Groupes

Thomas Dedieu

Rentrée 2019, compilé le 22 novembre 2019

Avertissement. Ceci n'est pas un polycopié de cours. Ce texte est constitué de mes notes personnelles pour un cours de préparation à l'agrégation, grossièrement mises en forme. Néanmoins, si vous trouvez des erreurs il m'intéresse que vous me les communiquiez.

Exercices propédeutiques

Exercice 1. Donner des exemples de :
— groupes abéliens finis non-cycliques ;
— groupes monogènes non-cycliques ;
— groupes abéliens infinis non-monogènes ;
— groupes infinis non-abéliens.

Exercice 2. Montrer que $\mathbf{Z}^2$ n'est pas monogène. En déduire que $\mathbf{Z}^2$ et $\mathbf{Z}$ sont deux groupes non-isomorphes. Sont-ils isomorphes en tant qu'ensembles ?

Exercice 3. 1) Démontrer le théorème de Lagrange : soit G un groupe fini. Pour tout sous-groupe $H < G$, l'ordre de H divise l'ordre de G.

2) En déduire le théorème d'Euler : soit $n > 0$ un entier. Pour tout entier x premier avec n, on a

$$x^{\varphi(n)} \equiv 1 \mod n,$$

où $\varphi(n) = \mathrm{Card}\{i \in [\![1, n]\!] : \mathrm{pgcd}(i, n) = 1\}$ est la *fonction indicatrice d'Euler*.

3) En déduire le petit théorème de Fermat : pour tout entier p premier, et tout entier a, on a $a^p \equiv a \mod p$.

Exercice 4. 1) Soit G un groupe, $K \triangleleft G$ un sous-groupe distingué. Montrer que l'ensemble quotient G/K est muni d'une structure de groupes canoniquement induite par la structure de groupe de G. Montrer que l'application $x \in G \mapsto \bar{x} \in G/K$ est un morphisme de groupes.

2) Soit $\phi : G \to H$ un morphisme de groupes. Montrer que le noyau $K = \ker(\phi)$ est un sous-groupe distingué de G. Montrer que ϕ induit un morphisme injectif $G/K \to H$.

3) Soit G un groupe, $K \triangleleft G$ un sous-groupe distingué. Soit H un groupe, et $\phi : G \to H$ un morphisme. On suppose que $\phi(K) = \{1_H\}$. Montrer qu'il existe un unique morphisme de groupes $\bar{\phi} : G/K \to H$ tel que $\phi = \bar{\phi} \circ \pi$, où π est le morphisme canonique $G \to G/K$.

4) Soit G un groupe. On considère

$$D(G) = \langle aba^{-1}b^{-1},\ a, b \in G \rangle$$

(sous-groupe *dérivé* de G).
a) Montrer que $D(G)$ est un sous-groupe distingué de G, et que le groupe quotient $G^{\mathrm{ab}} := G/D(G)$ est abélien.
b) Soit M un groupe abélien, $\phi : G \to M$ un morphisme de groupes. Montrer qu'il existe un unique morphisme $\bar{\phi} : G^{\mathrm{ab}} \to M$ tel que $\phi = \bar{\phi} \circ \pi$, où π est le morphisme canonique $G \to G^{\mathrm{ab}}$.

Exercice 5. Donner un morphisme de $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/17\mathbf{Z}$ dans $\mathrm{GL}_n(\mathbf{C})$.

Exercice 6. 1) Démontrer que tout sous-groupe de $\mathbf{Z}$ est monogène. Exhiber un sous-groupe de $\mathbf{R}$ qui n'est pas monogène.

2) Soit $a, b \in \mathbf{Z}$. Démontrer que

$$a\mathbf{Z} + b\mathbf{Z} = \mathrm{pgcd}(a, b)\mathbf{Z} \quad \text{et} \quad a\mathbf{Z} \cap b\mathbf{Z} = \mathrm{ppcm}(a, b)\mathbf{Z}.$$

3) a) Démontrer le théorème de Bezout : deux entiers a et b sont premiers entre eux si et seulement si il existe $u, v \in \mathbf{Z}$ tels que $au + bv = 1$.
b) Soit $d \in \mathbf{Z}$. Est-il vrai que $\text{pgcd}(a, b) = d$ si et seulement si il existe $u, v \in \mathbf{Z}$ tels que $au + bv = d$?

4) Soit a et b deux entiers. On note $d = \text{pgcd}(a, b)$ et $m = \text{ppcm}(a, b)$.
a) Montrer qu'il existe $a', b' \in \mathbf{Z}$ tels que $a = da'$ et $b = db'$.
b) Montrer que $m = ab' = a'b$.
c) Montrer que $md = ab$.

Exercice 7. 1) Démontrer que $\mathbf{Z}/n\mathbf{Z}$ est un corps si et seulement si n est un nombre premier.

2) Montrer que 18 est inversible pour la multiplication dans $\mathbf{Z}/55\mathbf{Z}$, et déterminer son inverse.

3) a) Soit $x = \bar{a} \in \mathbf{Z}/n\mathbf{Z}$. On note $d = \text{pgcd}(a, n)$. Montrer que $\langle x \rangle$ (le sous-groupe de $\mathbf{Z}/n\mathbf{Z}$ engendré par x) est égal à $\langle \bar{d} \rangle$.
b) Déterminer le sous-groupe engendré par 1038 dans $\mathbf{Z}/1\,000\,000\mathbf{Z}$.

4) Déterminer tous les générateurs du groupe additif $\mathbf{Z}/24\mathbf{Z}$.

5) Montrer que l'ensemble des éléments non nuls de $\mathbf{Z}/19\mathbf{Z}$ constitue un groupe pour la multiplication. Vérifier que ce groupe est cyclique, et trouver tous ses générateurs.

Exercice 8. Soit $a, b \in \mathbf{Z}$.

1) Déterminer le noyau du morphisme de groupes (ou d'anneaux)

$$n \in \mathbf{Z} \mapsto (n \bmod a, n \bmod b) \in \mathbf{Z}/a\mathbf{Z} \times \mathbf{Z}/b\mathbf{Z}.$$

En déduire qu'il existe un morphisme injectif $\mathbf{Z}/\text{ppcm}(a, b)\mathbf{Z} \to \mathbf{Z}/a\mathbf{Z} \times \mathbf{Z}/b\mathbf{Z}$.

2) Si a et b sont premiers entre eux, déduire de la question précédente qu'il existe un isomorphisme $\mathbf{Z}/ab\mathbf{Z} \cong \mathbf{Z}/a\mathbf{Z} \times \mathbf{Z}/b\mathbf{Z}$. (*Indication* : utiliser un argument de cardinalité).

3) On suppose a et b premiers entre eux, et on considère $u, v \in \mathbf{Z}$ tels que $au + bv = 1$. Montrer que l'application

$$(\bar{x}, \bar{y}) \in \mathbf{Z}/a\mathbf{Z} \times \mathbf{Z}/b\mathbf{Z} \mapsto xbv + yau \in \mathbf{Z}/ab\mathbf{Z}$$

est bien définie, et que c'est un morphisme de groupes (d'anneaux en fait). Vérifier que ce morphisme est l'inverse du morphisme $\mathbf{Z}/ab\mathbf{Z} \cong \mathbf{Z}/a\mathbf{Z} \times \mathbf{Z}/b\mathbf{Z}$ des questions précédentes.

4) On ne suppose plus a et b premiers entre eux, et on considère leurs décompositions en produits de facteurs irréductibles : soit $p_1, \ldots, p_r$ des nombres premiers deux à deux distincts, et $a_1, \ldots, a_r, b_1, \ldots, b_r \in \mathbf{N}$ tels que $a = p_1^{a_1} \cdots p_r^{a_r}$ et $b = p_1^{b_1} \cdots p_r^{b_r}$ (certains des b_i ou a_i peuvent être nuls).
a) Montrer que

$$\mathbf{Z}/a\mathbf{Z} \times \mathbf{Z}/b\mathbf{Z} \cong \left(\mathbf{Z}/p_1^{a_1}\mathbf{Z} \times \cdots \times \mathbf{Z}/p_r^{a_r}\mathbf{Z}\right) \times \left(\mathbf{Z}/p_1^{b_1}\mathbf{Z} \times \cdots \times \mathbf{Z}/p_r^{b_r}\mathbf{Z}\right)$$

b) En déduire que $\mathbf{Z}/a\mathbf{Z} \times \mathbf{Z}/b\mathbf{Z} \cong \mathbf{Z}/\text{pgcd}(a, b)\mathbf{Z} \times \mathbf{Z}/\text{ppcm}(a, b)\mathbf{Z}$.

Exercice 9. Déterminer la signature de la permutation σ, ainsi que σ^{10000} dans les cas suivants :
(i) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & 1 & 5 & 2 & 4 & 6 & 3 \end{pmatrix}$;
(ii) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 11 & 5 & 7 & 12 & 10 & 3 & 6 & 4 & 2 & 1 & 9 & 8 \end{pmatrix}$;
(iii) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 8 & 5 & 3 & 9 & 1 & 7 & 6 & 4 \end{pmatrix}$.

Exercice 10. Soient $n \in \mathbf{N}^*$, $\sigma \in \mathfrak{S}_n$, $a_1, a_2, \ldots, a_k$ k éléments deux à deux distincts de $[\![1, n]\!]$. Montrer que

$$\sigma \circ [a_1, a_2, \ldots, a_k] \circ \sigma^{-1} = [\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_k)].$$

Exercice 11. 1) Déterminer tous les sous-groupes des groupes symétriques $\mathfrak{S}_3$ et $\mathfrak{S}_4$. Lesquels sont des sous-groupes distingués ?

2) Déterminer un morphisme non constant du groupe $\mathfrak{S}_4$ dans le groupe $\mathfrak{S}_3$.

3) Vérifier que le groupe alterné $\mathfrak{A}_5$ possède deux sous-groupes isomorphes à $\mathfrak{A}_4$ et $\mathbf{Z}/5\mathbf{Z}$ respectivement, et tels que l'application de multipliciation

$$(\sigma', \sigma'') \in \mathfrak{A}_4 \times \mathbf{Z}/5\mathbf{Z} \mapsto \sigma' \circ \sigma'' \in \mathfrak{A}_5$$

réalise une bijection. Les groupes $\mathfrak{A}_4 \times \mathbf{Z}/5\mathbf{Z}$ et $\mathfrak{A}_5$ sont-ils isomorphes ?

4) Vérifier l'existence des suites de sous-groupes distingués suivantes :
a) $\{1\} = \mathfrak{A}_2 \lhd \mathfrak{S}_2 \cong \mathbf{Z}/2\mathbf{Z}$;
b) $\{1\} \lhd \mathfrak{A}_3 = \mathbf{Z}/3\mathbf{Z} \lhd \mathfrak{S}_3$;
c) $\{1\} \lhd \mathbf{Z}/2\mathbf{Z} \lhd V_4 \lhd \mathfrak{A}_4 \lhd \mathfrak{S}_4$ (V_4 est le groupe de Klein $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$).

Exercice 12. On considère le plan euclidien orienté $\mathbf{E}^2$, muni d'un repère orthonormal direct. On note pour tout $\alpha \in \mathbf{R}/(2\pi\mathbf{Z})$, r_α la rotation vectorielle d'angle α, et pour tout $\gamma \in \mathbf{R}/(\pi\mathbf{Z})$, s_γ la réflexion orthogonale par rapport à la droite D_γ formant un angle γ avec l'axe des abscisses.
1) Montrer que $R : \alpha \in \mathbf{R}/(2\pi\mathbf{Z}) \mapsto r_\alpha \in \mathrm{GL}(\mathbf{E})$ est un morphisme de groupes. Montrer que l'image de R est le noyau du morphisme $\det : u \in \mathrm{O}(\mathbf{E}) \mapsto \det(u) \in \mathbf{R}$. En déduire que l'image de R est un sous-groupe distingué de $\mathrm{O}(\mathbf{E})$. Est-ce un sous-groupe distingué de $\mathrm{GL}(\mathbf{E})$?

2) a) Soit $\gamma, \gamma' \in \mathbf{R}/(\pi\mathbf{Z})$. Montrer que $s_{\gamma'} \circ s_\gamma = r_{2(\gamma'-\gamma)}$. Faire un dessin.
b) L'ensemble $\mathbf{R}/(\pi\mathbf{Z})$ des réflexions orthogonales est contenu dans $\mathrm{GL}(E)$. L'injection correspondante $\mathbf{R}/(\pi\mathbf{Z}) \to \mathrm{GL}(\mathbf{E})$ est-elle un morphisme de groupes ?

3) Calculer $r_\alpha \circ s_\gamma$ et $s_\gamma \circ r_\alpha$ pour tout $\alpha \in \mathbf{R}/(2\pi\mathbf{Z})$ et $\gamma \in \mathbf{R}/(\pi\mathbf{Z})$. (*Indication* : écrire $r_\alpha = s_{\alpha/2+\gamma} \circ s_\gamma$ et $r_\alpha = s_\gamma \circ s_{\gamma-\alpha/2}$).

4) Soit $\alpha \in \mathbf{R}/(2\pi\mathbf{Z})$, $\gamma, \gamma' \in \mathbf{R}/(\pi\mathbf{Z})$. Vérifier les relations (faire des dessins) :
a) $s_\gamma r_\alpha s_\gamma = r_{-\alpha}$;
b) $r_\alpha s_\gamma r_{-\alpha} = s_{\gamma+\alpha}$;
c) $s_\gamma s_{\gamma'} s_\gamma^{-1} = s_{2\gamma-\gamma'}$ (réflexion orthogonale par rapport à la droite $s_\gamma(D_{\gamma'})$.

5) On considère l'ensemble D_4 à huit éléments

$$D_4 = \{r_0, r_{\pi/2}, r_\pi, r_{3\pi/2}, s_0, s_{\pi/4}, s_{\pi/2}, s_{3\pi/2}\}.$$

a) Montrer que D_4 est le groupe des isométries du carré formé des points d'affixe une racine 4-ème de l'unité dans l'identification $E^2 \cong \mathbf{C}$ donnée par le choix de notre repère.
b) On note $r = r_{\pi/2}$ et $s = s_0$. Montrer que

$$D_4 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}.$$

c) Montrer que D_4 est le groupe donné par générateurs et relations

$$\langle \mathsf{r}, \mathsf{s} : \mathsf{s}^2 = \mathsf{r}^4 = \mathsf{srsr} = 1 \rangle.$$

d) Déterminer les cinq classes de conjugaison de D_4.
e) Déterminer tous les sous-groupes de D_4. Lesquels sont distingués ?

I – Groupes opérant sur un ensemble

Slogan. « Un groupe c'est fait pour agir. »

1 – Définitions

1.1 – Actions de groupes

(1.1) Définition. G groupe, X ensemble. G agit à gauche sur X ($G \circlearrowleft X$) si [...]

Remarque. Chaque $\hat{g}$ est automatiquement une bijection.
(1.1.1) De manière équivalente, on veut un morphisme de groupes $G \to \mathrm{Bij}(X)$.

(1.2) Exemples. $\mathrm{GL}(E) \circlearrowleft E$ (telle quelle pas très intéressante en fait), $(E,+) \circlearrowleft \mathbf{A}_E$.
$\mathfrak{S}_n \circlearrowleft \{1,\dots,n\}$.
On en verra plein d'autres.

(1.3) Une action est *fidèle* si seul $1 \in G$ agit comme l'identité.

On peut toujours se ramener à une action fidèle en remplaçant G par le noyau du morphisme $G \to \mathfrak{S}(X)$ — qui est toujours un sous-groupe distingué ; on l'appelle le *noyau de l'action.*

(1.4) Une action est *transitive* si pour tous $x, y \in X$, il existe $g \in G$ tel que $y = g.x$.
Exemples. $E \circlearrowleft \mathbf{A}_E$ est transitive, $\mathrm{GL}(E) \circlearrowleft E$ non (il y a deux orbites, $\{0\}$ et $E \setminus \{0\}$, qui ne se ressemblent pas beaucoup). $\mathrm{PGL}_{n+1} \circlearrowleft \mathbf{P}^n$ est transitive.

(1.5) Plus généralement, pour $k \in \mathbf{N}$, une action $G \circlearrowleft X$ est k-transitive si [...]
Exemple. $\mathfrak{S}_n$ agit n-transitivement sur $\{1,\dots,n\}$. $\mathfrak{A}_n$ agit $(n-2)$-transitivement :

$$\begin{pmatrix} x_1 & \cdots & x_{n-2} & x_{n-1} & x_n \\ y_1 & \cdots & y_{n-2} & y_{n-1} & y_n \end{pmatrix} \quad \text{ou} \quad \begin{pmatrix} x_1 & \cdots & x_{n-2} & x_n & x_{n-1} \\ y_1 & \cdots & y_{n-2} & y_n & y_{n-1} \end{pmatrix}$$

convient ; en revanche $\mathfrak{A}_n \circlearrowleft \{1,\dots,n\}$ n'est pas $(n-1)$-transitive (remarque : dans ce cas, c'est équivalent à la n-transitivité).

1.2 – Orbites et partitions

(1.6) Définition. Pour $x \in X$, l'orbite $\omega(x)$ est $\{g.x : g \in G\}$.
Exemple. Action du groupe des rotations $(\mathbf{R}/2\pi\mathbf{Z}, +)$ sur $\mathbf{R}^2$.

(1.7) Proposition. $X = \coprod_{G\backslash X} \omega$.
Preuve. (i) $\omega_1 \neq \omega_2 \Rightarrow \omega_1 \cap \omega_2 = \emptyset$.
(ii) $x \in \omega(x)$. □

On peut aussi regarder la relation d'équivalence « être transporté l'un sur l'autre par l'action ».

2 – Groupe agissant sur lui-même

2.1 – Action par conjugaison

(2.1) $g.h = ghg^{-1}$.
Attention : $g^{-1}hg$ définit une action *à droite*.

(2.2) Principe de conjugaison.
(2.2.1) Exemple. Si p est la projection sur F dans la direction de G, $u \circ p \circ u^{-1}$ est la projection sur $u(F)$ dans la direction de $u(G)$.

Pour $f = \lambda_1 p_1 + \cdots + \lambda_s p_s$, on a donc [...]. Idem pour une décomposition de Dunford–Jordan.
(2.2.2) Exemple. Dans $\mathfrak{S}_n$, $\sigma\big(1, \ldots, k\big)\sigma^{-1} = \big(\sigma(1), \ldots, \sigma(k)\big)$.
(2.2.3) Lien avec la formule de changement de base.

2.2 – Action par multiplication et quotient

(2.3) $g.h = gh$ action $G \circlearrowleft G$ à gauche.

Quotient par un sous-groupe

(2.4) $H < G$ sous-groupe quelconque. H agit *à droite* sur G ($G \circlearrowleft H$) par multiplication : $g.h = gh$.

Pour $a \in G$, on note

$$aH = \omega(a) = \{ah : h \in H\} ;$$

ceci s'appelle une classe *à gauche* modulo H.

(2.5) Lemme. *Toutes les orbites sont en biijection avec* H.
En particulier si H est fini, elles ont toutes le même cardinal $|H|$.

Preuve. $\phi_a : H \to aH$ est une application injective et surjective pour tout a. □

(2.6) Application. Théorème de Lagrange.

Parenthèse : propriété universelle du quotient

(2.7) Proposition. *Soit G un groupe, et $K \triangleleft G$ un sous-groupe* distingué*, de sorte que le quotient G/K est muni d'une structure de groupe. On considère un autre groupe H. Les morphismes de groupes $G/K \to H$ sont en correspondance bi-univoque avec les morphismes de groupes $G \to H$ qui sont triviaux sur K.*

(2.8) Exercice. Si $H = M$ est un groupe abélien, l'ensemble $\mathrm{Hom}(G, H)$ est muni d'une structure canonique de groupe, automatiquement abélien.
1) La composition (à gauche) avec $G \to G/K$ et la restriction à K définissent respectivement deux morphismes de groupes

$$\mathrm{Hom}(G/K, M) \to \mathrm{Hom}(G, M) \quad \text{et} \quad \mathrm{Hom}(G, M) \to \mathrm{Hom}(K, M).$$

2) Le morphisme $\mathrm{Hom}(G/K, M) \to \mathrm{Hom}(G, M)$ est injectif, et son image est le noyau de $\mathrm{Hom}(G, M) \to \mathrm{Hom}(K, M)$.

Action sur un quotient

(2.9) $G \circlearrowleft G/H$ par multiplication à gauche : $g.aH = gaH$, autrement dit $g.\bar{a} = \overline{ga}$. Valable pour un sous-groupe quelconque (pas nécessairement distingué).
Attention : on ne peut pas écrire $\overline{ga} = \bar{g}\bar{a}$, quand H n'est pas distingué on ne peut même pas mettre de structure de monoïde sur le quotient. Il n'y a pas en général d'action $G/H \circlearrowleft G/H$ qui correspond à $G \circlearrowleft G/H$, c'est pour ça que cette dernière est intéressante.

(2.10) Lemme. *L'action $G \circlearrowleft G/H$ par multiplication à gauche est transitive, mais n'est pas fidèle en général. De plus, un $g \in G$ peut très bien agir avec points fixes.*

Preuve. L'action $G \circlearrowleft G/H$ est transitive comme $G \circlearrowleft G$: pour $a, b \in G$, $\bar{b} = ba^{-1}.\bar{a}$. Les autres affirmations sont justifiées par l'Exemple (2.10.2) ci-dessous. □

(2.10.1) Noyau de l'action $G \circlearrowleft G/H$. Il est clair que ça ne peut pas être H en général, sinon celui-ci serait distingué. En général :

$$\begin{aligned} g \in \ker\big(G \circlearrowleft G/H\big) &\Leftrightarrow \forall a \in G,\ \exists h(a) \in H : ga = ah(a) \\ &\Leftrightarrow \forall a \in G,\ g \in aHa^{-1}\ ; \end{aligned}$$

autrement dit, g agit trivialement ssi il est dans l'intersection de tous les conjugués de H.

(2.10.2) Exemple. On réalise $\mathbf{P}^n_{\mathbf{k}}$ comme un quotient de $\mathrm{GL}_{n+1}(\mathbf{k})$ par un certain sous-groupe (*cf.* (2.11)). L'espace projectif $\mathbf{P}^n_{\mathbf{k}}$ contient un espace affine $\mathbf{A}^n_{\mathbf{k}}$. Les transformations de $\mathbf{A}^n_{\mathbf{k}}$ provenant de l'action de GL_{n+1} sur $\mathbf{P}^n$ sont exactement les transformations affines. Parmi elles, on sait bien que certaines ont des points fixes.

Les homothéties dans GL_{n+1} agissent bien sûr trivialement sur $\mathbf{P}^n$, et on sait bien que ce sont les seules (*cf.* (2.11.1)).

(2.11) Grassmanniennes. A COMPLÉTER. Voici déjà un calcul pour comprendre le quotient par le sous-groupe des matrices triangulaires supérieures par bloc : dans le produit $M = NH$, soit

$$\left(\begin{array}{c|c|c} M_1 & \cdots & M_n \end{array}\right) = \left(\begin{array}{c|c|c} N_1 & \cdots & N_n \end{array}\right) \times \left(\begin{array}{c|c} A & B' \\ \hline 0 & B \end{array}\right),$$

les p premières colonnes (où p est la taille du bloc A) sont

$$\left(\begin{array}{c|c|c} M_1 & \cdots & M_p \end{array}\right) = \left(\begin{array}{c|c|c} N_1 & \cdots & N_n \end{array}\right) \times \left(\begin{array}{c} A \\ \hline 0 \end{array}\right) = \left(\begin{array}{c|c|c} N_1 & \cdots & N_p \end{array}\right) \times A.$$

(2.11.1) Noyau de $\mathrm{GL}_{n+1} \circlearrowleft \mathbf{P}^n$. Pour $A = (A_0, \ldots, A_n) \in \mathrm{GL}_{n+1}$ et $P \in \mathrm{GL}_{n+1}$, l'action de P sur $\bar{A} = [A_0] \in \mathbf{P}^n$ est induite par

$$P \times \left(\begin{array}{c|c|c} A_0 & \cdots & A_n \end{array}\right) = \left(\begin{array}{c|c|c} PA_0 & \cdots & PA_n \end{array}\right)$$

et donc $P.[A_0] = [PA_0]$ sans surprise. Les matrices P agissant trivialement sont celles agissant comme une homothétie sur toutes les droites ; on sait bien que ceci caractérise les homothéties.
(2.11.2) Question. Quel est le noyau de $\mathrm{GL}_{n+1} \circlearrowleft \mathbf{Gr}(k+1, n+1)$?

3 – Équation aux classes

(3.1) Pour $G \circlearrowleft X$ et $x \in X$, on note

$$\mathrm{Stab}(x) = \{g \in G : g.x = x\}.$$

C'est un sous-groupe de G, en général pas distingué.

(3.2) Lemme. *On a une bijection équivariante entre $\omega(x)$ et $G/\operatorname{Stab}(x)$.*

Peut-être contrairement aux apparences, $\mathrm{Stab}(x)$ n'a aucune raison d'être un noyau, et $\omega(x)$ n'est en général pas un groupe.

Preuve. On cherche $\phi : G/\operatorname{Stab}(x) \to \omega(x)$ bijection qui fasse commuter pour tout $g \in G$ le diagramme suivant :

$$\begin{array}{ccc} G/\operatorname{Stab}(x) & \xrightarrow{\phi} & \omega(x) \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle g} \\ G/\operatorname{Stab}(x) & \xrightarrow{\phi} & \omega(x) \end{array}$$

On prend

$$\phi : \bar{g} \in G/\operatorname{Stab}(x) \mapsto g.x \in \omega(x).$$

C'est bien défini, surjectif (définition de l'orbite), injectif (petit calcul), et équivariant :

$$g.\phi(\bar{h}) = g.(h.x) = gh.x = \phi(\overline{gh}) = \phi(g.\bar{h}).$$

□

(3.3) On déduit de (3.2) que l'orbite de x est finie ssi $\mathrm{Stab}(x)$ est d'indice fini dans G (il n'y a pas besoin que G soit fini), et dans ces conditions on a

$$|\,\omega(x)| = [G : \mathrm{Stab}(x)].$$

Si de plus G est fini, alors

$$[G : \mathrm{Stab}(x)] = \frac{|G|}{|\operatorname{Stab}(x)|}.$$

Les considérations précédentes indiquent que si x et x' appartiennent à la même orbite, alors

$$[G : \mathrm{Stab}(x)] = [G : \mathrm{Stab}(x')].$$

Une bonne raison pour cette égalité est le fait que les deux stabilisateurs sont conjugués ; en appliquant le principe de conjugaison, on voit immédiatement que

$$\mathrm{Stab}(g.x) = g \operatorname{Stab}(x) g^{-1}.$$

(3.3.1) Notation. Soit $\omega \in G \backslash X$. Si pour $x \in \omega$ le stabilisateur $\mathrm{Stab}(x)$ est fini, je note

$$\mathrm{st}(\omega) = |\operatorname{Stab}(x)|.$$

Je n'introduis pas de notation pour l'indice ; pour nous le plus souvent X et G seront tous les deux finis.

(3.4) Équation aux classes. Supposons l'ensemble X fini. On peut alors supposer G fini sans grand dommage, quitte à quotienter par le noyau de l'action ($\mathfrak{S}(X)$ est fini bien sûr) ; je le fais dès à présent. On déduit de la partition de X selon ses orbites sous l'action de G l'égalité

$$|X| = \sum_{\omega \in G\backslash X} |\,\omega\,|$$

puis, tenant compte de (3.3),

$$|X| = \sum_{\omega \in G\backslash X} \frac{|G|}{\mathrm{st}(\omega)}. \tag{3.4.1}$$

(3.5) Application. Soit p un nombre premier. On suppose ici en plus des hypothèses de (3.4) que G est un *p-groupe*, c'est-à-dire un groupe d'ordre une puissance de p. Alors

$$|X| \equiv \big|X^G\big| \mod p. \tag{3.5.1}$$

Preuve. Dans (3.4.1), on distingue les orbites constituées d'un seul élément et les autres : pour les premières on a $\omega = \{x\}$ et $|\,\omega\,| = 1$; pour les secondes

$$|\,\omega\,| = \frac{|G|}{\mathrm{st}(\omega)} = \frac{p^r}{p^s}$$

avec $r > s$, et donc $|\,\omega\,| \equiv 0 \mod p$. □

(3.5.2) Remarque. On observe de nouveau au cours de la preuve précédente que deux orbites sous une même action ont en général des tailles qui n'ont rien à se dire.

(3.6) De manière en quelque sorte duale par rapport à (3.1), on pose pour $g \in G$

$$\mathrm{Fix}(g) = \{x \in X : g.x = x\}$$

l'ensemble des points fixes sous l'action de g.

(3.7) Formule de Burnside. On considère l'action $G \circlearrowleft X$ d'un groupe fini sur un ensemble fini. On a les deux formules :

$$\big|G\setminus X\big| = \frac{1}{|G|} \sum_{x \in X} |\,\mathrm{Stab}(x)|, \tag{3.7.1}$$

$$\sum_{x \in X} |\,\mathrm{Stab}(x)| = \sum_{g \in G} |\,\mathrm{Fix}(g)|. \tag{3.7.2}$$

Preuve. On commence par montrer (3.7.2) ; elle s'obtient en calculant de deux façons équivalentes par le théorème de Fubini le cardinal du graphe des points fixes de l'action

$$\mathcal{F}ix\big(G \circlearrowleft X\big) = \big\{(g,x) \in G \times X : g.x = x\big\}.$$

Il y a une toute petite astuce pour (3.7.1) :

$$\big|G\setminus X\big| = \sum_{\omega \in G\backslash X} 1 = \sum_{\omega \in G\backslash X} \Big(\frac{1}{|\,\omega\,|} \sum_{x \in \omega} 1\Big) = \sum_{x \in X} \frac{|\,\mathrm{Stab}(x)|}{|G|}.$$

□

Remarque. Cette formule est un ingrédient essentiel dans la classification des sous-groupes finis de $\mathrm{SO}_3(\mathbf{R})$.

4 – Application : théorèmes de Sylow

Attention, les théorèmes de Sylow sont hors programme 2019 de l'agreg. En revanche les actions de groupes sont bien au programme, et les théorèmes de Sylow en sont une jolie application.

Il y a des preuves dans le cours de F. Castel, ainsi que dans ma feuille de TD 2012–2013. Je choisis ici de donner les énoncés sous la forme la plus synthétique et efficace possible, faisant fi d'une éventuelle chronologie.

(4.1) Théorème. *Soit p un nombre premier et G un groupe fini. Écrivons $|G| = p^\alpha m$, avec $\alpha \geqslant 0$ et m premier à p. Pour tout $\beta = 0, \dots, \alpha$, G possède un sous-groupe d'ordre p^β.*

Le premier théorème de Sylow est le cas $\beta = \alpha$ dans l'énoncé ci-dessus (1872 d'après Castel). Un sous-groupe d'ordre p^α s'appelle un p-Sylow (ou p-sous-groupe de Sylow). Le cas $\beta = 0$ de l'énoncé est vide ; le cas $\beta = 1$ est le théorème de Cauchy.

(4.2) Théorème. *Soit G un groupe fini.*
(a) Les p-Sylow de G sont conjugués deux à deux.
(b) Tout p-sous-groupe de G est contenu dans un p-Sylow.

Second théorème de Sylow (1872) pour l'ensemble, d'après Castel. Dans les notations de (4.1), (b) signifie que tout sous-groupe d'ordre p^β de G est contenu dans un sous-groupe d'ordre p^α.

(4.3) Corollaire. *Si G possède un seul p-Sylow, ce p-Sylow est un sous-groupe distingué.*

(4.4) Théorème. *On reprend les notations de (4.1). Pour tout $\beta = 0, \dots, \alpha$, notons $n_{p^\beta}(G)$ le nombre de sous-groupes d'ordre p^β de G.*
(a) Pour tout $\beta = 0, \dots, \alpha$,

$$n_{p^\beta} \equiv 1 \mod p.$$

(b) n_p divise m.

Le troisième théorème de Sylow (1872) est classiquement énoncé comme le cas $\beta = \alpha$ de (a) plus (b). La version complète de (a) est la version "améliorée" qu'on a établie avec Peter Haïssinsky.

(4.5) *Preuve de (4.4),* (a)*, et ainsi de (4.1).* Il suffit de démontrer la congruence (a) de (4.4), puisque si celle-ci est satisfaite on a nécessairement $n_{p^\beta} \neq 0$.

On considère $X = \mathcal{P}_{p^\beta}(G)$ l'ensemble des parties à p^β éléments de G, et l'action $G \circlearrowright X$ par translation à gauche :

$$g.\{a_1, \dots, a_{p^\beta}\} = \{ga_1, \dots, ga_{p^\beta}\}$$

(c'est bien défini, et c'est bien une action).

(4.5.1) Pour tout $A \in X$, on a $|\operatorname{Stab}(A)| \leqslant p^\beta$. En effet, pour tout choix d'un élément $a \in A$, on a une fonction injective

$$\phi_a : h \in \operatorname{Stab}(A) \mapsto ha \in A.$$

C'est effectivement injectif, puisque dans un groupe on a bien

$$ha = h'a \Leftrightarrow h = h'.$$

(4.5.2) Pour tout $\omega \in G\backslash X$, si $\mathrm{st}(\omega) = p^\beta$ alors ω contient un et un seul sous-groupe $H_\omega < G$. On va montrer ceci en deux temps.

(i) $A \in \omega$ est un sous-groupe ssi $1 \in A$.

La première implication est claire. Supposons donc $1 \in A \in \omega$. L'application

$$\phi_1 : h \in \mathrm{Stab}(A) \mapsto h \in A$$

du (4.5.1) est toujours injective, et ici surjective par égalité des cardinaux. On en déduit $A = \mathrm{Stab}(A)$ et donc notre assertion, puisque $\mathrm{Stab}(A)$ est un sous-groupe de G.

(ii) L'orbite ω contient un et un seul élément A tel que $1 \in A$.

L'existence d'un tel A est assez claire ; notons

$$A = \{a_1 = 1, a_2, \ldots, a_{p^\beta}\}.$$

Soit $g \in G$, et supposons que $1 \in g.A$. Alors $ga_i = 1$ pour un certain $i \in [\![1, p^\beta]\!]$. Mais A est le sous-groupe $\mathrm{Stab}(A)$ d'après (i), donc $g = a_i^{-1} \in \mathrm{Stab}(A)$ et $g.A = A$, d'où l'unicité.

(4.5.3) Pour $\omega \in G\backslash X$, si $\mathrm{st}(\omega) < p^\beta$ alors $|\,\omega\,| \equiv 0 \mod p^{\alpha-\beta+1}$. En effet, si $|\,\mathrm{Stab}(A)| < p^\beta$ on peut écrire

$$|\,\mathrm{Stab}(A)| = p^\gamma m',\ \gamma < \beta \text{ et } m'|m,$$

d'où l'on déduit

$$|\,\omega(A)| = \frac{|G|}{|\,\mathrm{Stab}(A)|} = \frac{m}{m'} p^{\alpha-\gamma} \equiv 0 \mod p^{\alpha-\beta+1}$$

comme il fallait, puisque $m/m' \in \mathbf{N}$ et $\alpha - \gamma \geqslant \alpha - \beta + 1$.

On a donc :

$$|X| = \sum_{\omega \in G\backslash X} |\,\omega\,| = \sum_{\mathrm{st}(\omega) < p^\beta} |\,\omega\,| + \sum_{\mathrm{st}(\omega) = p^\beta} |\,\omega\,|,$$

où le premier terme de la somme est divisible par $p^{\alpha-\beta+1}$ d'après (4.5.3), et le second égal à $n_{p^\beta}|G|/p^\beta = n_{p^\beta} m p^{\alpha-\beta}$ d'après (4.5.2). On a ainsi établi la congruence

$$\binom{mp^\alpha}{p^\beta} \equiv n_{p^\beta}(G) m p^{\alpha-\beta} \mod p^{\alpha-\beta+1}. \tag{4.5.4}$$

On conclut en considérant le groupe $G = \mathbf{Z}/mp^\alpha\mathbf{Z}$ qu'on connaît bien (*cf.* partie II). Puisque pour tout $d|n$, $\mathbf{Z}/n\mathbf{Z}$ possède un unique sous-groupe d'ordre d, on a

$$n_{p^\beta}\left(\mathbf{Z}/mp^\alpha\mathbf{Z}\right) = 1,$$

d'où l'on déduit la congruence à 0% de théorie des groupes

$$\binom{mp^\alpha}{p^\beta} \equiv m p^{\alpha-\beta} \mod p^{\alpha-\beta+1}. \tag{4.5.5}$$

par (4.5.4) (*cf.* (4.7) pour un calcul direct).

Mettant (4.5.4) et (4.5.5) bout à bout, on obtient pour G quelconque d'ordre mp^α :

$$\begin{aligned} & mp^{\alpha-\beta} \equiv n_{p^\beta}(G) m p^{\alpha-\beta} \mod p^{\alpha-\beta+1} \\ \iff \quad & p^{\alpha-\beta} \equiv n_{p^\beta}(G) p^{\alpha-\beta} \mod p^{\alpha-\beta+1}, \end{aligned}$$

l'équivalence entre les deux congruences étant donnée par l'inversibilité de m modulo $p^{\alpha-\beta+1}$ (*cf.* Proposition (2.1) ; m est premier à p par hypothèse, donc premier à $p^{\alpha-\beta+1}$ puisque p est premier). Il existe donc un entier q tel que

$$n_{p^\beta}(G) p^{\alpha-\beta} = p^{\alpha-\beta} + qp^{\alpha-\beta+1} \iff n_{p^\beta}(G) = 1 + qp,$$

comme il fallait démontrer. □

(4.6) Applications des théorèmes de Sylow [Castel, 4.2]**.**

(i) Prouver qu'un groupe n'est pas simple (en démontrant qu'un p-Sylow est distingué grâce au troisième théorème de Sylow).

(ii) Compter le nombre de sous-groupes d'un ordre donné (en particulier le nombre de p-Sylow). S'il n'y en a qu'un, il est caractéristique.

(iii) Montrer qu'un groupe est un produit semi-direct en exhibant un complément (généralement un p-Sylow) d'un sous-groupe distingué.

(iv) Montrer que des sous-groupes, ou simplement des éléments d'un certain ordre, sont conjugués.

(v) Prouver qu'il existe ou non des éléments d'un certain ordre.

(vi) Amorcer la classification des groupes finis et dans certains, pouvoir conclure. Les théorèmes de Sylow et une bonne connaissance des produits semi-directs permettent de classer assez facilement de nombreux groupes (*i.e.* de déterminer le nombre de classes d'isomorphie en fonction de l'ordre).

(4.7) Preuve directe de la congruence sur les coefficients binomiaux.
Dans [Francinou–Gianella–Nicolas, Alg. 1, 4.24], il est prouvé (et c'est facile !) que si p est un nombre premier, alors pour tout $k = 1, \dots, p^n - 1$:

$$v_p\left[\binom{p^n}{k}\right] = n - v_p(k).$$

C'est moins général que le fameux théorème de Kummer, qui donne la valuation p-adique de $\binom{N}{k}$ pour n'importe quel N.

II – Groupes monogènes

1 – Description générale

(1.1) Définition. Monogène, cyclique.

(1.2) Avatars "du" groupe cyclique. $\mathbf{Z}/n\mathbf{Z}$, μ_n, groupe des rotations d'angle $k2\pi/n$, $k \in \mathbf{Z}$ (= groupe des isométries directes d'un polygône régulier à n côtés).
NB : $\mathbf{Z}/2\mathbf{Z} = \big(\{0,1\},+\big) = \big(\{\pm 1\},\times\big)$.

(1.3) Proposition. *Tout groupe monogène est isomorphe (non canoniquement) à* $\mathbf{Z}$ *ou* $\mathbf{Z}/n\mathbf{Z}$.

Corollaire. Tout groupe monogène est abélien (OSD).

Rappel. Sous-groupes de $\mathbf{Z}$.

Preuve de (1.3). Le choix (non canonique) d'un générateur de G induit un morphisme surjectif $f : \mathbf{Z} \twoheadrightarrow G$. Le noyau de f est un sous-groupe de $\mathbf{Z}$. □

(1.4) Structure d'anneau induite par la structure de groupe. Tout comme $\mathbf{Z}$, $\mathbf{Z}/n\mathbf{Z}$ est non seulement un groupe mais aussi un anneau, et la structure d'anneau est induite par la structure de groupe :

$$k \cdot n = \underbrace{n + \cdots + n}_{k \text{ fois}}$$

dans $\mathbf{Z}$, et

$$\bar{k} \cdot \bar{n} = \overline{\underbrace{n + \cdots + n}_{k \text{ fois}}}$$

dans $\mathbf{Z}/n\mathbf{Z}$ (oui, c'est bien défini).

Il faut faire particulièrement attention quand on utilise une réalisation multiplicative de $\mathbf{Z}/n\mathbf{Z}$, par exemple μ_n :

$$\exp\big(2\pi i\tfrac{k}{n}\big) \cdot \exp\big(2\pi i\tfrac{k'}{n}\big) = \exp\big(2\pi i\tfrac{k+k'}{n}\big)$$

sans problème, mais où a disparu le produit ? Certes

$$\exp\big(2\pi i\tfrac{k}{n}\big)^{k'} = \exp\big(2\pi i\tfrac{kk'}{n}\big),$$

mais ça n'est pas tout-à-fait ce qu'on veut.

2 – Générateurs de $(\mathbf{Z}/n\mathbf{Z},+)$

(2.1) Proposition. *Soit* s, n *deux entiers,* $n \neq 0$. *LPSSE :*
(i) $\bar{s}$ *générateur de* $(\mathbf{Z}/n\mathbf{Z},+)$ *;*
(ii) s *et* n *premiers entre eux ;*
(iii) $\bar{s}$ *inversible de l'anneau* $(\mathbf{Z}/n\mathbf{Z},+,\cdot)$.

3 – Sous-groupes de $\mathbf{Z}/n\mathbf{Z}$

(3.1) Je vous rappelle que vous connaissez les sous-groupes de $(\mathbf{Z}, +)$, et $(\mathbf{R}, +)$ aussi d'ailleurs.

(3.2) Proposition. *(i) Tout sous-groupe d'un groupe monogène est monogène.*
(ii) Pour $d|n$, tout groupe cyclique d'ordre n possède un unique *sous-groupe d'ordre d.*

On peut voir cet énoncé comme un super théorème de Sylow dans le cas des groupes cycliques.

Preuve. (i) Soit G monogène, $f : \mathbf{Z} \twoheadrightarrow G$ induit par le choix d'un générateur. Soit $H < G$. On sait que $f^{-1}(H)$ est un sous-groupe de $\mathbf{Z}$, donc on peut écrire

$$f^{-1}(H) = d\mathbf{Z}.$$

On en déduit que $f(d)$ est un générateur de H. [1]

(ii) Soit $d > 0$ un diviseur de n. On va montrer que $\mathbf{Z}/n\mathbf{Z}$ possède un unique sous-groupe d'ordre d. Considérons le sous-groupe

$$H_d := \langle a \in \mathbf{Z}/n\mathbf{Z} : \text{ordre}(a) = d \rangle .$$

Il contient $\langle \overline{n/d} \rangle$, donc d divise l'ordre de H_d.

Comme tous les sous-groupes de $\mathbf{Z}/n\mathbf{Z}$ il est cyclique, engendré par un $x \in H_d$. On calcule $d \cdot x = 0$, donc l'ordre de x divise d. On conclut que l'ordre de H_d divise d.

Finalement on a démontré que $|H_d| = d$. D'autre part, tout sous-groupe d'ordre d de $\mathbf{Z}/n\mathbf{Z}$, étant monogène donc engendré par un élément d'ordre d, est contenu dans H_d, et donc en fait égal à H_d. □

Remarque. En général H_d n'est pas un sous-groupe : dans $\mathfrak{S}_n$, $(12)(23) = (123)$ n'est pas d'ordre 2. Si G est abélien, alors H_d est un sous-groupe, mais en général il n'est pas d'ordre d. Regarder par exemple le groupe de Klein.

Attention : $\mathbf{Z}/n\mathbf{Z}$ contient un unique sous-groupe d'ordre $d|n$, mais en général plusieurs éléments d'ordre d, qui sont les différents générateurs de H_d.
Exemple : $\langle \bar{2} \rangle = \langle \bar{4} \rangle$ dans $\mathbf{Z}/6\mathbf{Z}$.

(3.3) Proposition. *Soit $a \in \mathbf{Z}$, et notons $d = \text{pgcd}(a, n)$. On a*

$$\langle \bar{a} \rangle = a \cdot \mathbf{Z}/n\mathbf{Z} = d \cdot \mathbf{Z}/n\mathbf{Z} = \langle \bar{d} \rangle.$$

Preuve. Par définition,

$$\langle \bar{a} \rangle = \{k \cdot \bar{a} : k \in \mathbf{Z}\}.$$

Puisque $k \cdot \bar{a} = a \cdot \bar{k}$ (*cf.* (1.4)), on a $\langle \bar{a} \rangle = a \cdot \mathbf{Z}/n\mathbf{Z}$ comme annoncé.

Considérons la surjection canonique $f : \mathbf{Z} \twoheadrightarrow \mathbf{Z}/n\mathbf{Z}$ (pour le choix préféré de générateur, $\bar{1}$), et notons $H = \langle \bar{a} \rangle$. Puisque $H = f(a\mathbf{Z})$ et $\ker(f) = n\mathbf{Z}$, on a

$$f^{-1}(H) = f^{-1}(f(a\mathbf{Z})) = a\mathbf{Z} + n\mathbf{Z} = d\mathbf{Z},$$

donc

$$H = f(f^{-1}(H)) = f(d\mathbf{Z}) = d \cdot \mathbf{Z}/n\mathbf{Z}.$$

1. En général en théorie des ensembles, on a $f(f^{-1}(A)) \subseteq A$, et l'inclusion inverse est vraie si f est surjective.

Enfin, $d \cdot \mathbf{Z}/n\mathbf{Z} = \langle \bar{d} \rangle$ tout comme $\langle \bar{a} \rangle = a \cdot \mathbf{Z}/n\mathbf{Z}$. □

Exercice. Démontrer $f^{-1}(H) = a\mathbf{Z} + n\mathbf{Z}$ calmement par double inclusion.

Preuve élémentaire. Puisque $d|a$, on peut écrire $a = qd$, et donc pour tout entier k on a

$$k.\bar{a} = kq.\bar{d},$$

donc

$$\langle \bar{a} \rangle \subseteq \langle \bar{d} \rangle .$$

Pour montrer l'inclusion inverse, écrivons une relation de Bezout

$$au + nv = d.$$

On en déduit $\bar{d} = u\bar{a}$, et donc par le même raisonnement qu'avant

$$\langle \bar{d} \rangle \subseteq \langle \bar{a} \rangle .$$

□

Attention ! Il n'y a aucune raison pour que dans la relation de Bezout $au+nv = d$, u soit premier à n. Exemple :

$$-2 \times 4 + 1 \times 10 = 2.$$

(3.4) Corollaire. *(i) L'ordre de $\bar{a}$ est n/d.*
(ii) Les générateurs de $\mathbf{Z}/n\mathbf{Z}$ sont les $\bar{a}$ avec a premier à n.

(3.5) Proposition. *Tout quotient d'un groupe monogène est monogène.*

Preuve. Soit Q quotient de G monogène. On a une surjection canonique $\pi : G \twoheadrightarrow Q$. Considérons d'autre part une surjection $f : \mathbf{Z} \twoheadrightarrow G$. Le morphisme composé $\pi \circ f$ est surjectif de $\mathbf{Z}$ dans Q. Ceci prouve le caractère monogène de Q. □

(3.6) Proposition. *On reprend les notations de (3.3). On a*

$$\big(\mathbf{Z}/n\mathbf{Z}\big)/\langle \bar{a} \rangle \cong \mathbf{Z}/d\mathbf{Z}.$$

Preuve. Le quotient $\big(\mathbf{Z}/n\mathbf{Z}\big)/\langle \bar{a} \rangle$ est cyclique, d'ordre

$$\frac{n}{\text{ordre}(\bar{a})} = \frac{n}{n/d}.$$

□

On peut écrire une preuve un peu plus conceptuelle en s'appuyant sur l'énoncé ci-dessous, valable pour des groupes quelconques.

(3.7) Lemme. *Soit $f : G \to Q$ morphisme surjectif, et $H \lhd Q$. Alors*
(i) $\hat{H} := f^{-1}(H) \lhd G$, et
(ii) les deux groupes *$G/\hat{H}$ et Q/H sont isomorphes.*

Preuve. On considère la surjection canonique $\pi : Q \to Q/H$. Par définition, son noyau est le sous-groupe distingué H. Le morphisme composé $\pi \circ f : G \to Q/H$ est surjectif, de noyau $\hat{H}$. Ceci prouve d'une part le caractère distingué de $\hat{H}$ dans G ("un noyau c'est distingué"), d'autre part l'isomorphisme $G/\hat{H} \cong Q/H$. □

4 – Lemme chinois

C'est aussi un isomorphisme d'anneau. On a une réciproque : $\mathbf{Z}/a\mathbf{Z} \times \mathbf{Z}/b\mathbf{Z}$ est cyclique si et seulement si a et b sont premiers entre eux.

(4.1) Preuve 1. $(1,1) \in \mathbf{Z}/a\mathbf{Z} \times \mathbf{Z}/b\mathbf{Z}$ est d'ordre $\text{ppcm}(a,b) = ab$. □

(4.2) Preuve 2. On regarde le morphisme canonique $\mathbf{Z} \to \mathbf{Z}/a \times \mathbf{Z}/b$. Il est surjectif, et son noyau est $a\mathbf{Z} \cap b\mathbf{Z} = \text{ppcm}(a,b)\mathbf{Z} = ab\mathbf{Z}$.

(4.3) Construction de l'inverse. On cherche quelqu'un dans $\mathbf{Z}$ qui donne $(1,0)$ par le morphisme ci-dessus. Il doit donc être λb, avec $\lambda b \equiv 1 \mod a$.

On conclut que l'inverse s'écrit

$$(\bar{\alpha}, \bar{\beta}) \mapsto \overline{\alpha \cdot b'b + \beta \cdot a'a} \in \mathbf{Z}/ab$$

(où $a'a + b'b = 1$ relation de Bezout).

(4.4) Exercice.
(4.4.1) Si $\text{pgcd}(a,b) \neq 1$ alors $\mathbf{Z}/a \times \mathbf{Z}/b$ n'est pas cyclique.
(4.4.2) $\mathbf{Z}/a \times \mathbf{Z}/b \cong \mathbf{Z}/\text{pgcd} \times \mathbf{Z}/\text{ppcm}$.
(4.4.3) Démontrer sans utiliser la décomposition en produit de facteurs premiers l'identité $ab = \text{pgcd}(a,b) \cdot \text{ppcm}(a,b)$.

5 – Indicatrice d'Euler

(5.1) Définition. On désigne par $\varphi : \mathbf{N}^* \to \mathbf{N}^*$ la fonction indicatrice d'Euler, définie par

$$\forall n \geqslant 1 \quad \varphi(n) = \text{Card}\left\{k \in [\![1,n]\!] : n \wedge k = 1\right\}.$$

(5.2) Lemme. *Le nombre de générateurs dans un groupe cyclique à n éléments est $\varphi(n)$.*

C'est un corollaire immédiat de la Proposition (2.1).

(5.3) Proposition. $n = \sum_{0<d|n} \varphi(d)$.

S'obtient en comptant les éléments de $\mathbf{Z}/n\mathbf{Z}$ en les regroupant selon leur ordre ; ce n'est pas trivial, il faut le super-Sylow des groupes cycliques. (On peut aussi faire une récurrence en se basant sur (5.4) ci-dessous, en initialisant pour n une puissance d'un nombre premier, mais j'aime beaucoup moins).

(5.4) Lemme. *Si* $\text{pgcd}(a,b) = 1$, *alors* $\varphi(ab) = \varphi(a)\varphi(b)$.

S'obtient en mettant ensemble le lemme chinois et le Lemme (5.2) ci-dessus.

(5.5) Proposition. *Soit $n \in \mathbf{N}^*$, $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ sa décomposition en produits de facteurs premiers (les p_i sont des nombres premiers deux à deux distincts, et les α_i des entiers positifs). On a*

$$\varphi(n) = n \prod_{i=1}^{r} \big(1 - \frac{1}{p_i}\big).$$

Preuve. On commence par calculer $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ en comptant les nombres premiers à p entre 1 et p^α :

$$1, \ldots, p-1, p+1, \ldots, 2p-1, 2p+1, \ldots, (p^{\alpha-1}-1)p-1, (p^{\alpha-1}-1)p+1, \ldots, p^\alpha - 1 \ ;$$

il y en a $p^\alpha - p^{\alpha-1}$ puisque on a sauté tous les multiples de p.

Ensuite on utilise la formule (5.4) :

$$\varphi(n) = \prod_i \varphi(p_i^{\alpha_i} = \prod_i p_i^{\alpha_i - 1}(p_i - 1) = n \prod_i \frac{1}{p_i}(p_i - 1)$$

□

6 – Automorphismes de $(\mathbf{Z}/n\mathbf{Z}, +)$

(6.1) Remarquons que $(\mathrm{Aut}(\mathbf{Z}/n\mathbf{Z}), \circ)$ et $((\mathbf{Z}/n\mathbf{Z})^\times, \cdot)$ sont des groupes. Le premier *a priori* n'a aucune raison d'être abélien.

(6.2) Proposition. *On a les isomorphismes de* groupes *suivants :*
(6.2.1) $\mathrm{Aut}(\mathbf{Z}) \cong \mathbf{Z}/2$ *;*
(6.2.2) $\mathrm{Aut}(\mathbf{Z}/n\mathbf{Z}) \cong (\mathbf{Z}/n\mathbf{Z})^\times$*.*

Bien sûr la formulation intrinqèque de cet énoncé est « si G est monogène, alors le groupe $\mathrm{Aut}(G)$ des automorphismes du groupe G est isomorphe au groupe $G^\times$ des inversibles de l'anneau naturellement défini sur G ».

Preuve. Je le fais pour $\mathbf{Z}/n\mathbf{Z}$. On définit un morphisme de groupes

$$\phi : u \in \mathrm{Aut}(\mathbf{Z}/n\mathbf{Z}) \mapsto u(1) \in (\mathbf{Z}/n\mathbf{Z})^\times.$$

Déjà, si u est un automorphisme, $u(1)$ doit être comme 1 un générateur de $\mathbf{Z}/n\mathbf{Z}$, soit $u(1) \in (\mathbf{Z}/n\mathbf{Z})^\times$ d'après (2.1). Pour voir que ϕ est bien un morphisme, on dit que

$$u \circ v(1) = u\big(v(1)\big) = u(\underbrace{1 + \cdots + 1}_{v(1) \text{ fois}}) = \underbrace{u(1) + \cdots + u(1)}_{v(1) \text{ fois}}) = v(1) \cdot u(1) = u(1) \cdot v(1).$$

Le fond de l'histoire ici, c'est que vu comment est définie la structure d'anneau sur $\mathbf{Z}/n\mathbf{Z}$, un automorphisme du groupe $(\mathbf{Z}/n\mathbf{Z}, +)$ est automatiquement un automorphisme de l'anneau $(\mathbf{Z}/n\mathbf{Z}, +, \times)$.

C'est une correspondance injective, puisque une fois qu'on connaît $u(1)$ on a $u(x) = x \cdot u(1)$ pour tout $x \in \mathbf{Z}/n\mathbf{Z}$. C'est une correspondance surjective, puisque pour tout $a \in (\mathbf{Z}/n\mathbf{Z})^\times$, $x \mapsto ax$ est un automorphisme de $(\mathbf{Z}/n\mathbf{Z}, +)$. □

(6.3) Proposition. *Le groupe $\big(\mathbf{Z}/n\big)^\times$ est abélien d'ordre $\varphi(n)$.*

(6.4) Corollaire (théorème d'Euler). *Si a est premier à n, alors $a^{\varphi(n)} \equiv 1 \mod n$.*

(6.5) Lemme.

$$(\mathbf{Z}/n)^\times \cong \prod (\mathbf{Z}/p_i^{\alpha_i})^\times.$$

(C'est une application directe du lemme chinois).

(6.6) Classification (largement admise ; *cf.* [Perrin] pour les preuves complètes)**.**
(6.6.1) Pour tout p premier, $(\mathbf{Z}/p\mathbf{Z})^\times \cong \mathbf{Z}/(p-1)\mathbf{Z}$ (tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique, *cf.* (6.7) ci-dessous).
(6.6.2) Pour tout p premier, $p \neq 2$, on a de même $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times \cong \mathbf{Z}/\varphi(p^\alpha)\mathbf{Z} = \mathbf{Z}/(p^{\alpha-1}(p-1))\mathbf{Z}$.
(6.6.3) Pour $p = 2$, en revanche : $(\mathbf{Z}/2\mathbf{Z})^\times = \{1\}$; $(\mathbf{Z}/4\mathbf{Z})^\times \cong \mathbf{Z}/2\mathbf{Z}$; $(\mathbf{Z}/2^\alpha\mathbf{Z})^\times \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^{\alpha-2}\mathbf{Z}$ pour $\alpha \geqslant 3$.

Exercice. Trouver les éléments d'ordre 2 dans $(\mathbf{Z}/8\mathbf{Z})^\times$. En déduire que $(\mathbf{Z}/8\mathbf{Z})^\times \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

(6.7) Théorème. *Soit* $\mathbf{k}$ *un corps.*
(a) Tout sous-groupe fini du groupe multiplicatif $(\mathbf{k}^\times, \cdot)$ est cyclique.
(b) Pour tout $n \in \mathbf{N}$, $(\mathbf{k}^\times, \cdot)$ possède au plus un sous-groupe d'ordre n.

Preuve. Soit $x \in \mathbf{k}^\times$ un élément d'ordre d. On a l'égalité de polynômes à coefficients dans $\mathbf{k}$

$$X^d - 1 = \prod_{0 \leqslant \alpha \leqslant d-1} (X - x^\alpha),$$

donc tous les éléments d'ordre d de $k^\times$ sont dans $\langle x \rangle$. On en déduit que $k^\times$ contient 0 ou $\varphi(d)$ éléments d'ordre d.

Soit $G < \mathbf{k}^\times$ un sous-groupe fini d'ordre n. Pour tout diviseur d de n, si G contient un élément x d'ordre d, il contient $\langle x \rangle_{\mathbf{k}^\times}$ et donc tous les éléments d'ordre d de $\mathbf{k}^\times$. Donc, G contient 0 ou $\varphi(d)$ éléments d'ordre d. Puisque

$$|G| = n = \sum_{d|n} \varphi(d)$$

(Proposition (5.3)), $|G|$ doit en fait contenir $\varphi(d)$ éléments d'ordre d pour tout diviseur d de $|G|$. En particulier, il contient un élément d'ordre maximal n, donc il est cyclique.

Si G' est un autre sous-groupe d'ordre n de $\mathbf{k}^\times$, il est engendré par un élément d'ordre n de $\mathbf{k}^\times$. Puisque ceux-ci sont déjà tous dans G, $G' = G$. □

Exercice. (i) Montrer que tous les sous-groupes finis de $\mathbf{C}^*$ sont des μ_n. Exhiber un sous-groupe non monogène de $\mathbf{C}^*$ (nécessairement infini).
(ii) Montrer que $\mathbf{H}_8$ n'est pas cyclique.

III – Groupe symétrique

(0.1) Notation.

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

Application au calcul de la composée de deux permutations.

1 – Décomposition en produit de cycles à supports disjoints

(1.1) Théorème. *Soit $\sigma \in \mathfrak{S}_n$. Il existe des cycles $\kappa_1, \ldots, \kappa_r$ à supports disjoints tels que*

$$\sigma = \kappa_1 \cdots \kappa_r.$$

Une telle décomposition est unique à modifications triviales près.

Preuve. Regardons l'action de $\langle\sigma\rangle \cong \mathbf{Z}/a\mathbf{Z}$ ($a = \text{ordre}(\sigma)$) sur $X_n = [\![1, n]\!]$; on obtient

$$X_n = \coprod_{\omega \in \langle\sigma\rangle\backslash X_n} \omega = \omega_1 \sqcup \cdots \sqcup \omega_r \,.$$

Pour chaque orbite ω_i, choisissons un point de départ $x_i \in \omega_i$. Le stabilisateur $\text{Stab}(x_i)$ s'écrit $\langle\ell_i\rangle$ dans $\mathbf{Z}/a\mathbf{Z}$, $\ell_i \in [\![0, a-1]\!]$ diviseur de a :

$$\forall k \in \mathbf{Z}, \quad \sigma^k(x_i) = x_i \Leftrightarrow \ell_i | k,$$

et $\sigma^a(x_i) = x_i$. Ensuite ω_i s'identifie à $\langle\sigma\rangle \,/\, \text{Stab}(x_i) \cong \mathbf{Z}/\ell_i\mathbf{Z}$ *via* $\bar{k} \in \mathbf{Z}/\ell_i\mathbf{Z} \mapsto \sigma^k(x_i)$; autrement dit,

$$\omega_i = \big\{x_i, \sigma(x_i), \ldots, \sigma^{\ell_i - 1}(x_i)\big\},$$

avec $\sigma^k(x) \neq \sigma^{k'}(x)$ si $k \neq k'$ dans $[\![0, \ell_i - 1]\!]$. On voit ainsi que $\sigma|_{\omega_i}$ est un cycle de longueur ℓ_i.

Posons pour $i = 1, \ldots, r$,

$$\kappa_i = \big(x_i, \sigma(x_i), \ldots, \sigma^{\ell_i - 1}(x_i)\big) \;;$$

c'est un cycle de longueur ℓ_i et de support ω_i. On a bien $\sigma = \kappa_1 \cdots \kappa_r$ comme il fallait.

Réciproquement, si $\sigma = \kappa'_1 \cdots \kappa'_r$, alors quitte à rajouter tous les cycles triviaux (x) qu'il faut on a que les orbites de X_n sous l'action de $\langle\sigma\rangle$ sont les supports des κ'_i. De plus, pour $x_i \in \text{Supp}(\kappa'_i)$, on a $\text{Stab}(x_i) = \langle\ell(\kappa'_i)\rangle$, et

$$\kappa'_i = (x_i, \kappa'_i(x_i), \ldots, (\kappa'_i)^{\ell(\kappa'_i)-1}(x_i)) = (x_i, \sigma(x_i), \ldots, (\sigma)^{\ell(\kappa'_i)-1}(x_i)).$$

On obtient ainsi l'unicité de la décomposition. □

Remarque. On peut mener une analyse semblable dès qu'on a un groupe monogène qui agit sur un ensemble (si l'ensemble est fini, c'est exactement la présente analyse, d'ailleurs).

(1.2) Exercice. (i) Si $\kappa_1, \dots, \kappa_r$ sont des cycles à supports disjoints, alors

$$\text{ordre}(\kappa_1 \cdots \kappa_r) = \text{ppcm}\big(\ell(\kappa_1), \dots, \ell(\kappa_r)\big).$$

(Le point important est que si les supports sont disjoints alors les cycles commutent).
(ii) Quel est l'ordre de $(12)(23)$?

(1.3) Application (générateurs de $\mathfrak{S}_n$)**.**
(1.3.1) Question : à quoi ça sert de connaître un ensemble de générateurs ? et générateurs et relations ?
(1.3.2) $\mathfrak{S}_n$ *est engendré par les transpositions.* Il suffit de savoir écrire un cycle comme produit de transpositions, et

$$(a_0 \cdots a_{d-1}) = (a_0 a_1) \cdots (a_{d-2} a_{d-1}).$$

(1.4) Application (classes de conjugaison dans $\mathfrak{S}_n$)**.** *Deux permutations* $\sigma, \sigma' \in \mathfrak{S}_n$ *sont conjuguées si et seulement si leurs décompositions en produits de cycles à supports disjoints sont combinatoirement équivalentes.*

Autrement dit, si $\sigma = \kappa_1 \cdots \kappa_r$ et $\sigma' = \kappa'_1 \cdots \kappa'_{r'}$ (décompositions sans cycle trivial), σ et σ' sont conjuguées si et seulement si $r = r'$ et pour tout ℓ il y a autant de cycles de longueur ℓ parmi $\kappa_1, \dots, \kappa_r$ et parmi $\kappa'_1, \dots, \kappa'_r$.

(1.4.1) Corollaire. Le nombre de classes de conjugaison de $\mathfrak{S}_n$ est le nombre de partitions de n.

Preuve. On applique le principe de conjugaison sans mauvaise surprise. □

2 – Signature

(2.1) Théorème. *Il existe un unique morphisme de groupes non-trivial*

$$\varepsilon : \mathfrak{S}_n \to \{\pm 1\}.$$

Pour toute transposition τ *on ait* $\varepsilon(\tau) = -1$.

Preuve. Si $\varepsilon(\tau_0) = +1$ pour une transposition τ_0, alors $\varepsilon(\tau) = +1$ pour toute transposition τ puisque les transpositions sont conjuguées et $\{\pm 1\}$ est abélien. Ensuite l'unicité vient du fait que $\mathfrak{S}_n$ est engendré par les transpositions (tiens, ça peut servir à ça d'avoir un ensemble générateur).

Pour l'existence, on introduit le *nombre d'inversions* d'une permutation σ,

$$I(\sigma) = \text{Card}\big\{(i,j) \in [\![1,n]\!]^2 : i < j \text{ et } \sigma(i) > \sigma(j)\big\},$$

puis on définit $\varepsilon(\sigma) = (-1)^{I(\sigma)}$.

Si $\tau = (ab)$, $a < b$, alors

$$\begin{aligned}\big\{(i,j) \in [\![1,n]\!]^2 : i < j \text{ et } \tau(i) > \tau(j)\big\} \\ = \{(a, a+k), 1 \leqslant k < b-a\} \sqcup \{((a+k, b), 1 \leqslant k < b-a\} \sqcup \{(a,b)\}\end{aligned}$$

et donc $I(\tau)$ est impair.

Pour montrer que ε ainsi défini est un morphisme de groupes, on considère l'action $\mathfrak{S}_n \circlearrowleft \mathbf{Z}[X_1, \dots, X_n]$ définie par

$$(\sigma.P)(X_1, \dots, X_n) = P(X_{\sigma(1)}, \dots, X_{\sigma(n)}).$$

C'est bien une action de groupe. On regarde son effet sur

$$\Delta = \prod_{i<j}(X_j - X_i) = \begin{vmatrix} 1 & \cdots & 1 \\ X_1 & \cdots & X_n \\ \vdots & & \vdots \\ X_1^{n-1} & \cdots & X_n^{n-1} \end{vmatrix} :$$

on a $\sigma.\Delta = (-1)^{I(\sigma)}\Delta$ (*i.e.* $\sigma.\Delta = \varepsilon(\sigma)\Delta$) en regardant l'expression comme un produit, et ça permet de conclure. □

(2.2) Lemme. $\mathfrak{S}_n \circlearrowright \mathbf{Z}[X_1, \ldots, X_n]$ *est effectivement une action à gauche.*

(2.2.1) Déjà, une autre façon de définir l'action est de dire que

$$\sigma.(X_1^{a_1} \cdots X_n^{a_n}) = X_{\sigma(1)}^{a_1} \cdots X_{\sigma(n)}^{a_n}$$

et qu'ensuite on étend par linéarité. Une fois qu'on a écrit l'action comme ça, il me semble complètement évident que

$$\alpha.(X_{\beta(1)}^{a_1} \cdots X_{\beta(n)}^{a_n}) = X_{\alpha\beta(1)}^{a_1} \cdots X_{\alpha\beta(n)}^{a_n}.$$

Voyons voir ça :

$$X_{\sigma(1)}^{a_1} \cdots X_{\sigma(n)}^{a_n} = X_1^{a_{\sigma^{-1}(1)}} \cdots X_n^{a_{\sigma^{-1}(n)}};$$
$$\alpha.(X_{\beta(1)}^{a_1} \cdots X_{\beta(n)}^{a_n}) = X_{\alpha(1)}^{a_{\beta^{-1}(1)}} \cdots X_{\alpha(n)}^{a_{\beta^{-1}(n)}} = X_1^{a_{\beta^{-1}(\alpha^{-1}(1))}} \cdots X_n^{a_{\beta^{-1}(\alpha^{-1}(n))}}$$
$$= X_1^{a_{(\alpha\beta)^{-1}(1)}} \cdots X_n^{a_{(\alpha\beta)^{-1}(n)}} = X_{\alpha\beta(1)}^{a_1} \cdots X_{\alpha\beta(n)}^{a_n}.$$

Donc OK. □

(2.2.2) Si on préfère s'en tenir à la définition initiale, il vaut mieux faire un changement de variable :

$$\tilde{P}(X_1, \ldots, X_n) := (\beta.P)(X_1, \ldots, X_n) = P(X_{\beta(1)}, \ldots, X_{\beta(n)}) ;$$
$$(\alpha.\tilde{P})(Y_1, \ldots, Y_n) = \tilde{P}(Y_{\alpha(1)}, \ldots, Y_{\alpha(n)}) ;$$
$$\text{si } Y_i = X_{\beta(i)}, \text{ alors } Y_{\alpha(i)} = X_{\beta(\alpha(i))}.$$

□

(2.2.3) Il est fortement recommandé de regarder un (bon) exemple. Par exemple

$$P = X_1^2 + X_2 + X_1X_3,$$

avec $\alpha = (12)$ et $\beta = (123)$ et donc

$$\alpha\beta = (23) \quad \text{et} \quad \beta\alpha = (13),$$

de sorte que

$$\alpha\beta.P = P(X_1, X_3, X_2) = X_1^2 + X_3 + X_1X_2$$
$$\text{et} \quad \beta\alpha.P = P(X_3, X_2, X_1) = X_3^2 + X_2 + X_1X_3.$$

On a d'autre part

$$\beta.P(X_1, X_2, X_3) = P(X_2, X_3, X_1) = X_2^2 + X_3 + X_1X_2$$
$$\text{et} \quad \alpha.\beta.P(X_1, X_2, X_3) = \beta.P(X_2, X_1, X_3) = X_1^2 + X_3 + X_1X_2 = \alpha\beta.P.$$

(2.2.4) Exercice. Exhiber une matrice A_σ telle que

$$(\sigma.P)(X_1,\dots,X_n) = P\big((X_1,\dots,X_n)A_\sigma^{-1}.\big)$$

Pourquoi mettre A_σ^{-1} et pas simplement A_σ ? (il y a une bonne raison) Montrer que $\sigma \mapsto A_\sigma$ définit une représentation de $\mathfrak{S}_n$ (c'est la représentation de permutation standard).

2.1 – Formule de Laplace

(2.3) Proposition. *Soit $M = (a_{ij})_{1\leqslant i,j\leqslant n}$, matrice carrée à coefficients dans* $\mathbf{k}$ *anneau commutatif (oui !). On fixe un ensemble de colonnes $J = \{j_1 < \cdots < j_p\}$. On a*

$$\det(M) = \sum_{I=\{i_1<\cdots<i_p\}} (-1)^{|I|+|J|} \det(M_{IJ}) \det(M_{\bar I \bar J}),$$

où $|I| = i_1 + \cdots + i_p$.

La preuve est essentiellement semblable à celle du développement par rapport à une seule colonne, sauf qu'il y a un petit lemme pas complètement trivial sur la signature. C'est sur ce point qu'on se concentre ici.

(2.4) Notations. Pour tout $p \in [\![1,n]\!]$, on note $\mathcal{P}_p$ l'ensemble des parties à p éléments de $\{1,\dots,n\}$. Pour $I = \{i_1 < \cdots < i_p\} \in \mathcal{P}_p$, on note $\bar\imath_1 < \cdots < \bar\imath_{n-p}$ les $n-p$ entiers tels que

$$\{i_1,\dots,i_p,\bar\imath_1,\dots,\bar\imath_{n-p}\} = \{1,\dots,n\},$$

et $\omega_J^I = \big\{\sigma \in \mathfrak{S}_n : \sigma(J) = I\big\}$.

(2.5) Preuve. Le point de départ est la partition $\mathfrak{S}_n = \coprod \omega_J^I$, qui donne

$$\sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) a_{\sigma(1)1}\cdots a_{\sigma(n)n} = \sum_{I\in\mathcal{P}_p}\sum_{\sigma\in\omega_J^I} \varepsilon(\sigma) a_{\sigma(j_1)j_1}\cdots a_{\sigma(j_p)j_p} a_{\sigma(\bar\jmath_1)\bar\jmath_1}\cdots a_{\sigma(\bar\jmath_p)\bar\jmath_p}.$$

On va voir que $\sigma \in \omega_J^I$ se décompose en $(\sigma',\sigma'') \in \mathfrak{S}_I \times \mathfrak{S}_{\bar I}$ avec $\varepsilon(\sigma) = \varepsilon(\sigma')\cdot\varepsilon(\sigma'')$ (ensuite la conclusion est laissée au lecteur).

On définit une bijection

$$\Phi_J^I : \mathfrak{S}_p \times \mathfrak{S}_{n-p} \to \omega_J^I$$
$$\text{par} \quad \Phi_J^I(\sigma',\sigma'')(j_s) = i_{\sigma'(s)}, \quad \Phi_J^I(\sigma',\sigma'')(\bar\jmath_s) = \bar\imath_{\sigma''(s)}.$$

Manifestement Φ_J^I est injective, et il est à peu près aussi manifeste qu'elle est surjective ; de toute façon, pour les besoins de la preuve nous allons exhiber une réciproque à Φ_J^I. Attention toutefois : Φ_J^I n'est pas un morphisme de groupes ! d'ailleurs ω_J^I n'est même pas un groupe.

A tout $(\sigma',\sigma'') \in \mathfrak{S}_p \times \mathfrak{S}_{n-p}$, on associe une permutation $\Psi(\sigma',\sigma'') \in \mathfrak{S}_n$ définie par

$$\Psi(\sigma',\sigma'') = \begin{pmatrix} 1 & \cdots & p & p+1 & \cdots & p+(n-p) \\ \sigma'(1) & \cdots & \sigma'(p) & p+\sigma''(1) & \cdots & p+\sigma''(n-p) \end{pmatrix}.$$

Pour tout $I \in \mathcal{P}_p$, on définit une permutation $\rho_I \in \mathfrak{S}_n$ par

$$\rho_I = \begin{pmatrix} 1 & \cdots & p & p+1 & \cdots & p+(n-p) \\ i_1 & \cdots & i_p & \bar\imath_1 & \cdots & \bar\imath_{n-p} \end{pmatrix}.$$

Je prétends que

$$\sigma = \rho_I \circ \Psi(\sigma', \sigma'') \circ \rho_J^{-1}, \tag{2.5.1}$$

et je laisse au lecteur le soin de le démontrer. Si on n'était pas encore convaincu du caractère bijectif de Φ_I^J, on peut maintenant arguer du fait que $\rho_I^{-1}\sigma\rho_J$ est bien un $\Psi(\sigma', \sigma'')$.

Enfin on montre l'identité voulue sur les signatures en calculant des nombres d'inversions. D'une part, $\varepsilon(\Psi(\sigma', \sigma'')) = \varepsilon(\sigma')\varepsilon(\sigma'')$ car

$$\mathcal{I}(\Psi(\sigma', \sigma'')) = \big(\mathcal{I}(\sigma')\big) \cup \big((p,p) + \mathcal{I}(\sigma'')\big)$$

($\mathcal{I}$ désigne l'ensemble des inversions, dont il faut calculer le cardinal pour définir le nombre d'inversions). D'autre part,

$$\begin{aligned}
\mathcal{I}(\rho_I) &= \big\{(r, s') \in [\![1,p]\!] \times [\![p+1,n]\!] : i_r > \bar{\imath}_{s'-p}\big\} \\
&\simeq \coprod_{1 \leqslant r \leqslant p} \big\{s \in [\![1, n-p]\!] : \bar{\imath}_s < i_r\big\} \\
&\simeq \coprod_{1 \leqslant r \leqslant p} \bar{I} \cap [\![1, i_r - 1]\!] \\
&\simeq \coprod_{1 \leqslant r \leqslant p} [\![1, i_r - 1]\!] \setminus \{i_1, \ldots, i_{r-1}\}
\end{aligned}$$

donc

$$I(\rho_I) = \sum_{1 \leqslant r \leqslant p} \big(i_r - 1 - (r-1)\big) = \sum_{1 \leqslant r \leqslant p} i_r - \sum_{1 \leqslant r \leqslant p} r = |I| - \frac{p(p+1)}{2}.$$

□

3 – Groupe alterné

(3.1) Proposition. *$\mathfrak{A}_n$ est engendré par les 3-cycles.*
Preuve. Puisque le groupe symétrique est engendré par les transpositions, il suffit de savoir écrire le produit d'un nombre pair de transpositions comme produit de 3-cycles. Dans

$$\tau_1\tau_2 \cdots \tau_{2k-1}\tau_{2k},$$

chaque $\tau_{2i-1}\tau_{2i}$ $(1 \leqslant i \leqslant k)$ est ou bien $(12)(23) = (123)$, ou bien $(12)(34) = (123)(234)$. □

(3.2) Proposition. *Considérons une classe de conjugaison paire dans $\mathfrak{S}_n$, correspondant à la partition $n = b_1 + \cdots + b_r$ (chaque $b_i \in [\![1,n]\!]$). Cette classe constitue une classe de conjugaison dans $\mathfrak{A}_n$ si l'un au moins des b_i est pair ou s'il existe $i \neq j$ tels que $b_i = b_j$, et se scinde en deux classes de conjugaison sinon.*

J'appelle classe de conjugaison paire une classe dont tous les éléments sont de signature $+1$. Ceci équivaut à la condition

$$\sum\nolimits_{i=1}^{r} (b_i - 1) \equiv 0 \mod 2.$$

Preuve. Soit $\kappa_1, \ldots, \kappa_r$ des cycles à supports disjoints de longueurs $b_1, \ldots, b_r$, et $\sigma = \kappa_1 \cdots \kappa_r$. On a pour tout $s \in \mathfrak{S}_n$ et tout $i = 1, \ldots, k$,

$$s\kappa_1 \cdots \kappa_r s^{-1} = s\kappa_i\kappa_1 \cdots \kappa_r\kappa_i^{-1}s^{-1}.$$

Si b_i est pair, ou bien s ou bien $s\kappa_i$ est impair, donc toute permutation conjuguée à σ peut être obtenue en conjuguant par une permutation paire.

Si $b_i = b_j$, on utilise la même idée avec un élément du stabilisateur de σ d'un autre type. On peut supposer grâce à ce qui précède que $b = b_i = b_j$ est impair. Notant $\kappa_i = (x_1 \cdots x_b)$ et $\kappa_j = (y_1 \cdots y_b)$, on pose

$$\tau = (x_1 y_1) \cdots (x_b y_b).$$

C'est une permutation impaire si b est impair, qui laisse $\kappa_1 \cdots \kappa_r$ stable par conjugaison. Ainsi pour tout $s \in \mathfrak{S}_n$,

$$s\sigma s^{-1} = s\tau\sigma\tau^{-1}s^{-1}.$$

Ceci termine la preuve de la première partie de l'énoncé.

Pour démontrer l'autre partie, il faut se convaincre que si les b_i sont deux à deux distincts, alors

$$s\kappa_1 \cdots \kappa_r s^{-1} = \kappa_1 \cdots \kappa_r \iff s = \kappa_1^{\alpha_1} \cdots \kappa_r^{\alpha_r}$$

(si on veut, ça découle de la preuve du Théorème (1.1)). Ainsi, si de plus les b_i tous impairs, le stabilisateur de σ pour la conjugaison est un sous-groupe de $\mathfrak{A}_n$. On en déduit que pour toute transposition τ, σ et $\tau\sigma\tau^{-1}$ ne sont pas conjuguées dans $\mathfrak{A}_n$. En revanche, toute permutation conjuguée à σ dans $\mathfrak{S}_n$ est conjuguée dans $\mathfrak{A}_n$ ou bien à σ ou bien à $\tau\sigma\tau^{-1}$. □

(3.3) Exercice. On considère l'action de $\mathfrak{S}_n$ sur lui-même par conjugaison.
1) Montrer que si κ est un cycle de longueur b, alors $\mathrm{Stab}(\kappa) = \langle\kappa\rangle \cong \mathbf{Z}/b\mathbf{Z}$.
2) Montrer que si $\kappa_1, \ldots, \kappa_r$ sont des cycles de longueurs $b_1, \ldots, b_r$ deux à deux distinctes, alors

$$\mathrm{Stab}(\kappa_1 \cdots \kappa_r) = \langle\kappa_1, \ldots, \kappa_r\rangle \cong \mathbf{Z}/b_1\mathbf{Z} \times \cdots \times \mathbf{Z}/b_r\mathbf{Z}.$$

3) Déterminer le stabilisateur d'une permutation en général.

IV – Groupes abéliens de type fini (grabdetf)

Dans le programme 2018 de l'agreg : « matrices à coefficients dans un anneau commutatif. Opérations élémentaires sur les lignes et les colonnes, déterminant, inversibilité » ; « groupes abéliens de type fini ».

Pour cette partie, je recommande vivement les magnifiques notes de Fokko du Cloux.

1 – Groupes abéliens de type fini

(1.1) Définition. Groupe de type fini, abélien de type fini, abélien libre de type fini. Quotient du groupe libre à n générateurs, de $\mathbf{Z}^n$, isomorphe à $\mathbf{Z}^n$.

(1.2) Exemples. $\mathbf{Z}$, $\mathbf{Z}/n\mathbf{Z}$ sont des groupes abéliens de type fini. Ne sont pas de type fini en revanche : $(\mathbf{Z}[X],+)$ groupe additif des polynômes à coefficients entiers. $(\mathbf{Q},+)$ (donner quelques indications). $(\mathbf{R},+)$ et $(\mathbf{S}^1,\times)$ qui n'est autre que $\mathbf{R}/\mathbf{Z}$ *via* l'exponentielle.
Exercice. Tout sous-groupe de type fini de $(\mathbf{Q},+)$ est monogène. Dans $(\mathbf{R},+)$, $\langle a,b\rangle$ est monogène si et seulement si a et b sont commensurables.
Attention, on peut avoir a et b non commensurables et $\langle a,b\rangle \subsetneq \mathbf{R}$; exemple, $\left\langle 1,\sqrt{2}\right\rangle$ n'est certainement pas $\mathbf{R}$ tout entier.

(1.3) Théorème. *Tout groupe abélien de type fini s'écrit de manière unique*

$$\mathbf{Z}^r \times \mathbf{Z}/d_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d_s\mathbf{Z}, \tag{1.3.1}$$

avec $r,s \in \mathbf{N}$, *et* $1 < d_1 | \cdots | d_s$.

Exemple. $\mathbf{Z}/18\mathbf{Z} \times \mathbf{Z}/15\mathbf{Z} \times \mathbf{Z}/75\mathbf{Z}$.

Pour démonter l'existence, il suffit de traiter le cas d'un quotient de $\mathbf{Z}^n$, ce qui revient à comprendre la structure des sous-groupes de $\mathbf{Z}^n$. Pour démontrer l'unicité il faut se méfier un peu plus.

(1.4) Proposition. *Tout sous-groupe de* $(\mathbf{Z}^n,+)$ *est un groupe abélien de type fini.*

Cet énoncé traduit le fait que $\mathbf{Z}$ est un anneau noethérien, comme tous les anneaux principaux, *cf.* [Laszlo, p. 23]. En fait les sous-groupes de $\mathbf{Z}^n$ sont également libres, comme l'indique la preuve suivante ; c'est visible dans l'énoncé plus précis (1.5), que l'on déduit de (1.4) en utilisant seulement la partie "type fini".

Preuve. Par récurrence sur n. Si $n \leqslant 1$ c'est non trivial, mais on connaît. Si $n > 1$, soit $e_1,\ldots,e_n$ la base canonique, $N < \mathbf{Z}^n$ notre sous-groupe, et

$$N_1 = N \cap (\mathbf{Z}e_1 \oplus \cdots \oplus \mathbf{Z}e_{n-1}).$$

Si $N_1 = N$, alors $N < \mathbf{Z}^{n-1}$ et on conclut par récurrence ; sinon, N/N_1 est un sous-groupe non nul de $\mathbf{Z}^n/(\mathbf{Z}e_1 \oplus \cdots \oplus \mathbf{Z}e_{n-1}) \cong \mathbf{Z}$, donc monogène comme tout sous-groupe d'un groupe monogène.

Soit a générateur de N/N_1, $v \in N$ un représentant. Pour tout $x \in N$, il existe un unique $n \in \mathbf{Z}$ tel que $\bar{x} = n.a \Leftrightarrow x - n.v \in N_1$. Ainsi tout $x \in N$ s'écrit de manière unique $x_1 + n.v$, $x_1 \in N_1$, $n \in \mathbf{Z}$ (le v étant choisi au départ). Puisque $N_1 < \mathbf{Z}^{n-1}$ on peut lui appliquer l'hypothèse de récurrence, ce qui permet de conclure. □

(1.5) Proposition. *Tout sous-groupe de $(\mathbf{Z}^n, +)$ s'écrit canoniquement*

$$d_1\mathbf{Z} \times \cdots \times d_n\mathbf{Z} \subset \mathbf{Z} \times \cdots \times \mathbf{Z} = \mathbf{Z}^n,$$

dans une base adaptée de $\mathbf{Z}^n$ (cette dernière pas nécessairement unique), avec $0 \leqslant d_1 | \cdots | d_n$ (les premiers d_1 sont éventuellement 1, les derniers éventuellement 0).

Plus précisément, pour tout sous-groupe $N < \mathbf{Z}^n$ il existe un automorphisme $\phi : \mathbf{Z}^n \cong \mathbf{Z}^n$ donné par une matrice de $\mathrm{GL}_n(\mathbf{Z})$ tel que $\phi(N)$ soit comme dans la Proposition. La preuve s'appuie sur les résultats de la Section 2 et sera donnée là-bas.

(1.6) Corollaire. *Tout sous-groupe de $\mathbf{Z}^n$ est libre, engendré par au plus n éléments.*

La Proposition (1.5) donne l'existence d'une décomposition (1.3.1) pour un groupe abélien de type fini, mais ne suffit pas pour avoir l'unicité, en dépit de l'unicité d'écriture pour les sous-groupes de $\mathbf{Z}^n$ dans la Proposition (1.5).

En effet, on peut toujours prendre deux présentations différentes $\mathbf{Z}^n \twoheadrightarrow M$ et $\mathbf{Z}^m \twoheadrightarrow M$; il n'est pas très difficile de supposer $n = m$ en ajoutant des générateurs triviaux, mais *a priori* rien n'interdit que deux telles présentations donnent des décompositions différentes ; il faut déterminer à quelle condition deux sous-groupes $H_1, H_2 < \mathbf{Z}^n$ donnent des quotients isomorphes, autrement dit quelle condition un diagramme à lignes exactes

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H_1 & \longrightarrow & \mathbf{Z}^n & \longrightarrow & Q & \longrightarrow & 0 \\ & & & & \| & & \| & & \\ 0 & \longrightarrow & H_2 & \longrightarrow & \mathbf{Z}^n & \longrightarrow & Q & \longrightarrow & 0 \end{array}$$

impose sur H_1 et H_2. 1) On pourrait dire quelque chose si on savait que $\mathbf{Z}^n = Q \times H_1$ et $\circlearrowleft_2$, mais les suites exactes ne sont même pas scindées en général : typiquement, tous les morphismes $\mathbf{Z}/2\mathbf{Z} \to \mathbf{Z}$ sont triviaux ! 2) On est hors du domaine d'application du lemme des cinq [Laszlo, p. 18], qui étant donné un diagramme de groupes abéliens de type fini

$$\begin{array}{ccccccccc} M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & M_4 & \longrightarrow & M_5 \\ \downarrow f_1 & & \downarrow f_2 & & \downarrow f_3 & & \downarrow f_4 & & \downarrow f_5 \\ N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & N_4 & \longrightarrow & N_5 \end{array}$$

dit des choses sur f_3 sachant des choses sur f_1, f_2, f_4 ou f_5, f_2, f_4. Dans notre situation, on n'a *a priori* même pas de flèche f_2.

La preuve de l'unicité se fait pas à pas en s'appuyant sur la théorie de la dimension pour les espaces vectoriels. On verra qu'au bout du compte, $\mathbf{Z}^n/H_1 \cong \mathbf{Z}^n/H_2$ ssi $H_1 \cong H_2$, mais il faut bien le démontrer !

2 – Matrices à coefficients dans un anneau principal

(2.1) Pivot de Gauss et théorème des facteurs invariants. Voir la section correspondante dans le cours d'algèbre linéaire.

(2.2) Exemple.

$$\begin{pmatrix} -2 & -11 & -7 \\ 5 & 18 & 11 \\ -6 & -20 & -12 \end{pmatrix} \sim \begin{matrix} L_2 + 2L_1 \\ L_1 \\ L_3 - 3L_1 \end{matrix} \begin{pmatrix} 1 & -4 & -3 \\ -2 & -11 & -7 \\ 0 & 13 & 9 \end{pmatrix}$$
$$\sim \begin{matrix} \\ L_2 + 2L_1 \\ \\ \end{matrix} \begin{pmatrix} 1 & -4 & -3 \\ 0 & -19 & -13 \\ 0 & 13 & 9 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 19 & 13 \\ 0 & 13 & 9 \end{pmatrix}$$
$$\sim \begin{matrix} \\ -2L_2 + 3L_3 \\ 13L_2 - 19L_3 \end{matrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & -2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

C'est plus intéressant comme ça qu'en étant malin pour fabriquer un 1 au premier coup avec L_2 et L_3, car on voit ainsi un vrai algorithme d'Euclide en cours de route :

$$\begin{aligned} 19 &= 13 \times 1 + 6 & 6 &= 19 - 13 \\ 13 &= 6 \times 2 + 1 & 1 &= 13 - 2 \cdot 6 \\ & & &= 13 - 2(19 - 13) = -2 \cdot 19 + 3 \cdot 13. \end{aligned}$$

(2.3) Interprétation géométrique du pivot de Gauss. Si on a $F \in \mathcal{M}_{n,m}(\mathbf{Z})$ dont les colonnes $F_1, \ldots, F_m$ sont les coordonnées de vecteurs $f_1, \ldots, f_m \in \mathbf{Z}^n$ dans une base $\mathcal{B}$:

(i) pour $P \in \mathrm{GL}_n(\mathbf{Z})$, les colonnes de la matrice $P^{-1}F$ sont les coordonnées de $f_1, \ldots, f_m \in \mathbf{Z}^n$ dans la base $\mathcal{B}'$ telle que $P = \mathrm{Mat}(\mathcal{B}, \mathcal{B}')$;

(ii) pour $Q \in \mathrm{GL}_m(\mathbf{Z})$, les colonnes de la matrice FQ sont les coordonnées des vecteurs $f'_1, \ldots, f'_m \in \mathbf{Z}^n$,

$$f'_j = q_{1j} f_1 + \cdots + q_{mj} f_j,$$

et on a

$$\langle f_1, \ldots, f_m \rangle_{\mathbf{Z}^n} = \langle f'_1, \ldots, f'_m \rangle_{\mathbf{Z}^n}$$

puisque pour tout $\Lambda \in \mathbf{Z}^m$ on a $F\Lambda = (FQ)(Q^{-1}\Lambda)$ (et $(FQ)(\Lambda) = F(Q\Lambda)$!).

Quand on a une matrice sous forme normale, la famille correspondante est libre une fois débarassée des vecteurs nuls correspondant aux d_i nuls.

(2.4) Interprétation d'un quotient de $\mathbf{Z}^n$ comme groupe abélien défini par générateurs et relations. $\mathbf{Z}^n$ est le groupe abélien engendré par $e_1, \ldots, e_n$ sans aucune relation. Quotienter par (le sous-groupe engendré par) $(a_1, \ldots, a_n)$ revient à imposer la relation

$$a_1.e_1 + \cdots + a_n.e_n = 0.$$

3 – Unicité de la décomposition

3.1 – Rang

Ici on s'attache à démontrer la canonicité du nombre r de copies de $\mathbf{Z}$ dans la décomposition (1.3.1). Le fond de l'histoire, c'est que

$$r(M) = \dim_{\mathbf{Q}}\big(M \otimes_{\mathbf{Z}} \mathbf{Q}\big).$$

(3.1) Pour M groupe abélien, le sous-groupe de torsion de M est

$$M_{\text{tors}} = \big\{\text{éléments d'ordre finis}\big\} = \big\langle\text{éléments d'ordre finis}\big\rangle.$$

On dit que M est sans torsion si $M_{\text{tors}} = \{0\}$.

(3.2) Proposition. *Un groupe abélien de type fini est libre si et seulement si il est sans torsion.*

Preuve. C'est un corollaire de la partie existence du Théorème (1.3), donnée par la Proposition (1.5). Si M est sans torsion, toute écriture (1.3.1) donne $M \simeq \mathbf{Z}^r$, ce qui dit que M est libre (même si l'unicité de r n'est pas encore acquise à ce stade).

Réciproquement, un groupe abélien libre est manifestement sans torsion. □

(3.2.1) Attention : c'est complètement faux si on retire l'hypothèse de type fini. En effet, le groupe $(\mathbf{Q}, +)$ est sans torsion mais n'est pas libre. (Même si *a contrario*, $\langle 1/2, 1/3\rangle$ est bien libre, puisque c'est $\mathbf{Z}.1/6$).
(3.2.2) « Tout module de type fini sur un un anneau principal sans torsion est libre. » $\rightsquigarrow$ c'est un énoncé de géométrie algébrique !

(3.3) Lemme. *Des vecteurs $v_1, \ldots, v_s \in \mathbf{Q}^n$ sont linéairement indépendants sur $\mathbf{Z}$ ssi ils le sont sur $\mathbf{Q}$.*

(3.4) Proposition. *Soit M abélien libre de type fini. Toutes les bases de M ont le même cardinal, appelé* rang *de M.*

Preuve. On peut supposer $M = \mathbf{Z}^n \subset \mathbf{Q}^n$. Par le Lemme (3.3), toute famille libre de $\mathbf{Z}^n$ est une famille libre de $\mathbf{Q}^n$, donc est constituée d'au plus n vecteurs d'après la théorie de la dimension. Ainsi toute famille finie extraite d'une base de $\mathbf{Z}^n$ est de cardinal au plus n, ce qui prouve que toute base de $\mathbf{Z}^n$ est finie (pas OSD !).

Soit $\mathcal{B}$ base de $\mathbf{Z}^n$ à m élements : $m \leqslant n$ par ce qui précède. Si $m < n$, on aurait $\mathbf{Z}^n \simeq \mathbf{Z}^m < \mathbf{Q}^m$ donc toutes les bases de $\mathbf{Z}^n$ auraient au plus m éléments, en contradiction avec l'existence manifeste d'une base à n éléments de $\mathbf{Z}^n$. □

(3.5) Conclusion. L'entier $r(M)$ est le rang du groupe abélien libre de type fini M/M_{tors}, qui est un invariant intrinsèque de M.

3.2 – Facteurs invariants

Ici on démontre la canonicité des facteurs invariants $1 < d_1 | \cdots | d_s$ dans la décomposition (1.3.1). On peut supposer $M = M_{\text{tors}}$, canoniquement défini à partir de M. L'unicité provient du fait que, pour tout p premier,

$$\dim_{\mathbf{F}_p}\big(\mathbf{Z}/d\mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{F}_p\big) = \begin{cases} 1 & \text{si } p|d \\ 0 & \text{si } p \not| d. \end{cases}$$

Attention : $\mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{F}_p \cong \mathbf{F}_p$, donc si on ne suppose pas $M = M_{\text{tors}}$ il faut tenir compte des facteurs libres dans les comptes.

Rappel. On a en général $M \otimes_A A/I \cong M/IM$, donc pour ce qui nous intéresse ici

$$\mathbf{Z}/a\mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{Z}/b\mathbf{Z} \cong \mathbf{Z}/\text{pgcd}(a,b)\mathbf{Z}.$$

(3.6) Soit M groupe abélien, p un nombre premier. La multiplication externe $\mathbf{Z} \times M \to M$ induit une structure de $\mathbf{F}_p$-espace vectoriel sur le quotient M/pM.

Si $M = \mathbf{Z}/d\mathbf{Z}$,

$$\dim_{\mathbf{F}_p}\big(M/pM\big) = \begin{cases} 1 & \text{si } p|d \\ 0 & \text{si } p \not| d. \end{cases}$$

En effet, si p divise d, alors $M/pM \cong (\mathbf{Z}/d\mathbf{Z})/p(\mathbf{Z}/d\mathbf{Z}) \cong \mathbf{Z}/p\mathbf{Z}$ est un groupe monogène non trivial, et si p ne divise pas n, alors $\bar{p}$ est un générateur de M donc $M/pM = \{0\}$ (voir (3.6) pour les deux).

(3.7) Unicité des facteurs invariants. Soit M groupe abélien *fini*. On sait à présent qu'il existe des entiers $1 < d_1 | \cdots | d_s$ tels que

$$M \cong \mathbf{Z}/d_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d_s\mathbf{Z}. \tag{3.7.1}$$

Montrons par récurrence sur l'ordre de M que les entiers $d_i > 1$ sont uniquement déterminés par M.

Si $|M| = 1$ c'est trivial ($s = 0$ et il n'y a pas de d_i). Sinon, choisissons p réalisant la borne

$$\sup_{p \text{ premier}} \Big(\dim_{\mathbf{F}_p}(M/pM)\Big)\ ; \tag{3.7.2}$$

l'ensemble des tels p est visiblement indépendant de tout choix (il n'y a qu'à regarder la définition du sup !). Il faut quand même se convaincre que ce sup est atteint. L'existence d'une décomposition (3.7.1) permet de le voir : d'après (3.6) la dimension de M/pM est $\leqslant s$, et cette dimension est réalisée pour tous les p divisant d_1, et donc tous les d_i. En particulier le supremum détermine le nombre s de facteurs cycliques dans n'importe quelle écriture.

Partant de la décomposition, (3.7.1), on a

$$\begin{aligned} pM \cong p\big(\mathbf{Z}/d_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d_s\mathbf{Z}\big) &\cong p\mathbf{Z}/d_1\mathbf{Z} \times \cdots \times p\mathbf{Z}/d_s\mathbf{Z} \\ &\cong \mathbf{Z}/(d_1/p)\mathbf{Z} \times \cdots \times \mathbf{Z}/(d_s/p)\mathbf{Z}. \end{aligned} \tag{3.7.3}$$

C'est une décomposition du type voulu une fois qu'on s'est débarassé des facteurs triviaux, *i.e.* ceux pour lesquels $d_i/p = 1$. Puisque $|pM| < |M|$ (sinon $M/pM = \{0\}$ pour tout p, donc $M = \{0\}$), on a une décomposition *unique*

$$pM \cong \mathbf{Z}/d'_1\mathbf{Z} \times \cdots \times p\mathbf{Z}/d'_{s'}\mathbf{Z},$$

qui est nécessairement (3.7.3). Ceci détermine $d_1 = \cdots = d_{s-s'} = p$ et $d_{s-s'+i} = pd'_i$ pour $i = 1, \ldots, s'$. □