.
• Si a est dans $I(A)$, son inverse $b = a^{-1}$ est inversible d'inverse a, donc $b \in I(A)$.

d) Vu le a), ce résultat généralise le théorème de Fermat du 3).

5) Retour dans le très concret

a) Soit $n = 3^{1000}$. On veut la classe de n modulo 100.
(M1) On applique le théorème de Fermat-Euler
Comme $3 \wedge 100 = 1$, ce théorème s'applique et on sait donc que $3^{\varphi(100)} \equiv 1\,[100]$.
Le problème est de calculer $\varphi(100) = \varphi(2^2 \times 5^2)$. Les nombres entre 1 et 100 premiers avec 100 seront les nombres impairs qui ne se terminent pas par 5 : il y en a 50 (les impairs) moins 10 (les nombres qui se terminent par 5) donc $\varphi(100) = 40$ et donc $3^{40} \equiv 1\,[100]$.
Comme $1000 = 40 \times 25$, $3^{1000} \equiv (3^{40})^{25} \equiv 1^{25} \equiv 1\,[100]$.
(M2) On commence par remarquer que $100 = 4 \times 25$ **et on applique le théorème chinois**
Par le théorème Chinois, il est équivalent de connaître la classe de n modulo 4 et modulo 25.
• La classe modulo 4 est immédiate : $3 \equiv -1\,[4] \Rightarrow 3^{1000} \equiv (-1)^{1000} = 1\ [4]$ (1).
• Cherchons la classe modulo $25 = 5^2$: pour cela, on peut utiliser la formule d'Euler. On a $\varphi(5^2) = 5^2 - 5 = 20$.
Donc comme $3 \wedge 25 = 1$, on a par le théorème d'Euler $3^{\varphi(25)} \equiv 1\,[25]$. Donc $3^{20} \equiv 1\,[25]$.
Comme $1000 = 20 \times 50$ on a $3^{1000} \equiv 1\,[25]$ (2).
Avec (1) et (2) et le théorème chinois, on obtient finalement que $n \equiv 1[100]$ autrement dit les deux derniers chiffres de n sont 01.
b) Cette fois la **(M1)** du a) ne s'applique pas puisque 2 et 100 ne sont pas premiers entre eux. En revanche la **(M2)** s'applique, autrement dit on peut utiliser le théorème chinois pour travailler modulo 25 et modulo 4.
• Pour la classe modulo 4 : $2^2 \equiv 0\,[4] \Rightarrow 2^{1000} \equiv 0\,[4]$ (1). Notons qu'ici la formule d'Euler ne s'applique pas, mais ce n'est pas grave.

• Pour la classe modulo 25 : comme au b), comme $2 \wedge 25 = 1$, on sait par théorème d'Euler que $2^{\varphi(25)} \equiv 1\,[25]$ donc que $2^{20} \equiv 1\,[25]$. A fortiori $2^{1000} \equiv 1\;[25]$ (2).

Ensuite, si on a bien digéré la cuisine chinoise : vu (1) et (2) on cherche l'unique $a \in [\![0,99]\!]$ tel que $a \equiv 1\,[25]$ et $a \equiv 0\,[4]$.

Il suffit de tester modulo 4 les quatre représentants de 1 modulo 25 à savoir $1, 26, 51, 76$ et c'est 76 qui convient.

Ainsi $\begin{cases} a \equiv 1\,[25], \\ a \equiv 0\,[4] \end{cases} \Leftrightarrow \begin{cases} a \equiv 76\,[25], \\ a \equiv 76\,[4] \end{cases} \Leftrightarrow a \equiv 76\;[100]$ la dernière équivalence étant vraie car $25 \wedge 4 = 1$.

Ainsi $2^{1000} \equiv 76\,[100]$ c'est-à-dire que les deux derniers chiffres cherchés sont 76.

Remarque : si on n'utilise pas la formule d'Euler, on peut quand même tout calculer « à la main sans machine ».

Pour cela, on regarde à la main les puissances de 2 modulo 25, on a, *en multipliant par* 2 *et en réduisant modulo* 25 *à chaque étape* :

$2, 4, 8, 16, 32 \equiv 7[25], 14$ puis $28 \equiv 3, 6, 12, 24 \equiv -1$ i.e. $2^{10} \equiv -1\,[25]$ et on retrouve donc que $2^{20} \equiv 1[25]$. Mieux ce calcul montre que l'élément $\overline{2}$ est exactement d'ordre 20 le groupe $I(\mathbb{Z}/25\mathbb{Z})$.