

PARTITION D'UN ENTIERS ET STRUCTURE DES GROUPES ABÉLIENS FINIS

CORRECTION

1. ALGÈBRE LINÉAIRE

- (1) La réflexivité est triviale, et la symétrie également puisque $P^{-1} \in \mathbf{GL}_n(\mathbb{C})$. Soient A, B et $C \in \mathbf{M}_n(\mathbb{C})$ et $P, Q \in \mathbf{GL}_n(\mathbb{C})$ telles que

$$A = PBP^{-1} \quad ; \quad B = QCQ^{-1}$$

donc

$$A = P(QCQ^{-1})P^{-1} = (PQ)C(PQ)^{-1}$$

avec $PQ \in \mathbf{GL}_n(\mathbb{C})$, donc A et C sont semblables, d'où la transitivité.

- (2) f est semblable à ν donc il existe g un isomorphisme de \mathbb{C}^n tel que $f = g\nu g^{-1}$. Si ν est nilpotent, alors il existe $n \in \mathbb{N}$ tel que $\nu^n = 0$. On a donc

$$f^n = (g\nu g^{-1})^n = g\nu^n g^{-1} = 0$$

donc f est nilpotente.

- (3) Par la réduction de Jordan, M est semblable à une matrice par blocs

$$J = \begin{pmatrix} J_{r_1,0} & & & \\ & J_{r_2,0} & & \\ & & \ddots & \\ & & & J_{r_s,0} \end{pmatrix}$$

avec $r_1 \leq r_2 \leq \dots \leq r_s$. J est nilpotente (triangulaire supérieure à diagonale nulle), donc la réciproque de la question précédente est vraie.

- (4) Deux isomorphismes nilpotents ne sont pas dans la même classe si leurs décompositions de Jordan respectives diffèrent. On voit donc qu'il y a autant de classes de similitude contenant des endomorphismes nilpotents que d'uplets (r_1, \dots, r_s) avec $r_1 \leq \dots \leq r_s$ et $r_1 + \dots + r_s = n$, c'est-à-dire $P(n)$!
- (5) Soient J_M et J_N les décompositions de Jordan respectives de M et N . Alors il existe $P, Q \in \mathbf{GL}_n(\mathbb{C})$ telles que

$$M = PJ_M P^{-1} \quad ; \quad N = QJ_N Q^{-1}.$$

Si M et N sont semblables alors il existe $R \in \mathbf{GL}_n(\mathbb{C})$ telle que $M = RNR^{-1}$, donc $M = (RQ)J_N(RQ)^{-1}$ et $RQ \in \mathbf{GL}_n(\mathbb{C})$ donc J_N est une décomposition de Jordan de M et par unicité, $J_N = J_M$.

Réciproquement, si $J_N = J_M$, alors $J_M = J_N = Q^{-1}NQ$ et

$$M = PQ^{-1}NQP^{-1} = (PQ^{-1})^{-1}N(PQ^{-1})$$

et $(PQ^{-1})^{-1} \in \mathbf{GL}_n(\mathbb{C})$ donc M et N sont semblables.

2. PERMUTATIONS

- (6) La classe de conjugaison d'une permutation $\sigma \in S_n$ est $\{\rho \circ \sigma \circ \rho^{-1} \mid \rho \in S_n\}$.
- (7) On rappelle que deux permutations sont conjuguées dans S_n si et seulement si les listes des longueurs des cycles à supports disjoints qui les composent sont les mêmes. Cela revient au même que de dire que deux permutations sont conjuguées dans S_n si et seulement si les listes des longueurs des cycles à supports disjoints qui les composent sont les mêmes et le nombre de points fixe est le même. Si ℓ_1, \dots, ℓ_k sont les longueurs des cycles à supports disjoints dans l'ordre croissant et m le nombre de points fixes, alors en posant

$$i_j = \begin{cases} 1 & \text{si } j \leq m \\ \ell_{j+1-m} & \text{si } j > m \end{cases}$$

la donnée de (i_1, \dots, i_{k+m}) avec $i_1 \leq \dots \leq i_{k+m}$ caractérise une classe de conjugaison de permutation. Il y a autant de classes de conjugaison que de tels uplets, c'est-à-dire $P(k+m) = P(n)$.

3. GROUPES ABÉLIENS FINIS

- (8) Soit a un générateur de G . Soit $\varphi: G \rightarrow \mathbb{Z}/n\mathbb{Z}$ défini par $\varphi(a) = \bar{1}$. Soit $b \in G$. Il existe un unique $0 \leq m < n$ tel que $b = a^m$, donc $\varphi(b) = \overline{m}$ et φ est bien définie sur tout G . Si $b, b' \in G$, alors il existe $m, m' < n$ tels que $b = a^m$ et $b' = a^{m'}$, d'où

$$\varphi(bb') = \varphi(a^{m+m'}) = \overline{m+m'} = \varphi(b) + \varphi(b').$$

donc φ est un morphisme, clairement bijectif.

- (9) Si ce n'est pas le cas, alors pour tout $m \in \mathbb{Z}$, alors $(m, *, \dots, *) \in G$ et il y a un nombre infini de tels uplets.
- (10) Nous allons montrer que le nombre de groupes abéliens d'ordre n à isomorphisme près vaut $P(\alpha_1) \cdots P(\alpha_r)$.
- (a) Si $r = 1$, alors $n = p_1^{\alpha_1}$. Les d_i sont de la forme $p_1^{\beta_i}$, avec par conséquent $\alpha_1 = \sum_{i=1}^r \beta_i$ et $\beta_1 \leq \dots \leq \beta_r$ (condition de divisibilité). Réciproquement, toute partition de α_1 permet de construire un groupe abélien de cardinal n .
- (b) Si $r \geq 2$, considérons une partition $\{\beta_{i,j}\}_{j=1}^{s_i}$ de chaque exposant α_i . Soit $s = \max_{i=1, \dots, r}(s_i)$. Quitte à rajouter des 0 au début des partitions, on peut supposer qu'elles sont toutes de taille $s = \max_{i=1, \dots, r}(s_i)$. Considérons alors $d_j = p_1^{\beta_{1,j}} \cdots p_r^{\beta_{r,j}}$ pour $j \in \{1, \dots, s\}$. On a bien $\prod_{i=1}^r d_j = n$ et $d_i \mid d_{i+1}$ (car $\beta_{i,j} \leq \beta_{i+1,j}$). On en déduit donc le résultat.
- (11) $250 = 5^3 \times 2$, donc il y a $P(3)P(1) = 3$ groupes abéliens d'ordre 250 à isomorphisme près : $\mathbb{Z}/250\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$...

4. STRUCTURE DES GROUPES ABÉLIENS FINIS

4.1. Exposant d'un groupe.

(12) Soit $g \in G$. Une conséquence au théorème de Lagrange assure que l'ordre de g divise l'ordre de G , i.e. n , donc s'écrit sous la forme $\prod_{i=1}^r p_i^{\gamma_i}$.

(13) On va montrer que $o(h_0)$ est le produit des $p_i^{\beta_i}$. Comme G est abélien

$$h_0^{\prod_{i=1}^r p_i^{\beta_i}} = h_1^{p_1^{\beta_1}} \cdots h_r^{p_r^{\beta_r}} = 1$$

et $o(h_0)$ divise $\prod_{i=1}^r p_i^{\beta_i}$. Réciproquement, $o(h_0) = \prod_{i=1}^r p_i^{\gamma_i}$. Si $o(h_0) \neq \prod_{i=1}^r p_i^{\beta_i}$, il existe $j \in \{1, \dots, r\}$ tel que $\gamma_j < \beta_j$. On a donc $o(h_0)$ qui est un multiple de

$$\ell = p_1^{\beta_1} \cdots p_{j-1}^{\beta_{j-1}} p_j^{\gamma_j} p_{j+1}^{\beta_{j+1}} \cdots p_r^{\beta_r}.$$

On en déduit donc que

$$1 = h_0^\ell = h_1^{p_1^{\beta_1}} \cdots h_{j-1}^{p_{j-1}^{\beta_{j-1}}} h_j^{p_j^{\gamma_j}} h_{j+1}^{p_{j+1}^{\beta_{j+1}}} \cdots h_r^{p_r^{\beta_r}} = h_j^{p_j^{\gamma_j}}$$

ce qui est absurde, puisque h_j est d'ordre $p_j^{\beta_j} > p_j^{\gamma_j}$. Finalement

$$o(h_0) = \prod_{i=1}^r p_i^{\beta_i}.$$

(14) Si $j \in \{1, \dots, r\}$, alors $g^{\prod_{i=1, i \neq j}^r p_i^{\gamma_i}}$ est d'ordre $p_j^{\beta_j}$, donc $\gamma_j \leq \beta_j$ par maximalité de β_j , et ceci est valable pour tout j , ce qui montre que $o(g)$ divise $o(h_0)$. h_0 est donc un élément de G d'ordre l'exposant de G .

4.2. Dévissage de groupes à l'aide d'une rétraction.

(15) Soit $g \in G$ tel que $\pi \times \rho(g) = (\bar{1}, 1)$. Comme $\pi(g) = \bar{1}$, alors $g \in H$, d'où (par propriété de ρ) $1 = \rho(g) = g$. Ainsi, $\pi \times \rho$ est injectif.

(16) On a

$$\left\{ \begin{array}{l} \pi(g) = \pi(g') \\ \rho(g) = h' \end{array} \right\} \iff \left\{ \begin{array}{l} \exists h \in H, g = hg' \\ \rho(g) = h' \end{array} \right\} \iff \left\{ \begin{array}{l} \exists h \in H, g = hg' \\ h\rho(g') = h' \end{array} \right\} \iff \left\{ \begin{array}{l} g = hg' \\ h = \frac{h'}{\rho(g')} \end{array} \right\}$$

Il suffit donc de prendre $g = g'h'/\rho(g')$.

(17) Si $G = \{1, i, -1, -i\}$ et $H = \{-1, 1\}$, alors $G/H \cong \{-1, 1\}$ et $G/H \times H$ ne contient que des éléments d'ordre 2 alors que G contient un élément d'ordre 4.

4.3. Prolongement des caractères.

(18) Le procédé est assuré de terminer puisque G est fini...

(19) (a) G/H est fini aussi, donc il existe un n tel que $\bar{a} \in G/H$ vérifie $\bar{a}^n = \bar{1}$ (nous allons le prendre minimal, i.e égal à l'ordre de \bar{a} , pour la prochaine question). Donc $\bar{a}^n = \bar{1}$, c'est-à-dire que $a^n \in H$.

- (b) (i) Supposons que $ha^r = 1$. Alors $a^r = h^{-1} \in H$, donc r est un multiple de l'ordre de \bar{a} dans G/H , disons $r = ns$. Ainsi, $1 = h(a^n)^s$. On peut donc appliquer χ puisque tous les éléments sont dans H et

$$1 = \chi(h)\chi(a^n)^s = \chi(h)(a^n)^s = \chi(h)\alpha^r.$$

- (ii) Comme $ha^r = h'a^{r'}$, alors $h^{-1}h'a^{r'-r} = 1$ et par ce qui précède,

$$\chi(h^{-1}h')\alpha^{r'-r} = 1$$

d'où

$$\chi(h')\alpha^{r'} = \chi(h)\alpha^r.$$

4.4. Structure des groupes abéliens finis.

Existence.

- (20) Si le résultat à montrer est juste, l'exposant de G est le maximum des d_i (ou d_n).
- (21) (a) a existe d'après la partie 4.1.
- (b) H est cyclique (car monogène et fini) d'ordre e , donc isomorphe à $\mathbb{Z}/e\mathbb{Z}$. De même, μ_e est cycle d'ordre e donc isomorphe à $\mathbb{Z}/e\mathbb{Z}$. On en déduit immédiatement que $H \cong \mu_e$.
- (c) Le morphisme $\chi: H \rightarrow \mathbb{C}^*$ est un caractère de H , donc peut être prolongé en un caractère

$$\bar{\chi}: G \rightarrow \mathbb{C}^*.$$

Soit $g \in G$. On a $g^e = 1$, donc $\bar{\chi}(g)^e = 1$. Ainsi, $\text{Im}(\bar{\chi}) \subset \mu_e$. Or, $H \subset G$, donc $\text{Im}(\bar{\chi}) \supset \bar{\chi}(H) = \chi(H) = \mu_e$. Finalement

$$\text{Im}(\bar{\chi}) = \mu_e.$$

- (d) $\rho = \chi^{-1} \circ \bar{\chi}: G \rightarrow G$ est un morphisme de groupes (comme composée de morphismes de groupes). Soit $h \in H$. On a $\bar{\chi}(h) = \chi(h)$ puisque $\bar{\chi}$ prolonge χ , d'où $\rho(h) = h$. Ainsi, $\rho|_H = \text{id}_H$. De plus, $\chi^{-1}: \mu_e \rightarrow H$, donc $\text{Im}(\rho) \subset H$. Ainsi, ρ est bien une rétraction de G sur H .
- (e) Soit e' l'exposant de G' . Soit $b \in G$ tel que $\pi(b) \in G'$ soit d'ordre e' . Comme $b^e = 1$ passe modulo H :

$$\pi(b)^e = \pi(b^e) = \pi(1) = 1 \Rightarrow e' \mid e.$$

- (22) On pose $d_n = e$ et on itère la question précédente avec G' qui est d'ordre strictement inférieur à celui de G et divisant celui de G , et on pose $d_{n-1} = e'$. On réitère le procédé et on obtient donc une suite $d_1 \mid \dots \mid d_n$ telle que

$$G \cong \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_n\mathbb{Z}.$$

Unicité.

(23) Soient $a, b \in \mathbb{Z}^*$. Une démarche naturelle est de regarder la multiplication par a :

$$\begin{aligned} \varphi: \mathbb{Z}/(b/\text{pgcd}(a,b))\mathbb{Z} &\longrightarrow a(\mathbb{Z}/b\mathbb{Z}) \\ \hat{x} &\longmapsto \overline{ax} \end{aligned}$$

où les barres et les chapeaux marquent respectivement les classes modulus b et $b/\text{pgcd}(a,b)$. Vérifions que φ est bien défini. Soient $x, y \in \mathbb{Z}$. On a

$$\hat{x} = \hat{y} \Rightarrow (b/\text{pgcd}(a,b)) \mid y - x \Rightarrow \underbrace{\left(\frac{a}{\text{pgcd}(a,b)}\right)}_{\in \mathbb{Z}} b \mid ay - ax \Rightarrow \overline{ay} = \overline{ax}.$$

Soit $x \in \mathbb{Z}$ tel que $\overline{ax} = 0$. On a donc $b \mid ax$, d'où $\frac{b}{\text{pgcd}(a,b)} \mid \frac{a}{\text{pgcd}(a,b)}x$. Or, $\frac{b}{\text{pgcd}(a,b)}$ et $\frac{a}{\text{pgcd}(a,b)}$ sont premiers entre eux, donc $\frac{b}{\text{pgcd}(a,b)} \mid x$, i.e. $\hat{x} = 0$, et φ est injectif. La surjectivité est claire, donc φ est un isomorphisme.

(24) (a) En multipliant par d_1 , on obtient

$$\prod_{i=1}^m d_1\mathbb{Z}/c_i\mathbb{Z} \cong \prod_{j=1}^n d_1\mathbb{Z}/d_j\mathbb{Z}$$

et avec la question précédente, on en déduit que

$$\prod_{i=1}^m \mathbb{Z}/(c_i/\text{pgcd}(d_1, c_i))\mathbb{Z} \cong \prod_{j=1}^n \mathbb{Z}/(d_j/\text{pgcd}(d_1, d_j))\mathbb{Z} = \prod_{j=1}^n \mathbb{Z}/(d_j/d_1)\mathbb{Z}$$

puisque $d_1 \mid d_j$.

(b) En regardant le cardinal de G , on sait que

$$\prod_{i=1}^m c_i = \prod_{j=1}^n d_j.$$

De même, en regardant les cardinaux dans la relation précédente, on en déduit que

$$\prod_{i=1}^m c_i/\text{pgcd}(d_1, c_i) = \prod_{j=1}^n d_j/d_1$$

D'où, par simplification

$$d_1^n = \prod_{i=1}^m \text{pgcd}(c_i, d_1) \leq \prod_{i=1}^m d_1 = d_1^m$$

et donc que $n \leq m$. On a donc $n = m$ par symétrie.

(c) Comme on a égalité, alors pour tout $i \in \{1, \dots, m\}$, on a $\text{pgcd}(c_i, d_1) = d_1$, d'où $d_1 \mid c_1$. Par symétrie, $c_1 = d_1$.

(d) On recommence en multipliant par d_2 et en tenant compte de l'égalité $c_1 = d_1$, pour aboutir à $c_2 = d_2$, et ainsi de suite. L'égalité $n = m$ assure qu'on épuise les c_i en même temps que les d_j , ce qui conclut la preuve.