DM n°1 – Algèbre 1

Hugo Salou
Dept. Informatique

ENS DE LYON

3 octobre 2024

Exercice 1.

1. Afin de montrer que l'application $\alpha : \bar{k} \mapsto \bar{k} \cdot (g_0, \ldots, g_{p-1})$ est une action, nous devons montrer deux propriétés :
   - ▷ L'application α est un morphisme de groupe. En effet, pour un élément $x = (g_0, \ldots, g_{p-1}) \in X$, on a

$$\begin{aligned}\big(\alpha(-\bar{\ell}) \circ \alpha(\bar{k})\big)(x) &= \alpha(\overline{-\ell})(g_k, \ldots, g_{p+k-1}) \\ &= (g_{k-\ell}, \ldots, g_{p+k-\ell-1}) \\ &= \alpha(\bar{k} - \bar{\ell})(x)\end{aligned}$$

.

   - ▷ Pour $\bar{k} \in \mathbb{Z}/p\mathbb{Z}$, l'application $f_{\bar{k}} x \mapsto \alpha(\bar{k})(x)$ est une bijection. En effet, l'application $g_{\bar{k}} : x \mapsto \alpha(-\bar{k})(x)$ vérifie l'égalité $g_{\bar{k}} \circ f_{\bar{k}} = f_{\bar{k}} \circ g_{\bar{k}} = \mathrm{id}_X$. Autrement dit, $f_{\bar{k}}$ est bijective.

   On en déduit que α est bien une action de groupe.
2. a) Soit $x = (g_0, \ldots, g_{p-1}) \in X$. On sait que $\operatorname{Stab} x \leq \mathbb{Z}/p\mathbb{Z}$. Ainsi, par le théorème de Lagrange, on a $\#\operatorname{Stab} x \in \{1, p\}$ car p premier. On a donc deux cas à considérer.
      - ▷ Si $\#\operatorname{Stab} x = p$, alors on a un sous-groupe de $\mathbb{Z}/p\mathbb{Z}$ de même cardinal, d'où $\operatorname{Stab} x = \mathbb{Z}/p\mathbb{Z}$. Et, les éléments $x = (g_0, \ldots, g_{p-1})$ qui vérifient la condition sur le cardinal du stabilisateur sont les $x = (g_0, \ldots, g_0)$ qui vérifient ${g_0}^p = e$. Ainsi, ce sont les éléments d'ordre p, ou l'identité.
      - ▷ Sinon $\#\operatorname{Stab} x = 1$, et alors le stabilisateur est un sous-groupe de $\mathbb{Z}/p\mathbb{Z}$ de cardinal 1, c'est donc le groupe trivial $\{\bar{0}\}$.

b) On applique la formule des classes

$$\#X = \sum_{x \in G} \frac{\#(\mathbb{Z}/p\mathbb{Z})}{\#(\mathrm{Stab}\ x)}.$$

D'une part, on dénombre $\#X = \#G^{p-1}$ car $(g_0, \ldots, g_{p-2})$ détermine entièrement l'élément g_{p-1} pour que $(g_0, \ldots, g_{p-1}) \in X$.

D'autre part, on peut disjoindre les cas en fonction de l'élément $x \in G$:

- ▷ soit x est d'ordre p et alors $\#\mathrm{Stab}\ x = p$ (il y en a $\mathrm{ord}_p(G)$) ;
- ▷ soit x est l'élément neutre et alors $\#\mathrm{Stab}\ x = p$ (il y en a 1) ;
- ▷ sinon, on a $\#\mathrm{Stab}\ x = 1$.

On en déduit

$$\#G^{p-1} = (1 + \mathrm{ord}_p G) \cdot \frac{p}{p} + p \cdot \#x \in G \mid \#\mathrm{Stab}\ x = 1,$$

d'où par passage modulo p,

$$\#G^{p-1} \equiv 1 + \mathrm{ord}_p G \pmod p.$$

3. On procède en deux temps.

- ▷ D'une part, si $p \mid \#G$, alors $\mathrm{ord}_p G \equiv -1 \pmod p$, il a donc au moins un élément d'ordre p.
- ▷ D'autre part, si G a un élément d'ordre p, alors $p \mid \#G$, car l'ordre d'un élément divise l'ordre du groupe.

D'où l'équivalence.

Exercice 2.

1. Soit G un groupe abélien. Alors,

$$[g,h] = ghg^{-1}g^{-1} = gg^{-1}hh^{-1} = e,$$

pour deux éléments $g, h \in G$. On en déduit que $D(G) = \{e\}$ le groupe trivial.

2. On sait que $D(G)$ est un sous-groupe. Soit $x \in G$. Montrons que $xD(G)x^{-1} = D(G)$.

On calcule, pour $g, h \in G$:

$$x[g,h]x^{-1} = \overbrace{xgx^{-1}}\,\overbrace{xhx^{-1}}\,\overbrace{xg^{-1}x^{-1}}\,\overbrace{xh^{-1}x^{-1}} = [xgx^{-1}, xhx^{-1}].$$

On sait que l'application $y \mapsto xyx^{-1}$ est un isomorphisme d'où l'égalité

$$xD(G)x^{-1} = \langle x[g,h]x^{-1}\rangle_{g,h\in G} = \langle [xgx^{-1}, xhx^{-1}]\rangle_{g,h\in G} = D(G).$$

On en déduit que $D(G)$ est un sous-groupe distingué de G.

3. On calcule

$$gh = ghg^{-1}h^{-1}hg = [g,h]hg.$$

D'où, $G/D(G)$ est abélien.

4. Soit A un groupe abélien, et soient $x, g, h \in G$. On a

$$\varphi(x[g,h]) = \varphi(x)\cdot\varphi(g)\,\varphi(h)\,\varphi(g)^{-1}\,\varphi(h)^{-1} = \varphi(x).$$

Ainsi, on en déduit que l'application

$$\begin{aligned} \bar{\varphi} : \quad G^{\mathrm{ab}} &\longrightarrow A \\ x\,D(G) &\longmapsto \varphi(x). \end{aligned}$$

est bien définie. De plus, c'est bien un morphisme car φ l'est.

5. Soit $H \triangleleft G$ tel que G/H est abélien. Ainsi, pour deux éléments quelconques $g, h \in G$, on a $ghH = hgH$ donc $ghg^{-1}h^{-1} \in H$, et on en déduit que $D(G) \subseteq H$ car $D(G)$ est engendré par les commutateurs.

6. On construit l'isomorphisme

$$\begin{aligned} \Phi : G^* &\longrightarrow (G^{\mathrm{ab}})^* \\ \varphi &\longmapsto \bar{\varphi}, \end{aligned}$$

où l'application $\bar{\varphi}$ est définie en question 4. (On peut l'appliquer car $\mathbb{C}^\times$ est un groupe abélien). Vue la définition précédente de $\bar{\varphi}$, l'application Φ est un morphisme. Montrons que Φ est un isomorphisme.

- ▷ D'une part, Φ est injective. En effet, soit $\psi \in \ker \Phi$. Ainsi, on a $\bar{\psi} = 0$, ce qui implique que $\psi = 0$ (sinon un élément d'image non nul impliquerai, après passage au quotient, une image non nulle).
- ▷ D'autre part, Φ est surjective. En effet, pour $\bar{\varphi} \in (G^{\mathrm{ab}})^*$, on pose $\psi = \pi \circ \varphi$, où $\pi : G \to G/D(G)$ est la projection canonique. On a bien $\bar{\psi} = \bar{\varphi}$ car l'application φ passe au quotient.

D'où l'isomorphisme.

Exercice 3.

1. Soient $x, y, z, x', y,', z' \in \mathbb{Z}/p\mathbb{Z}$. On calcule

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & x' & y' \\ 0 & 1 & z' \\ 0 & 0 & 0 \end{pmatrix} = \cdot \begin{pmatrix} 1 & x + x' + 0 & y + y' + xz' \\ 0 & 1 & z + z' + 0 \\ 0 & 0 & 1 \end{pmatrix},$$

d'où

$$h(x, y, z) \cdot h(x', y', z') = h(x + y', y + y' + xz', z + z').$$

De plus, $\mathrm{I}_3 = h(\bar{0}, \bar{0}, \bar{0})$. Aussi, $\det h(x, y, z) = 1 \neq 0$, la matrice admet donc un inverse. Finalement, on remarque que

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & -x & -y + xz \\ 0 & 1 & -z \\ 0 & 0 & 1 \end{pmatrix} = \mathrm{I}_3,$$

d'où $h(x, y, z)^{-1} = h(-x, -y + xz, -z)$.

Ainsi, G est bien un sous-groupe de $\mathrm{GL}_3(\mathbb{Z}/p\mathbb{Z})$.

2. a) On procède par récurrence pour montrer la formule pour $n \in \mathbb{N}$ et $-n \in \mathbb{N}$.
   - ▷ On a $h(x, y, z)^0 = h(0, 0, 0) = \mathrm{I}_3$.
   - ▷ On a

$$\begin{aligned} h(x, y, z)^{n+1} &= h(x, y, z)^n \cdot h(x, y, z) \\ &= h\left(nx + x, ny + \frac{n(n-1)}{2}xz + y + xz, nz + z\right) \\ &= h\left((n+1)x, (n+1)y + \frac{(n+1)n}{2}xz, (n+1)z\right) \end{aligned}$$

.

- On a

$$\begin{aligned} h(x,y,z)^{-(n+1)} &= h(x,y,z)^{-n} \cdot h(x,y,z)^{-1} \\ &= h\left(-nx - x, -ny + \frac{n(n-1)}{2}xz - y + xz, -nz - z\right) \\ &= h\left(-(n+1)x, -(n+1)y + \frac{(n+1)n}{2}xz, -(n+1)z\right) \end{aligned}$$

.

On en conclut par récurrence.

b) Soit p premier impair. Soient $x, y, z \in \mathbb{Z}/p\mathbb{Z}$. On cherche le plus petit $k \in \mathbb{N}$ tel que $h(x,y,z)^k = h(\bar{0},\bar{0},\bar{0})$, ce qui est vrai si et seulement si $kx = \bar{0}$ et $ky + k(k-1)xz/2 = \bar{0}$ et $kz = \bar{0}$. On procède à une disjonction de cas.

- Si $x = y = z = \bar{0}$ alors, l'ordre de $h(x,y,z)$ est 1.
- Si $y \neq x = z = \bar{0}$ alors, par primalité de p et imparité de p, l'ordre de $h(x,y,z)$ est p.
- Sinon ($x \neq \bar{0}$ ou $z \neq \bar{0}$), alors par primalité de p, l'ordre de $h(x,y,z)$ est p.

c) Soit p premier pair, donc $p = 2$. On procède à tous les cas : il n'y a que 8 éléments dans G.

- L'ordre de $h(\bar{0},\bar{0},\bar{0})$ est 1.
- L'ordre de $h(\bar{0},\bar{0},\bar{1})$ est 2.
- L'ordre de $h(\bar{0},\bar{1},\bar{0})$ est 2.
- L'ordre de $h(\bar{0},\bar{1},\bar{1})$ est 2.
- L'ordre de $h(\bar{1},\bar{0},\bar{0})$ est 2.
- L'ordre de $h(\bar{1},\bar{0},\bar{1})$ est 4.
- L'ordre de $h(\bar{1},\bar{1},\bar{0})$ est 2.
- L'ordre de $h(\bar{1},\bar{1},\bar{1})$ est 4.

3. On calcule l'ensemble

$$Z(G) = \{\, A \in G \mid \forall B \in G, AB = BA \,\}.$$

On pose $A = h(x,y,z)$ et $B = h(x',y',z')$ deux éléments de G. On a $AB = BA$ si et seulement si $xz' = zx'$ (les autres conditions sont symétriques et ont des opérations commutatives). La contrainte que A commute pour tout B implique que $x = 0 = z$. D'où,

$$Z(G) = \{\, h(0, y, 0) \mid y \in \mathbb{Z}/p\mathbb{Z} \,\}.$$

4. Soient $A, B \in G$. On calcule

$$[A, B] = ABA^{-1}B^{-1} = h(0, \underbrace{xz' - x'z}_{c}, 0).$$

On en déduit que $D(G) = \{h(0, c, 0) \mid c \in \mathbb{Z}/p\mathbb{Z}\}$. On remarque que $D(G) = Z(G)$.

5. On a

$$G/D(G) \cong \{\, h(x, \bar{0}, z) \mid x, z \in \mathbb{Z}/p\mathbb{Z} \,\} \cong (\mathbb{Z}/p\mathbb{Z})^2.$$

Fin du DM.