LES MATHÉMATIQUES AUX CONCOURS X-Mines-Centrale

MP/MP* MPI/MPI*

En 300 énoncés d'oraux et 100 thèmes classiques pour les écrits et les oraux

Florent Nicaise
Philippe Lauron

ellipses

1

Arithmétique, groupes et anneaux

► CLASSIQUE 1 **Action d'un groupe sur un ensemble, Burnside et Cayley**

Soient $(G,*)$ un groupe et E un ensemble. Une action de groupe *de G sur E est la donnée d'un morphisme de groupes θ de $(G,*)$ dans $(S(E),\circ)$ (groupe des bijections de $E \to E$). On notera pour $(g,x) \in G \times E$: $g \cdot x = \big(\theta(g)\big)(x) \in E$. On définit :*

$\Omega(x) = \{g{\cdot}x, g \in G\}$ *(orbite de x) et* $\mathrm{Stab}(x) = \{g \in G, g{\cdot}x = x\}$ *(stabilisateur de x).*

a) Prouver que : $\forall (g,g',x,y) \in G^2 \times E^2, g{\cdot}(g'{\cdot}x) = (g{*}g'){\cdot}x$ *et* $g{\cdot}x = y \iff x = g^{-1}{\cdot}y$.

b) Démontrer que : $\forall (x,y) \in E^2, \Omega(x) \cap \Omega(y) = \emptyset$ *ou* $\Omega(x) = \Omega(y)$.

c) Soit $x \in E$, démontrer que $\mathrm{Stab}(x)$ *est un sous-groupe de G.*

d) On suppose ici que G est fini. Prouver que $\mathrm{card}(\Omega(x)) \times \mathrm{card}(\mathrm{Stab}(x)) = \mathrm{card}(G)$.

e) On suppose ici que G et E sont finis. On définit le fixateur *de $g \in G$ par* $\mathrm{Fix}(g) = \{x \in E, g{\cdot}x = x\}$. *Soit p le nombre d'orbites distinctes sous l'action de G. Prouver la* formule de Burnside *:*

$$p = \frac{1}{\mathrm{card}(G)} \sum_{g \in G} \mathrm{card}\left(\mathrm{Fix}(g)\right).$$

f) Prouver que l'application $\theta : g \mapsto (x \mapsto g * x * g^{-1})$ définit une action de groupe de G sur lui-même, appelée action par conjugaison.

g) Soit S_n l'ensemble des permutations de $[\![1\ ;\ n]\!]$ (pour $n \geqslant 1$). Décrire l'orbite d'une permutation de S_n pour l'action de lui-même par conjugaison.

h) On note $n = \mathrm{card}(G)$: prouver le théorème de Cayley *: $(G,*)$ est isomorphe à un sous-groupe de S_n.*

► **Une correction**

a) Soit $(g,g',x,y) \in G^2 \times E^2$, alors :

$$g \cdot (g' \cdot x) = (\theta(g))\big((\theta(g'))(x)\big) = \big((\theta(g)) \circ (\theta(g'))\big)(x) = \big(\theta(g * g')\big)(x) = (g * g') \cdot x$$

en utilisant la propriété de morphisme de θ. De plus :

$$g \cdot x = y \Longrightarrow (g^{-1}) \cdot (g \cdot x) = g^{-1} \cdot y \Longrightarrow (g^{-1} * g) \cdot x = g^{-1} \cdot y \Longrightarrow n_G \cdot x = g^{-1} \cdot y.$$

Or, $\theta(n_G) = Id_E$ par conservation du neutre via un morphisme, donc :
$n_G \cdot x = Id_E(x) = x = g^{-1} \cdot y$.

b) • On peut prouver les choses de manière ensembliste, mais ce principe de partionnement de E par les $\Omega(x)$ peut inciter à introduire une relation d'équivalence, en l'occurrence :

$$\forall (x,y) \in E^2, x \mathscr{R} y \iff \exists g \in G, g \cdot x = y.$$

➢ elle est réflexive : $x \mathscr{R} x$ en prenant $g = n_G$ (neutre de G) (on a vu que $n_G \cdot x = x$ au a)) ;

➢ elle est symétrique car :

$$x \mathscr{R} y \iff \exists g \in G, g \cdot x = y \Longrightarrow x = g^{-1} \cdot y \Longrightarrow y \mathscr{R} x$$

par la a) ;

➢ elle est transitive car, si $x = g \cdot y$ et $y = g' \cdot z$, $x = g \cdot (g' \cdot z) = (g * g') \cdot z$.

• Par définition, $\Omega(x)$ est la classe d'équivalence de x pour $\mathscr{R}$: il s'ensuit que ces classes d'équivalence partitionnent G, ce qui implique le résultat.

c) Clairement, $\mathrm{Stab}(x) \subset G$ et $Id_E \in \mathrm{Stab}(x)$ car on a vu que $n_G \cdot x = x$. Soient g et g' dans $\mathrm{Stab}(x)$. Alors $(g * g') \cdot x = g \cdot (g' \cdot x) = g \cdot x = x$, donc $\mathrm{Stab}(x)$ est stable par composition. De plus on a vu que $g \cdot x = x$ donne $x = g^{-1} \cdot x$ donc $\mathrm{Stab}(x)$ est stable par inversion. On en déduit que $\mathrm{Stab}(x)$ est un sous-groupe de $(G, \circ)$.

d) • Notons :

$$f : \left| \begin{array}{ccc} G & \longrightarrow & \Omega(x) \\ g & \longmapsto & g \cdot x \end{array} \right.$$

f est clairement surjective. Soit $y = g \cdot x \in \Omega(x)$, comptons ses antécédents g' par f : $f(g') = g \cdot x$ ssi $g \cdot x = g' \cdot x$ c'est-à-dire $x = (g^{-1} * g') \cdot x$ soit $g^{-1} * g' = g'' \in \mathrm{Stab}(x)$. L'ensemble des antécédents de $g \cdot x$ est

$$g\,\mathrm{Stab}(x) = \{g * g'', g'' \in \mathrm{Stab}(x)\},$$

image de $\mathrm{Stab}(x)$ par la bijection $g'' \mapsto g * g''$ (d'inverse $g'' \mapsto g^{-1} * g''$). Ainsi, chaque $y = g \cdot x \in \Omega(x)$ possède exactement $\mathrm{card}(\mathrm{Stab}(x))$ antécédents par f donc :

$$\forall y \in \Omega(x), \mathrm{card}\left(f^{-1}(\{y\})\right) = \mathrm{card}(\mathrm{Stab}(x)).$$

• Les $f^{-1}(\{y\})$, lorsque y décrit $\Omega(x)$, partitionnent G :

$$G = \bigcup_{y \in \Omega(x)} f^{-1}(\{y\}) \quad \text{donc} \quad \mathrm{card}(G) = \sum_{y \in \Omega(x)} \mathrm{card}(f^{-1}(\{y\})) = \mathrm{card}(\Omega(x)) \times \mathrm{card}(\mathrm{Stab}(x)).$$

e) Puisque E est fini, il est partitionné en p orbites distinctes $\Omega_1, \ldots, \Omega_p$. La fonction indicatrice $\mathbb{1}_P$ d'une proposition P vaut 1 si la proposition est vérifiée, 0 sinon, ce qui permet d'écrire en utilisant Fubini pour les sommes finies :

$$\sum_{g \in G} \mathrm{card}\,(\ \mathrm{Fix(g)}\ ) = \sum_{g \in G} \sum_{x \in E} \mathbb{1}_{(g \cdot x = x)} = \sum_{x \in E} \sum_{g \in G} \mathbb{1}_{(g \cdot x = x)} = \sum_{x \in E} \mathrm{card}\,(\ \mathrm{Stab(x)}\ )\,.$$

On utilise la question d), qui prouve en particulier que le cardinal du stabilisateur est constant le long d'une orbite Ω_i, en regroupant les termes de la somme précédente suivant les Ω_i et avec la question b) :

$$\sum_{g \in G} \mathrm{card}\,(\ \mathrm{Fix(g)}\ ) = \sum_{i=1}^{p} \sum_{x \in \Omega_i} \frac{\mathrm{card}(G)}{\mathrm{card}(\Omega_i)} = \mathrm{card}(G) \left(\sum_{i=1}^{p} \sum_{x \in \Omega_i} \frac{1}{\mathrm{card}(\Omega_i)} \right) = p \times \mathrm{card}(G),$$

d'où le résultat.

f) Observons que, si g et g' sont dans G, on a pour tout $x \in G$:

$$\big(\theta(g) \circ \theta(g')\big)(x) = g * (g' * x * (g')^{-1}) * g^{-1} = (g * g') * x * (g * g')^{-1} = \big(\theta(g * g')\big)(x).$$

Ceci prouve que l'on a bien un morphisme de $(G, *)$ dans $(S(G), *)$.

g) • Commençons par remarquer que deux cycles de même longueur sont conjugués, effectivement si $c = (a_1 \quad \ldots \quad a_p)$ est un cycle et $\sigma \in S_n$ alors on peut montrer que :

$$\sigma \circ c \circ \sigma^{-1} = (\sigma(a_1) \quad \ldots \quad \sigma(a_p)) \qquad (*).$$

Pour cela on note f le membre de gauche, g celui de droite, soit $i \in [\![1\ ;\ n]\!]$.

➢ **Cas 1 :** $i \in \{\sigma(a_1), \dots, \sigma(a_p)\}$, on note $i = \sigma(a_j)$. On montre que $f(i) = \sigma(a_{j+1}) = g(i)$ (en notant $a_{p+1} = a_1$).

➢ **Cas 2 :** sinon i est invariant par f comme g.

D'où l'égalité d'applications $f = g$. En choisissant bien σ, tout p-cycle est donc conjugué à tout autre p-cycle. L'orbite d'un p-cycle par l'action de conjugaison est donc l'ensemble des p-cycles.

• Soit $\tau \in S_n$, elle se décompose en un produit commutatif de cycles de supports disjoints $\tau = c_1 \circ \cdots \circ c_p$. Définissons son *caractère* comme la suite $(\ell_1, \dots, \ell_p)$ des longueurs des cycles $c_1, \dots, c_p$ dans l'ordre décroissant. Par exemple, le caractère de la permutation :

$$(1 \quad 2 \quad 3)\,(4 \quad 5 \quad 6)\,(7 \quad 8)$$

est $(3, 3, 2)$. Remarquons que :

$$\sigma \circ \tau \circ \sigma^{-1} = (\sigma \circ c_1 \circ \sigma^{-1}) \circ \dots (\sigma \circ c_p \circ \sigma^{-1}) = c_1' \circ \cdots \circ c_p' = \tau',$$

où c_i' se déduit de c_i comme dans $(*)$. On remarque que l'on obtient une permutation de caractère identique à celui de τ. Réciproquement, pour toute permutation τ' ayant le même caractère que τ, on peut construire σ tel que $\tau' = \sigma \circ \tau \circ \sigma^{-1}$ (on définit σ par ses restrictions aux supports des cycles). En conclusion, l'orbite d'une permutation τ est l'ensemble des permutations ayant le même caractère que τ.

h) Nous allons définir l'action d'un groupe *par translation* sur lui-même, définie par :

$$\theta : \left| \begin{array}{ccc} G & \longrightarrow & S(G) \\ g & \longmapsto & (x \mapsto g * x) \end{array} \right. .$$

Elle est bien définie car les $x \mapsto g * x$ sont des bijections (inverse : $x \mapsto g^{-1} * x$). De même qu'à la question précédente, on peut prouver que $\theta(g * g') = \theta(g) \circ \theta(g')$, nous avons donc une action de groupe. θ est injective car si $g \in \mathrm{Ker}(\theta)$:

$$\theta(g) = Id_G \Longrightarrow \forall x \in G, g * x = x \Longrightarrow g = n_G$$

par le choix $x = n_G$. L'application

$$\left| \begin{array}{ccc} (G, *) & \longrightarrow & (\mathrm{Im}(\theta), \circ) \\ g & \longmapsto & \theta(g) \end{array} \right.$$

est donc un isomorphisme de groupe donc G est isomorphe à un sous-groupe de $S(G)$. Ayant $(S(G), \circ)$ et $(S_n, \circ)$ isomorphes (il suffit de numéroter les éléments de G), on peut conclure.

► Classique 2 — *Réduction d'une équation diophantienne modulo 7*

Donner les $(x, y, z) \in \mathbb{Z}^3$ tels que :

$$(E) : x^2 + y^2 = 7z^2.$$

► Une correction

• *Analyse.* Si (x, y, z) convient, on passe aux classes dans $\mathbb{Z}/7\mathbb{Z}$:

$$\overline{x}^2 + \overline{y}^2 = \overline{0}. \qquad (*)$$

Remarquons que, lorsque $\overline{x}$ décrit $\mathbb{Z}/7\mathbb{Z}$, $\overline{x}^2$ décrit l'ensemble $I = \{\overline{0}, \overline{1}, \overline{2}, \overline{4}\}$. Après un examen exhaustif, la seule possibilite pour que a, b soient dans I et $a + b = \overline{0}$ est que $a = b = \overline{0}$. Ainsi :

$$(*) \Longrightarrow (\overline{x} = \overline{y} = \overline{0}).$$

On peut noter $x = 7x'$ et $y = 7y'$ pour x', y' entiers. En revenant à (E) :

$$(49((x')^2 + (y')^2) = 7z^2) \Longrightarrow (7(7((x')^2 + (y')^2) - z^2) = 0) \Longrightarrow (7((x')^2 + (y')^2) = z^2)$$

par intégrité dans $\mathbb{Z}$, donc z est divisible par 7, on peut noter $z = 7z'$. Un retour à (E) donne que :

$$(x')^2 + (y')^2 = 7(z')^2.$$

Nous avons obtenu que, si (x, y, z) est une solution de (E) dans $\mathbb{Z}^3$, alors $(x/7, y/7, z/7)$ aussi. En itérant, $(x/7^n, y/7^n, z/7^n)$ est dans $\mathbb{Z}^3$ pour tout $n \in \mathbb{N}$. Supposons par l'absurde que $x \neq 0$ et notons $v \in \mathbb{N}$ sa valuation en 7 dans la décomposition de x en facteurs premiers. On a obtenu que $x/7^{v+1} \in \mathbb{Z}$, donc 7^{v+1} divise x, ce qui contredit la définition de la valuation. Donc $x = 0$, et de même $y = z = 0$.

- *Synthèse.* Réciproquement, le triplet $(0, 0, 0)$ est une solution triviale de (E).
- *Conclusion.* L'ensemble des solutions de (E) est réduit au singleton $\{(0, 0, 0)\}$.

► CLASSIQUE 3 **Structure de groupe quotient par un sous-groupe distingué**

Soit $(G, *)$ un groupe. On dit qu'un sous-groupe H est distingué *si et seulement si :*

$$\forall x \in G, xH = Hx,$$

en notant $xH = \{x * h, h \in H\}$ et $Hx = \{h * x, h \in H\}$.

a) Montrer que la relation : $x\mathscr{R}y \iff y^{-1} * x \in H$ est une relation d'équivalence sur G, et que xH est la classe de x. On notera $G/H = \{xH, x \in G\}$ l'ensemble des classes d'équivalence de $\mathscr{R}$, appelé ensemble quotient.

b) Prouver le théorème de Lagrange [a] *: si G est fini, le cardinal d'un sous-groupe divise le cardinal de G et*

$$\mathrm{card}(G/H) \times \mathrm{card}(H) = \mathrm{card}(G).$$

c) Montrer que le centre de G*, défini par $Z(G) = \{y \in G, \forall x \in G, x * y = y * x\}$, est un sous-groupe distingué.*

d) Soit $f : (G, *) \to (G', \bullet)$ un morphisme de groupes. Montrer que $\mathrm{Ker}(f)$ est un sous-groupe distingué de G.

e) A partir de maintenant, on suppose que H est un sous-groupe distingué. Prouver que cette définition de la loi $\star$ sur G/H a un sens :

$$\forall (xH, yH) \in (G/H)^2, (xH) \star (yH) = (x * y)H.$$

f) Montrer que $(G/H, \star)$ est un groupe, appelé groupe quotient *de G par H.*

g) On suppose que $(G/Z(G), \star)$ est monogène, prouver que $(G, *)$ est abélien.

h) Soit $f : (G, *) \to (G', \bullet)$ un morphisme de groupes. On définit :

$$\widetilde{f} : \left| \begin{array}{ccc} (G/\mathrm{Ker}(f), \star) & \longrightarrow & (\mathrm{Im}(f), \bullet) \\ x\,\mathrm{Ker}(f) & \longmapsto & f(x) \end{array} \right. .$$

Montrer que $\widetilde{f}$ est bien définie et que c'est un isomorphisme. En déduire que, si G est fini :

$$\mathrm{card}(G) = \mathrm{card}(\mathrm{Ker}(f))\,\mathrm{card}(\mathrm{Im}(f)).$$

a. La version au programme ne considère que le cas où H est cyclique.

▶ **Remarque :** nous verrons à l'exercice 32 page 50 un exemple d'application de la structure quotient aux p-groupes.

▶ **Une correction**

a) • On a :

➢ *Réflexivité :* $x^{-1} * x = n_G \in H$ (car H est un sous-groupe) ;

➢ *Symétrie :* $x\mathscr{R}y \Longrightarrow y^{-1} * x \in H$ donc, puisque H est stable par inversion : $\left(y^{-1} * x\right)^{-1} = x^{-1} * y \in H$. D'où $y\mathscr{R}x$;

➢ *Transitivité :* si $y^{-1} * x \in H$ et $z^{-1} * y \in H$, par stabilité : $(z^{-1} * y) * (y^{-1} * x) = z^{-1} * x \in H$ donc $x\mathscr{R}z$.

• Soit $x \in G$, y est dans la classe de x si et seulement si $x\mathscr{R}y$ c'est-à-dire :

$$\exists h \in H, y^{-1} * x = h \Longleftrightarrow \exists h \in H, y = x * h^{-1}.$$

La fonction $h \mapsto h^{-1}$ étant une bijection de $H \to H$, on a bien y dans la classe de x si et seulement si $y \in xH$.

b) G étant fini, il est partitionné en p classes d'équivalences notées x_1H, $\ldots x_pH$, donc $p = \text{card}(G/H)$ et :

$$G = \bigcup_{i=1}^{p} x_iH \quad \text{donc} \quad \text{card}(G) = \sum_{i=1}^{p} \text{card}(x_iH).$$

Observons que l'application $h \in H \mapsto x * H \in xH$ est une bijection (d'inverse $h \mapsto x^{-1} * h$). Ainsi, $\text{card}(x_iH) = \text{card}(H)$ pour tout i donc

$$p \times \text{card}(H) = \text{card}(G) \quad \text{donc} \quad \text{card}(G/H) \times \text{card}(H) = \text{card}(G).$$

c) Soit $x \in G$, on a directement par définition du centre que $xZ(G) = Z(G)x$.

d) Soit $x \in G$, par propriété des morphismes de groupes : $f(x^{-1}) = (f(x))^{-1}$. L'application

$$\left|\begin{array}{ccc} \text{Ker}(f) & \longrightarrow & \text{Ker}(f) \\ h & \longmapsto & x * h * x^{-1} \end{array}\right.$$

est donc bien définie, c'est une bijection (d'inverse $h \mapsto x^{-1} * h * x$), donc :

$$\{x * h * x^{-1}, h \in \text{Ker}(f)\} = \text{Ker}(f).$$

On en déduit par double inclusion que $x\,\text{Ker}(f) = \text{Ker}(f)x$ pour tout x, donc $\text{Ker}(f)$ est distingué.

e) La définition de $\star$ dépend a priori du choix de deux réprésentants dans xH et yH, nous allons vérifier qu'en fait elle n'en dépend pas. Soient $x' \in xH$ et $y' \in yH$, donc il existe h_1, h_2 dans H tels que $x' = x * h_1$ et $y' = y * h_2$. Ainsi $x' * y' = x * (h_1 * y) * h_2$. On a $h_1 * y \in Hy = yH$ (vu H distingué) donc il existe $h_3 \in H$ tel que $h_1 * y = y * h_3$, donc :

$$x' * y' = (x * y) * (h_3 * h_2) \in (x * y)H.$$

Ainsi, $(x'H * y'H)\mathscr{R}(xH * yH)$ donc les classes d'équivalences sont égales : $(x' * y')H = (x * y)H$, donc on a bien démontré que $(x'H) \star (y'H) = (xH) \star (yH)$.

f) Déjà, $\star$ est une loi de composition interne sur G/H. De plus, pour tout (xH, yH, zH) dans $(G/H)^3$:

$$xH \star (yH \star zH) = xH \star ((y * z)H) = (x * (y * z))H = ((x * y) * z))H = (xH \star yH) \star zH.$$

Si $xH \in G/H$, par définition : $(xH) \star (H) = (xH) \star (n_GH) = (x * n_G)H = xH$, ce prouve que H est un neutre pour $(G/H, \star)$. Ayant ceci, on prouve facilement que $x^{-1}H$ est l'inverse de xH pour $\star$, ce qui achève de montrer que $(G/H, \star)$ est un groupe.

g) Soit $(x,y) \in G^2$. Comme $G/Z(G)$ est monogène, il existe une classe notée $aZ(G)$ qui engendre les autres, d'où l'existence de k_1 dans $\mathbb{Z}$ tel que :

$$(x*y)Z(G) = (aZ(G))^{k_1} = a^{k_1}Z(G),$$

la première puissance est au sens de $\star$ et la seconde de $*$. Comme $x*y \in (x*y)Z(G)$, il existe donc $z_1 \in Z(G)$ tel que : $x*y = a^{k_1} * z_1$. De même il existe un entier k_2 et $z_2 \in Z(G)$ tels que $y*x = a^{k_2} * z_2$. On peut alors vérifier, les z_i étant dans le centre, que :

$$x*y = y*x = a^{k_1+k_2} * z_1 * z_2,$$

d'où le résultat.

h) • La bonne définition de f consiste à vérifier que l'image d'une classe ne dépend pas du choix d'un représentant de cette classe, c'est-à-dire que si $x' \in x\operatorname{Ker}(f)$ alors $f(x') = f(x)$. Notons $x' = x*k$ avec $k \in \operatorname{Ker}(f)$, comme f est un morphisme alors :

$$f(x') = f(x) \bullet f(k) = f(x) \bullet n_{G'} = f(x),$$

d'où la bonne définition.

• Montrons que $\widetilde{f}$ est un morphisme. Soient x, y dans G. Alors par définition de $\star$ et $\widetilde{f}$:

$$\begin{aligned} & \widetilde{f}((x\operatorname{Ker}(f)) * (y\operatorname{Ker}(f)) = \widetilde{f}((x*y)\operatorname{Ker}(f)) \\ = \quad & f(x*y) = f(x) \bullet f(y) = \widetilde{f}(x\operatorname{Ker}(f)) \bullet \widetilde{f}(y\operatorname{Ker}(f)). \end{aligned}$$

• Montrons que $\widetilde{f}$ est surjectif : soit $y \in \operatorname{Im}(f)$ et x tel que $f(x) = y$, par définition de $\widetilde{f}$: $\widetilde{f}(x\operatorname{Ker}(f)) = f(x) = y$, d'où la surjectivité.

• Pour l'injectivité, soit $x\operatorname{Ker}(f) \in \operatorname{Ker}(\widetilde{f})$: alors $f(x) = n_{G'}$ donc $x \in \operatorname{Ker}(f)$, donc $x\operatorname{Ker}(f) = \operatorname{Ker}(f)$ par double inclusion, or $\operatorname{Ker}(f)$ est le neutre de $(G/H, \star)$, donc $\widetilde{f}$ est injective.

• La relation sur les cardinaux découle directement du caractère bijectif de $\widetilde{f}$ et de la question b).

► CENTRALE 4 ***Un théorème de Legendre dans un groupe abélien***

On veut montrer le résultat suivant : si $(G,*)$ est un groupe fini abélien et p un facteur premier de $\operatorname{card}(G)$, alors il existe un élément d'ordre p.

a) Justifier qu'il existe $r \in \mathbb{N}^*$ et $x_1, \ldots, x_r$ dans G tels que :

$$G = \langle \{x_1, \ldots, x_r\} \rangle$$

(la notation $\langle \cdot \rangle$ désigne le sous-groupe engendré par une partie).

b) Conclure en utilisant l'application :

$$\varphi : \left| \begin{array}{ccc} \langle x_1 \rangle \times \cdots \times \langle x_r \rangle & \longrightarrow & G \\ (x_1^{k_1}, \ldots, x_r^{k_r}) & \longmapsto & x_1^{k_1} * \cdots * x_r^{k_r} \end{array} \right. .$$

► **Une correction**

a) On peut tout simplement prendre $r = \operatorname{card}(G)$ et pour les x_i les éléments de G.

b) • Cette application est surjective par la définition de x_i.

• Mettons la loi produit, notée $\cdot$, sur le groupe de départ $G' = \langle x_1\rangle \times \cdots \times \langle x_r\rangle$, comme G est abélien, on a :

$$\begin{aligned}\varphi\left((x_1^{k_1},\dots,x_r^{k_r})\cdot(x_1^{k'_1},\dots,x_r^{k'_r})\right) &= \varphi\left((x_1^{k_1+k'_1},\dots,x_r^{k_r+k'_r})\right)\\ &= x_1^{k_1+k'_1} * \cdots * x_r^{k_r+k'_r}\\ &= x_1^{k_1} * x_2^{k_2} * \cdots * x_{r-1}^{k'_{r-1}} * x_r^{k'_r}\\ &= \varphi\left((x_1^{k_1},\dots,x_r^{k_r})\right) * \varphi\left((x_1^{k'_1},\dots,x_r^{k'_r})\right).\end{aligned}$$

• Soit $y \in \mathrm{Im}(\varphi)$, soit $x' \in G'$ tel que $\varphi(x') = y$. Alors x'' est un antécédent du même y si et seulement si , par les propriétés d'un morphisme de groupe : $\varphi(x') = \varphi(x'')$, c'est-à-dire $\varphi((x')^{-1}\cdot x'') = n_G$ (neutre de G). On en déduit l'ensemble des antécédents de y par φ :

$$\varphi^{-1}(\{y\}) = \{x'\cdot k, k \in \mathrm{Ker}(\varphi)\}.$$

Cet ensemble est l'image de $\mathrm{Ker}(\varphi)$ par la bijection $y \in G' \mapsto x'\cdot y \in G'$ (d'inverse $y \mapsto (x')^{-1}\cdot y$) donc :

$$\forall y \in \mathrm{Im}(\varphi), \mathrm{card}\left(\varphi^{-1}(\{y\})\right) = \mathrm{card}(\mathrm{Ker}(\varphi)).$$

Ces images réciproques partitionnent G', c'est-à-dire :

$$\begin{aligned}G' = \bigcup_{y\in\mathrm{Im}(\varphi)} \varphi^{-1}(\{y\}) \quad\Longrightarrow\quad \mathrm{card}(G') &= \sum_{y\in\mathrm{Im}(\varphi)} \mathrm{card}(\mathrm{Ker}(\varphi))\\ &= \mathrm{card}(\mathrm{Im}(\varphi))\times\mathrm{card}(\mathrm{Ker}(\varphi)) = \mathrm{card}(G)\times\mathrm{card}(\mathrm{Ker}(\varphi)).\end{aligned}$$

Comme G' est le groupe produit des $\langle x_i\rangle$ de cardinal $o(x_i)$ (ordre de x_i) :

$$\prod_{i=1}^{r}\mathrm{card}(\langle x_i\rangle) = \prod_{i=1}^{r} o(x_i) = \mathrm{card}(G)\times\mathrm{card}(\mathrm{Ker}(\varphi)) \qquad (*)$$

Comme p divise $\mathrm{card}(G)$ il divise le produit de gauche or p est premier, par Euclide il existe i tel que $p/o(x_i)$ donc il existe $q \in \mathbb{N}^*$ tel que $o(x_i) = pq$. On vérifie que $o(x_i^q) = p$, x_i^q est donc un élément d'ordre p.

► MINES 5 ***Une question de divisibilité***

Montrer que pour tout $n \in \mathbb{N}$, 19 divise $2^{2^{6n+2}} + 3$.

► Une correction

Pour $n \in \mathbb{N}$, on pose $p_n = 2^{2^{6n+2}} + 3$ et $\mathscr{P}(n)$ la propriété : « 19 divise p_n ».

Procédons par récurrence sur $\mathbb{N}$.

• *Initialisation :* $p_0 = 19$ donc $\mathscr{P}(0)$ est vraie.

• *Hérédité :* supposons $\mathscr{P}(n)$ vraie pour un $n \in \mathbb{N}$ et montrons $\mathscr{P}(n+1)$. On écrit,

$$\begin{aligned}p_{n+1} &= 2^{2^{6n+8}} + 3 = 2^{2^{6n+2}\times 2^6} + 3\\ &= \left(2^{2^{6n+2}}\right)^{2^6} + 3 = (p_n - 3)^{2^6} + 3\end{aligned}$$

Comme $p_n \equiv 0\,[19]$, on a $p_n - 3 \equiv -3\,[19]$ ainsi, $(p_n-3)^{2^6} \equiv 3^{2^6}\,[19]$. Cependant, $3^4 \equiv 5\,[19]$ donc $3^{2^3} \equiv 6\,[19]$ puis $3^{2^4} \equiv -2\,[19]$, et $3^{2^5} \equiv 4\,[19]$, enfin $3^{2^6} \equiv -3\,[19]$. On en déduit que $(p_n-3)^{2^6} + 3 \equiv 0\,[19]$ donc $p_{n+1} \equiv 0\,[19]$. La récurrence est établie.