

LE THÉORÈME DE CHERMAK-DELGADO

Les démonstrations ont tendance à se compliquer à mesure qu'une théorie se développe, mais certaines preuves simples échappent à la règle et ne sont étonnamment découvertes que très tard. Le *théorème de Chermak-Delgado*, publié en 1989, est l'une de ces pépites.

■ **Théorème (Théorème de Chermak-Delgado)** Soit G un groupe fini. Il existe un sous-groupe abélien distingué I de G pour lequel $|G : I| \leq |G : A|^2$ pour tout sous-groupe abélien A de G .

En résumé, si un groupe fini possède un gros sous-groupe abélien, il possède aussi un assez gros sous-groupe abélien **DISTINGUÉ**. Les sous-groupes abéliens d'un groupe fini simple non abélien s'avèrent en particulier plutôt de petite taille.

■ **Théorème (Théorème de Chermak-Delgado pour les groupes simples non abéliens)** Soit G un groupe fini simple non abélien. Pour tout sous-groupe abélien A de G : $|G| \leq |G : A|^2$, ou encore $|A| \leq \sqrt{|G|}$.

Ce corollaire est à rapprocher d'un résultat presque trivial mais très utile qu'on pourrait appeler le *principe factoriel*. Dans les deux cas, l'ordre d'un groupe fini simple non abélien est majoré par une fonction de l'indice de certains sous-groupes.

■ **Théorème (Principe factoriel)** Soit G un groupe fini simple non abélien. Pour tout sous-groupe propre H de G , l'entier $|G|$ divise $\frac{|G : H|!}{2}$.

Démonstration En résumé, l'action par translation à droite de G sur l'ensemble G/H de ses classes à droite modulo H plonge G dans le groupe alterné de G/H , lequel est d'ordre $\frac{|G : H|!}{2}$. ■

Si elle ne présente pas l'avantage d'un énoncé en termes de divisibilité, la majoration du théorème de Chermak-Delgado est à l'évidence plus fine que celle du principe factoriel.

Ce texte est découpé en trois parties.

- Le théorème de Chermak-Delgado est démontré dans la première, mais on y établit au passage un corollaire important par la suite.
- La deuxième partie, consacrée à un *théorème de Lucchini*, prolonge le théorème de Chermak-Delgado dans le cas d'un sous-groupe cyclique.
- Dans la troisième partie, on déduit du théorème de Lucchini un *théorème d'Horosevskii* selon lequel tout automorphisme d'un groupe fini non trivial G est d'ordre inférieur ou égal à $|G| - 1$.

Certains exemples seront présentés sous forme d'exercices, dont une correction succincte est donnée en fin de texte.

Nous terminerons cette introduction par le rappel de quelques notations.

1	Double notation pour l'élément neutre d'un groupe et le sous-groupe trivial $\{1\}$
$H \leq G$	« H est un sous-groupe du groupe G »
$ X $	Cardinal de l'ensemble X
$ x $	Ordre de l'élément x
$ G : H $	Indice du sous-groupe H dans le groupe G
$C_H(X)$	Centralisateur de la partie X d'un groupe donné dans le sous-groupe H
$Z(G)$	Centre du groupe G
$\langle X \rangle$	Sous-groupe engendré par la partie X dans un groupe donné
x^g	Conjugué $g^{-1}xg$ de l'élément x par l'élément g

H^g	Conjugué $g^{-1}Hg$ du sous-groupe H par l'élément g
$\text{Aut}(G)$	Groupe des automorphismes du groupe G
\mathbb{Z}_n	Quotient du groupe \mathbb{Z} par son sous-groupe $n\mathbb{Z}$ pour un entier naturel non nul n

1 DÉMONSTRATION DU THÉORÈME DE CHERMAK-DELGADO

Soit G un groupe fini fixé une fois pour toutes dans cette partie. La preuve du théorème de Chermak-Delgado est une série de lemmes élémentaires sur les sous-groupes de G .

■ **Théorème 1 (À propos du cardinal du produit de deux sous-groupes)** Soient $H, K \leq G$.

- (i) L'ensemble $HK = \{hk \mid h \in H \text{ et } k \in K\}$ a pour cardinal $|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$.
- (ii) $|H| \cdot |K| \leq |H \cap K| \cdot |\langle H \cup K \rangle|$.
- (iii) $|C_G(H)| \cdot |C_G(K)| \leq |C_G(H \cap K)| \cdot |C_G(\langle H \cup K \rangle)|$, avec $C_G(H \cap K) = C_G(H)C_G(K)$ en cas d'égalité.

Démonstration

- (i) Le résultat est classique. Si on note φ l'application $(h, k) \mapsto hk$ de $H \cdot K$ dans HK , alors $|\varphi^{-1}(x)| = |H \cap K|$ pour tout $x \in HK$, donc $|H| \cdot |K| = |HK| \cdot |H \cap K|$ d'après le lemme des bergers.
- (ii) Simple conséquence de (i) car $HK \subset \langle H \cup K \rangle$.
- (iii) Pour commencer : $C_G(\langle H \cup K \rangle) = C_G(H \cup K) = C_G(H) \cap C_G(K)$. Ensuite, $C_G(H) \leq C_G(H \cap K)$ et $C_G(K) \leq C_G(H \cap K)$, donc $C_G(H)C_G(K) \leq C_G(H \cap K)$. Comme voulu, d'après (i) :

$$|C_G(H \cap K)| \geq |C_G(H)C_G(K)| = \frac{|C_G(H)| \cdot |C_G(K)|}{|C_G(H) \cap C_G(K)|} = \frac{|C_G(H)| \cdot |C_G(K)|}{|C_G(\langle H \cup K \rangle)|} \quad \blacksquare$$

Dans ce premier résultat, chacune des applications $H \mapsto |H|$ et $H \mapsto |C_G(H)|$ peut être vue comme une manière de mesurer les sous-groupes de G , et il s'avère qu'une paire de sous-groupes $\{H, K\}$ est en ce sens toujours moins grosse que la paire $\{H \cap K, \langle H \cup K \rangle\}$. Par produit, l'application $H \mapsto |H| \cdot |C_G(H)|$ jouit naturellement de la même propriété.

D'un autre côté, les applications $H \mapsto |H|$ et $H \mapsto |C_G(H)|$ sont respectivement croissante et décroissante. Leur produit $H \mapsto |H| \cdot |C_G(H)|$ mesure dès lors une forme d'équilibre entre la taille d'un sous-groupe et la manière dont ses éléments commutent à ceux de G . Ce que Chermak et Delgado ont découvert, c'est que les sous-groupes de G qui maximisent cette mesure d'équilibre ont des propriétés tout à fait particulières.

■ **Définition-théorème 2 (Mesure de Chermak-Delgado et μ -maximalité)**

- (i) Pour tout $H \leq G$, on appelle *mesure de Chermak-Delgado* de H l'entier $\mu(H) = |H| \cdot |C_G(H)|$.
Pour tous $H, K \leq G$: $\mu(H) \mu(K) \leq \mu(H \cap K) \mu(\langle H \cup K \rangle)$, avec $C_G(H \cap K) = C_G(H)C_G(K)$ en cas d'égalité.
- (ii) Pour tout $H \leq G$, on dit que H est μ -maximal si $\mu(K) \leq \mu(H)$ pour tout $K \leq G$.
En particulier, pour tous $H, K \leq G$ μ -maximaux, $H \cap K$ est lui aussi μ -maximal et $C_G(H \cap K) = C_G(H)C_G(K)$.

Par exemple, $\mu(1) = |G|$ et $\mu(G) = \mu(Z(G)) = |G| \cdot |Z(G)|$.

Rappelons à présent qu'un sous-groupe de G est *caractéristique* dans G s'il est stable par tout automorphisme de G . Un tel sous-groupe est en particulier distingué dans G .

■ **Définition-théorème 3 (Sous-groupe de Chermak-Delgado)**

- (i) L'intersection I des sous-groupes μ -maximaux de G est elle aussi un sous-groupe μ -maximal de G . Nous l'appellerons le *sous-groupe de Chermak-Delgado* de G .
- (ii) Pour tout $H \leq G$: $|G : I| \leq |G : H| \cdot |G : C_G(H)|$, avec égalité si et seulement si H est μ -maximal.
En particulier, pour tout $A \leq G$ abélien : $|G : I| \leq |G : A|^2$.
- (iii) Le sous-groupe I est caractéristique de G .

Démonstration

- (i) Simple conséquence de 2 (ii).
- (ii) Par μ -maximalité de I : $|H| \cdot |C_G(H)| = \mu(H) \leq \mu(I) = |I| \cdot |C_G(I)| \leq |I| \cdot |G|$. Le résultat en découle.
 Dans le cas particulier où A est abélien, $A \leq C_G(A)$ donc $|G : C_G(A)| \leq |G : A|$.
- (iii) Pour tous $\varphi \in \text{Aut}(G)$ et $H \leq G$, $C_G(\varphi(H)) = \varphi(C_G(H))$ donc $\mu(\varphi(H)) = \mu(H)$. En particulier, l'ensemble des sous-groupes μ -maximaux de G est stable par tout automorphisme de G , et cette propriété se transmet naturellement à leur intersection I . ■

Le théorème de Chermak-Delgado est presque démontré à ce stade, mais les inégalités (ii) du précédent théorème ne sont d'aucun intérêt en l'état car elles n'excluent pas la possibilité que I soit G tout entier. Le résultat qui suit montre justement en quoi les idées de Chermak et Delgado contraignent la structure de I .

■ **Théorème 4 (Centralisateur d'un sous-groupe μ -maximal)**

- (i) Pour tout $H \leq G$: $\mu(H) \leq \mu(C_G(H))$, avec $C_G(C_G(H)) = H$ en cas d'égalité.
 En particulier, pour tout $H \leq G$ μ -maximal, $C_G(H)$ est lui aussi μ -maximal et $C_G(C_G(H)) = H$.
- (ii) Le sous-groupe I est abélien et contient $Z(G)$.

Démonstration

- (i) Évidemment $H \leq C_G(C_G(H))$, donc $\mu(H) = |H| \cdot |C_G(H)| \leq |C_G(C_G(H))| \cdot |C_G(H)| = \mu(C_G(H))$ avec $C_G(C_G(H)) = H$ en cas d'égalité.
- (ii) D'après (i) et la μ -maximalité de I , $C_G(I)$ est μ -maximal, donc contient I par définition de celui-ci, de sorte que I est abélien. Mais l'assertion (i) prouve aussi que $C_G(C_G(I)) = I$, et donc $Z(G) \leq I$. ■

Nous avons finalement établi un théorème de Chermak-Delgado un peu plus fort que celui du début de ce texte.

■ **Théorème 5 (Théorème de Chermak-Delgado)** Soit G un groupe fini. Il existe un sous-groupe abélien caractéristique I de G pour lequel pour tout $H \leq G$: $|G : I| \leq |G : H| \cdot |G : C_G(H)|$.
 En particulier, pour tout $A \leq G$ abélien : $|G : I| \leq |G : A|^2$, et $|A| \leq \sqrt{|G|}$ si $I = 1$.

On peut se demander bien sûr à quoi ressemble le sous-groupe de Chermak-Delgado des groupes les plus classiques et quelle majoration de l'ordre de leurs sous-groupes abéliens en découle.

Si G est abélien, alors pour tout $H \leq G$ distinct de G : $\mu(H) = |H| \cdot |G| < |G|^2 = \mu(G)$, donc G est à lui-même son propre sous-groupe de Chermak-Delgado. Le théorème éponyme est ici sans intérêt.

Le cas des groupes diédraux, du groupe des quaternions, des groupes symétriques et des groupes linéaires est étudié ci-dessous sous forme d'exercices. Ce qu'il faut en retenir, c'est que la majoration de Chermak et Delgado n'est pas vraiment effective, le résultat a avant tout une portée théorique et c'est son universalité qui le rend précieux.

Exemple Soit $n \geq 3$. Le groupe diédral D_n peut être défini abstraitement comme le produit semi-direct $\mathbb{Z}_2 \ltimes \mathbb{Z}_n$ issu de l'action par inversion de \mathbb{Z}_2 sur \mathbb{Z}_n . Plus explicitement, cela veut dire que $D_n = \langle \tau \rangle \langle \sigma \rangle$ où τ est une involution, σ un élément d'ordre n , et $\sigma^\tau = \sigma^{-1}$.

- 1) Déterminer le sous-groupe de Chermak-Delgado de D_4 .
- 2) Montrer que si $n \neq 4$, D_n admet $\langle \sigma \rangle$ pour sous-groupe de Chermak-Delgado.

Exemple Montrer que le sous-groupe de Chermak-Delgado du groupe des quaternions est exactement son centre.

Exemple Pour tout $n \geq 5$, le groupe symétrique S_n ne possède pas de sous-groupe abélien distingué non trivial, donc son sous-groupe de Chermak-Delgado est trivial.

- 1) Montrer que S_4 a lui aussi un sous-groupe de Chermak-Delgado trivial.

Finalement, pour tout $n \geq 4$ et pour tout $A \leq S_n$ abélien, le théorème de Chermak-Delgado nous garantit que $|A| \leq \sqrt{n!}$. Cette majoration est hélas des plus grossières, comme on le découvre dans les questions qui suivent.

- 2) Soient $n \in \mathbb{N}^*$ et G un sous-groupe abélien transitif de S_n , i.e. un sous-groupe abélien de S_n dont l'action naturelle sur l'ensemble $\llbracket 1, n \rrbracket$ est transitive. Montrer que $|G| = n$.
- 3) Pour tout $n \in \mathbb{N}^*$, on note \mathcal{P}_n l'ensemble des *partitions* de n , i.e. l'ensemble des familles (n_1, \dots, n_r) d'entiers naturels non nuls, où r n'est pas fixé, pour lesquelles $n_1 + \dots + n_r = n$. On pose alors $p_n = \max \{n_1 \dots n_r \mid (n_1, \dots, n_r) \in \mathcal{P}_n\}$. Montrer que pour tout $n \in \mathbb{N}^*$: $p_{3n} = 3^n$, $p_{3n+1} = 4 \cdot 3^{n-1}$ et $p_{3n+2} = 2 \cdot 3^n$.
- 4) Montrer que pour tout $n \in \mathbb{N}^*$, tout sous-groupe abélien de S_n est d'ordre inférieur ou égal à p_n et étudier le cas d'égalité. On est bien loin de la majoration $\sqrt{n!}$ de Chermak et Delgado.

Le cas des groupes linéaires demande davantage de travail et ne sera qu'esquissé.

Exemple Soient $n \geq 2$ et q une puissance d'un nombre premier pour lesquels $(n, q) \neq (2, 2)$ et $(n, q) \neq (2, 3)$.

- 1) Montrer que $|\mathrm{GL}_n(\mathbb{F}_q)| = q^{\frac{n(n-1)}{2}} \prod_{k=1}^n (q^k - 1)$ et $|\mathrm{Z}(\mathrm{GL}_n(\mathbb{F}_q))| = q - 1$.

Par hypothèse sur le couple (n, q) , il est connu que les sous-groupes abéliens distingués de $\mathrm{GL}_n(\mathbb{F}_q)$ sont les seuls sous-groupes de son centre. Le groupe linéaire $\mathrm{GL}_n(\mathbb{F}_q)$ admet dès lors son centre pour sous-groupe de Chermak-Delgado, de sorte que pour tout $A \leq \mathrm{GL}_n(\mathbb{F}_q)$ abélien : $|\mathrm{GL}_n(\mathbb{F}_q) : \mathrm{Z}(\mathrm{GL}_n(\mathbb{F}_q))| \leq |\mathrm{GL}_n(\mathbb{F}_q) : A|^2$, ou encore $|A| \leq \sqrt{|\mathrm{GL}_n(\mathbb{F}_q)| \cdot |\mathrm{Z}(\mathrm{GL}_n(\mathbb{F}_q))|}$. Si q est grand et n fixé, cette majoration de Chermak-Delgado en $q^{\frac{n^2+1}{2}}$ s'avère de nouveau grossière, car en réalité pour tout $A \leq \mathrm{GL}_n(\mathbb{F}_q)$ abélien : $|A| \leq \max \{q^n - 1, q^{\lfloor \frac{n^2}{4} \rfloor} (q - 1)\}$. À défaut de le prouver, nous pouvons au moins montrer qu'elle est optimale en exhibant dans $\mathrm{GL}_n(\mathbb{F}_q)$ des sous-groupes d'ordres $q^n - 1$ et $q^{\lfloor \frac{n^2}{4} \rfloor} (q - 1)$.

Pour la valeur $q^n - 1$, rappelons que le groupe multiplicatif de \mathbb{F}_{q^n} est cyclique, disons engendré par ζ . L'application $x \mapsto \zeta x$ est alors un automorphisme \mathbb{F}_q -linéaire d'ordre $q^n - 1$ de \mathbb{F}_{q^n} , et comme \mathbb{F}_{q^n} est un \mathbb{F}_q -espace vectoriel de dimension n , cet automorphisme nous fournit un automorphisme \mathbb{F}_q -linéaire d'ordre $q^n - 1$ de \mathbb{F}_q^n via le choix d'une base.

- 2) a) Montrer que pour tout $r \in \llbracket 1, n-1 \rrbracket$, les matrices $\begin{pmatrix} I_r & M \\ 0 & I_{n-r} \end{pmatrix}$, M décrivant $\mathcal{M}_{r, n-r}(\mathbb{F}_q)$, forment un sous-groupe abélien de $\mathrm{GL}_n(\mathbb{F}_q)$.
 b) En déduire que $\mathrm{GL}_n(\mathbb{F}_q)$ possède un sous-groupe d'ordre $q^{\lfloor \frac{n^2}{4} \rfloor} (q - 1)$.
- 3) Montrer que si $n \in \{2, 3\}$, alors $q^n - 1 > q^{\lfloor \frac{n^2}{4} \rfloor} (q - 1)$, et que si $n \geq 4$, alors $q^{\lfloor \frac{n^2}{4} \rfloor} (q - 1) > q^n - 1$.

Le corollaire suivant du théorème de Chermak-Delgado nous sera utile dans la prochaine partie.

Théorème 6 (Un raffinement strict du théorème de Chermak-Delgado) Soit G un groupe fini non trivial sans sous-groupe abélien distingué non trivial. Pour tout $A \leq G$ abélien : $|G| < |G : A|^2$, ou encore $|A| < \sqrt{|G|}$.

Démonstration Nous allons montrer en fait un peu plus, à savoir que $|G| < |G : A| \cdot |G : C_G(A)|$ pour tout $A \leq G$ abélien non trivial. Le résultat découlera aussitôt de l'inclusion $A \leq C_G(A)$. Le cas du sous-groupe trivial se traite aisément à part.

L'hypothèse principale du théorème rend trivial le sous-groupe de Chermak-Delgado de G , donc d'après le théorème éponyme, $|G| \leq |G : A| \cdot |G : C_G(A)|$ pour tout $A \leq G$ abélien, avec égalité si et seulement si A est μ -maximal. Il nous suffit dès lors de montrer qu'aucun sous-groupe abélien non trivial de G ne peut être μ -maximal.

Supposons justement par l'absurde que cela soit possible et intéressons-nous à un sous-groupe abélien μ -maximal non trivial A de G qui soit minimal pour ces propriétés. L'hypothèse principale du théorème interdit à A d'être distingué dans G . Nous pouvons donc nous donner un élément x de G pour lequel $A^x \neq A$. Le sous-groupe A^x est alors lui aussi μ -maximal, car $\mu(A^x) = |A^x| \cdot |C_G(A^x)| = |A| \cdot |C_G(A)^x| = |A| \cdot |C_G(A)| = \mu(A)$. Par intersection, $A \cap A^x$ est à son tour μ -maximal, mais donc $A \cap A^x = 1$ par minimalité de A . Finalement, d'après le cas d'égalité du théorème 2 (ii) : $G = C_G(1) = C_G(A \cap A^x) = C_G(A) C_G(A^x) = C_G(A) C_G(A)^x$. En particulier, $x = c x^{-1} c' x$ pour certains $c, c' \in C_G(A)$, donc $x = c' c \in C_G(A)$, et enfin $A^x = A$ — contradiction. Comme voulu, aucun sous-groupe abélien non trivial de G n'est donc μ -maximal. ■

Nous ne démontrerons par le corollaire qui suit car sa preuve n'est qu'une adaptation de la précédente.

Théorème 7 (Théorème de Chermak-Delgado pour les groupes simples non abéliens) Soit G un groupe fini simple non abélien. Pour tout $H \leq G$: $|H| \cdot |C_G(H)| \leq |G|$, avec égalité si et seulement si $H = 1$ ou $H = G$.

En particulier, pour tout $A \leq G$ abélien : $|G| < |G : A|^2$, ou encore $|A| < \sqrt{|G|}$.

Cette majoration n'est pas optimale, mais elle est tout de même assez fine pour une preuve très courte. On peut montrer en exploitant la classification des groupes finis simples que la racine carrée de Chermak et Delgado peut être remplacée par une racine cubique, sauf dans le cas des groupes $\mathrm{PSL}_2(\mathbb{F}_q)$ où l'ordre de grandeur en racine cubique est le bon, mais où la majoration est fautive à proprement parler.

2 LE THÉORÈME DE LUCCHINI

Le théorème de Chermak-Delgado, ou plutôt l'idée de mesure qui le sous-tend, ont inspiré un certain nombre de travaux depuis 1989, dont un joli théorème de 1998 que nous présentons à présent, le *théorème de Lucchini*. En quelques mots, le théorème de Lucchini renforce le théorème de Chermak-Delgado dans le cas d'un sous-groupe cyclique, mais une définition préalable s'impose.

■ **Définition (Cœur d'un sous-groupe)** Soient G un groupe et $H \leq G$. On appelle *cœur de H dans G* et on note H_G l'intersection des conjugués de H dans G :
$$H_G = \bigcap_{x \in G} H^x.$$

Il est équivalent de dire que H_G est le plus petit sous-groupe distingué de G inclus dans H , mais on peut aussi voir H_G comme le noyau de l'action par translation à droite de G sur l'ensemble G/H de ses classes à droite modulo H . Cette action plonge le quotient $\frac{G}{H_G}$ dans le groupe symétrique de G/H comme on l'a déjà vu en introduction avec le principe factoriel.

■ **Théorème 8 (Théorème de Lucchini)**
Soient G un groupe fini et A un sous-groupe cyclique propre de G . Alors $|G : A_G| < |G : A|^2$.

En particulier, pour tout $x \in G$, $|x| < \sqrt{|G|}$ si $\langle x \rangle$ ne contient aucun sous-groupe distingué non trivial de G .

Dans le cas où G est simple non abélien, le corollaire 2 du théorème de Chermak-Delgado affirmait exactement la même chose que le théorème de Lucchini, mais l'intérêt du théorème de Lucchini réside justement dans sa portée générale.

Enfin, le théorème requiert que A soit distinct de G uniquement parce que l'inégalité est une égalité si $A = G$.

■ **Théorème 9 (Préliminaires)**

- (i) Soient G un groupe fini et N un sous-groupe abélien distingué non trivial de G , minimal pour ces propriétés. Alors N est isomorphe au groupe \mathbb{F}_p^n pour un certain nombre premier p et un certain $n \in \mathbb{N}^*$.
- (ii) Soient p un nombre premier et $n \in \mathbb{N}^*$. Tout automorphisme du groupe additif \mathbb{F}_p^n est en fait un automorphisme linéaire du \mathbb{F}_p -espace vectoriel \mathbb{F}_p^n . En d'autres termes : $\mathrm{Aut}(\mathbb{F}_p^n) = \mathrm{GL}_n(\mathbb{F}_p)$.
- (iii) Tout élément de $\mathrm{GL}_n(\mathbb{F}_p)$ est d'ordre inférieur ou égal à $p^n - 1$.

Nous avons vu dans la partie 1, dans notre exemple sur les groupes linéaires, que la majoration $p^n - 1$ de l'assertion (iii) est optimale, il y a vraiment des éléments d'ordre $p^n - 1$ dans $\mathrm{GL}_n(\mathbb{F}_p)$.

Démonstration

(i) Soit p un diviseur premier de $|N|$. Comme N est abélien, l'ensemble $N_p = \{x \in N \mid x^p = 1\}$ est un sous-groupe de N . Ensuite, pour tous $x \in N$ et $g \in G$, $x^g \in N$ car N est distingué dans G , et $(x^g)^p = (x^p)^g = 1$ donc $x^g \in N_p$. Conclusion : N_p est un sous-groupe abélien distingué non trivial de G . Par minimalité de N , $N = N_p$.

Il n'est enfin pas difficile de vérifier que N est un \mathbb{F}_p -espace vectoriel pour la loi externe $(\lambda, x) \mapsto x^\lambda$, forcément de dimension finie pour une raison de cardinal.

- (ii) Soient $\varphi \in \text{Aut}(\mathbb{F}_p^n)$, $\lambda \in \mathbb{F}_p$ et $(x_1, \dots, x_n) \in \mathbb{F}_p^n$. Le scalaire λ est l'image dans \mathbb{F}_p d'un certain entier k . Les égalités qui suivent montrent que φ n'est pas seulement un morphisme de groupes, c'est en fait déjà une application \mathbb{F}_p -linéaire.

$$\begin{aligned} \varphi(\lambda \cdot (x_1, \dots, x_n)) &= \varphi(\underbrace{x_1 + \dots + x_1}_{k \text{ termes}}, \dots, \underbrace{x_n + \dots + x_n}_{k \text{ termes}}) = \varphi(\underbrace{(x_1, \dots, x_n) + \dots + (x_1, \dots, x_n)}_{k \text{ termes}}) \\ &= \underbrace{\varphi(x_1, \dots, x_n) + \dots + \varphi(x_1, \dots, x_n)}_{k \text{ termes}} = \lambda \cdot \varphi(x_1, \dots, x_n). \end{aligned}$$

- (iii) Toute matrice M de $\text{GL}_n(\mathbb{F}_p)$ possède un polynôme annulateur de degré n d'après le théorème de Cayley-Hamilton, donc engendre une sous- \mathbb{F}_p -algèbre $\mathbb{F}_p[M]$ de $\mathcal{M}_n(\mathbb{F}_p)$ de dimension au plus n . En particulier, $|\mathbb{F}_p[M]| \leq p^n$ donc $|M| \leq |\mathbb{F}_p[M] \setminus \{0\}| \leq p^n - 1$. ■

Nous sommes maintenant prêts pour la démonstration du théorème de Lucchini, qui n'est pas vraiment simple.

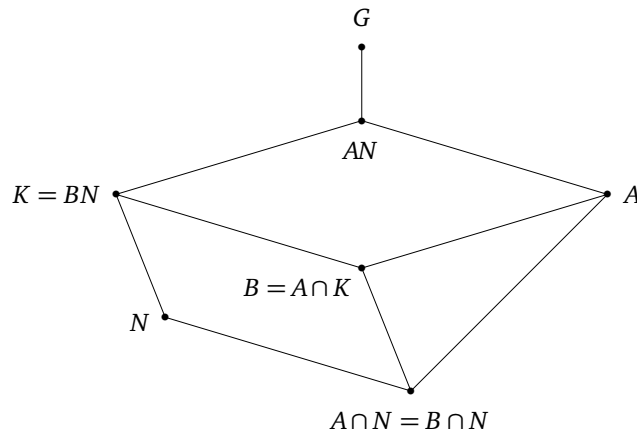
Démonstration Soient G un groupe fini et A un sous-groupe cyclique propre de G . Raisonnant par récurrence, nous pouvons supposer le théorème de Lucchini vrai dans tout groupe d'ordre strictement inférieur à $|G|$.

- Tout d'abord, $\frac{A}{A_G}$ est un sous-groupe cyclique propre de $\frac{G}{A_G}$ et il est clair que $\left(\frac{A}{A_G}\right)_G = 1$, donc par hypothèse de récurrence, si $A_G \neq 1$: $|G : A_G| = \left| \frac{G}{A_G} : \left(\frac{A}{A_G}\right)_G \right| < \left| \frac{G}{A_G} : \frac{A}{A_G} \right|^2 = |G : A|^2$. Nous pouvons ainsi supposer que $A_G = 1$ et viser l'inégalité $|G| < |G : A|^2$.
- Or si G ne possède aucun sous-groupe abélien distingué non trivial, le théorème 6 montre justement que $|G| < |G : A|^2$. Nous pouvons ainsi supposer que G possède des sous-groupes abéliens distingués non triviaux et nous en donner un qui soit minimal, disons N . D'après 9 (i), N est isomorphe à \mathbb{F}_p^n pour un certain nombre premier p et un certain $n \in \mathbb{N}^*$.

- Notons K l'unique sous-groupe de G contenant N , nécessairement distingué, pour lequel $\frac{K}{N} = \left(\frac{AN}{N}\right)_G$. Clairement $\frac{K}{N} \leq \frac{AN}{N}$, donc $N \leq K \leq AN$, donc $K = BN$ si on pose $B = A \cap K$. Observons en outre que $A \cap N = A \cap (K \cap N) = (A \cap K) \cap N = B \cap N$. Par hypothèse de récurrence :

$$\begin{aligned} |G| = |G : K| \cdot |K| &= \left| \frac{G}{N} : \frac{K}{N} \right| \cdot |K| \leq \left| \frac{G}{N} : \frac{AN}{N} \right|^2 \cdot |K| = \frac{|G|^2 \cdot |BN|}{|AN|^2} = |G|^2 \times \frac{|A \cap N|^2}{|A|^2 \cdot |N|^2} \times \frac{|B| \cdot |N|}{|B \cap N|} \\ &= |G : A|^2 \times \frac{|B| \cdot |B \cap N|}{|N|} \quad \star, \end{aligned}$$

avec égalité si et seulement si $\frac{G}{N} = \frac{AN}{N}$, i.e. $G = AN$, et même $G = AN = K$. Il nous reste ainsi à montrer que $|B| \cdot |B \cap N| \leq |N|$ si l'inégalité \star est stricte, ou bien $|B| \cdot |B \cap N| < |N|$ si elle est large.



- Or n'oublions pas que N est un sous-groupe abélien distingué non trivial de G minimal à ce titre. Comme K est distingué dans G , cela nous met face à l'alternative suivante — soit $N \cap Z(K) = 1$, soit $N \leq Z(K)$.
- **Cas où $N \leq Z(K)$:**

$$\begin{aligned} \text{Pour tout } g \in G : \quad B^g N &= B^g N^g \quad \text{car } N \text{ est distingué dans } G \\ &= (BN)^g = K^g = K \quad \text{car } K \text{ est distingué dans } G \\ &= BN. \end{aligned}$$

$$\begin{aligned} \text{Ensuite, à la puissance } p : \quad (B^p)^g &= (B^g)^p = (B^g)^p N^p \quad \text{car tout élément de } N \text{ est d'ordre 1 ou } p \\ &= (B^g N)^p \quad \text{car } N \leq Z(K) \text{ et } B^g \leq K \\ &= (BN)^p = B^p \quad \text{pour les mêmes raisons.} \end{aligned}$$

Cette égalité valable pour tout $g \in G$ montre que le sous-groupe B^p de A est distingué dans G , mais donc $B^p = 1$ car $A_G = 1$. Comme B est cyclique, cela veut dire que B est soit trivial, soit d'ordre p .

Remarquons par ailleurs que $B \neq N$, car N est distingué dans G et non trivial alors que $B \leq A$ et $A_G = 1$.

Comme N est un p -groupe, cela signifie que $|B \cap N| \leq \frac{|N|}{p}$, et donc que $|B| \cdot |B \cap N| \leq |N|$. Comme nous l'avons vu, c'est exactement le résultat visé, sauf si l'inégalité \star est une égalité.

Dans ce cas particulier, $G = AN = K$ et ces égalités font de G un groupe abélien car d'une part A est abélien et d'autre part $N \leq Z(K) = Z(G)$. Or tout sous-groupe de G est dès lors distingué dans G . En particulier, $A = A_G = 1$, auquel cas le théorème de Lucchini est trivial.

• **Cas où $N \cap Z(K) = 1$:**

En tant que sous-groupe de A , B est abélien. Il en découle que tout sous-groupe de B qui commute à N commute plus généralement à $BN = K$, et donc est inclus dans $Z(K)$. En particulier, $C_B(N) \leq Z(K)$ mais également $B \cap N \leq N \cap Z(K) = 1$.

L'inclusion $C_B(N) \leq Z(K)$ est en fait une égalité. Soit en effet $z = bn \in Z(K)$ avec $b \in B$ et $n \in N$. Pour tout $b' \in B$, B étant abélien : $b'n = b'b^{-1}z = b^{-1}b'z = b^{-1}zb' = nb'$, donc n commute à B . Or n commute aussi à N car N est abélien, donc n commute à $K = BN$, ou encore $n \in N \cap Z(K) = 1$. Conclusion : $z = b \in B$, donc $z \in C_B(N)$.

L'égalité $C_B(N) = Z(K)$ montre en particulier que $C_B(N)$ est distingué dans G puisque K l'est, mais par ailleurs $C_B(N) \leq A$ et $A_G = 1$, donc $C_B(N) = 1$. L'action par conjugaison de B sur N , dont $C_B(N)$ est le noyau, identifie dès lors B à un sous-groupe cyclique de $\text{Aut}(N)$, lequel est isomorphe à $\text{GL}_n(\mathbb{F}_p)$ d'après 9 (ii). Aussitôt, $|B| < p^n = |N|$ d'après l'assertion (iii) du même théorème, donc $|B| \cdot |B \cap N| < |N|$ comme voulu car $B \cap N = 1$. ■

3 LE THÉORÈME D'HOROSEVSKII

Le théorème d'Horosevskii date de 1974. Nous allons le déduire du théorème de Lucchini, mais Horosevskii ne disposait pas des idées de Chermak et Delgado à l'époque.

■ **Théorème 10 (Théorème d'Horosevskii)** Soit G un groupe fini non trivial. Pour tout $\varphi \in \text{Aut}(G)$: $|\varphi| \leq |G| - 1$.

Nous avons vu dans la partie 2 que pour tout nombre premier p et pour tout $n \in \mathbb{N}^*$, tout élément de $\text{Aut}(\mathbb{F}_p^n) = \text{GL}_n(\mathbb{F}_p)$ est d'ordre inférieur ou égal à $p^n - 1$. Le théorème d'Horosevskii n'est finalement que la généralisation de ce résultat à tout groupe fini.

Démonstration La notion de produit semi-direct est supposée connue, mais quelques rappels sont peut-être nécessaires.

Soit $\varphi \in \text{Aut}(G)$. Notons A le sous-groupe cyclique $\langle \varphi \rangle$ de $\text{Aut}(G)$ et Γ le produit semi-direct $\Gamma = A \ltimes G$ de G par A défini par l'action naturelle de A sur G . Les groupes A et G peuvent être vus comme des sous-groupes de Γ et tout élément de Γ s'écrit d'une et une seule manière sous la forme ag avec $a \in A$ et $g \in G$. Pour définir la loi de Γ , il est suffisant de savoir conjuguer tout élément g de G par un élément a de A : $g^a = a(g)$. Cette relation énonce en particulier que G est normalisé par A , donc distingué dans Γ . Pour tous $a, a' \in A$ et $g, g' \in G$, enfin : $(ag)(a'g') = (aa')(a'^{-1}ga'g') = (aa')(g^a g')$.

À présent, pour tous $a \in A_\Gamma$ et $g \in G$, $(g^a)^{-1}g \in G$ car G est distingué dans Γ , et de même, A_Γ étant distingué dans Γ : $(g^a)^{-1}g = a^{-1}a^g \in A_G \leq A$. Conclusion : $(g^a)^{-1}g \in G \cap A = 1$, autrement dit $g^a = g$, ou encore $a(g) = g$. Comme c'est vrai pour tout $g \in G$, on vient de montrer que $A_\Gamma = 1$.

Finalement, $\Gamma \neq A$ car G n'est pas trivial, donc d'après le théorème de Lucchini :

$$|\varphi| \cdot |G| = |A| \cdot |G| = |\Gamma| = |\Gamma : A_\Gamma| < |\Gamma : A| = |G|^2, \quad \text{ou encore } |\varphi| \leq |G| - 1. \quad \blacksquare$$

L'inégalité d'Horosevskii est une égalité dans le cas des groupes \mathbb{F}_p^n où p est un nombre premier et $n \in \mathbb{N}^*$, mais l'est-elle pour d'autres groupes ? La réponse est non, nous ne le montrerons pas mais cela résulte d'un autre théorème d'Horosevskii. Certains travaux récents vont en réalité beaucoup plus loin. Vdovin a montré en 2015 deux résultats particulièrement jolis que nous nous contenterons d'énoncer en guise de conclusion.

- Si un groupe fini G possède un automorphisme d'ordre strictement supérieur à $\frac{|G|}{2}$, alors G est abélien.
- Si un groupe fini G possède un automorphisme d'ordre strictement supérieur à $\frac{|G|}{10}$, alors G est résoluble. Contrairement au premier, ce résultat repose hélas sur la classification des groupes finis simples...

Pour en savoir plus :

- I. M. Isaacs, *Finite group theory*, Graduate studies in mathematics, volume 92 (2008).
On trouve dans cet excellent livre à la fois le théorème de Chermak-Delgado, le théorème de Lucchini et le théorème d'Horosevskii, mais le théorème de Lucchini est déduit d'un théorème de Zenkov et non du théorème de Chermak-Delgado.
- A. Chermak & A. Delgado, *A measuring argument for finite groups*, Proceedings of the American Mathematical Society, volume 107, numéro 4 (1989), pages 907-914.
- A. Lucchini, *On the order of transitive permutation groups with cyclic point-stabilizer*, Atti della Accademia Nazionale dei Lincei, Classe di Scienze Fisiche, Matematiche e Naturali, Rendiconti Lincei, Matematica e Applicazioni, série 9, volume 9 (1998), pages 241-243.
- M. V. Horosevskii, *On automorphisms of finite groups*, Matematicheskii Sbornik, volume 22, numéro 4 (1974), pages 584-594.

■ 4 CORRECTION DES EXERCICES

■ 4.1 GROUPES DIÉDRAUX

Nous traiterons d'un coup d'un seul le cas de tous les groupes diédraux D_n avec $n \geq 3$. Il est connu que si n est impair, alors $Z(D_n) = 1$, et si n est pair, alors $Z(D_n) = \langle \sigma^{\frac{n}{2}} \rangle$. En outre, $\langle \sigma \rangle$ est abélien distingué dans D_n et $C_{D_n}(\sigma) = \langle \sigma \rangle$, donc $\mu(\langle \sigma \rangle) = |\langle \sigma \rangle|^2 = n^2$.

Nous pouvons nous contenter de chercher le sous-groupe de Chermak-Delgado de D_n parmi les sous-groupes abéliens distingués de D_n contenant $Z(D_n)$. Soit donc H un tel sous-groupe.

- Si H est le groupe D_n lui-même ou son centre :

$$\mu(H) = |D_n| \cdot |Z(D_n)| = \begin{cases} 2n < n^2 & \text{si } n \text{ est impair} \\ 4n \leq n^2 & \text{si } n \text{ est pair, avec égalité si et seulement si } n = 4. \end{cases}$$

Dans le cas contraire, H est propre et non central, donc $\mu(H) = |H| \cdot |C_{D_n}(H)| \leq n^2$, avec égalité si et seulement si $|H| = |C_{D_n}(H)| = n$. Dans tous les cas, H est μ -maximal si et seulement si $\mu(H) = n^2$, et par minimalité, le sous-groupe de Chermak-Delgado de D_4 est son centre $\langle \sigma^2 \rangle$.

- Supposons $n \neq 4$. À quelle condition a-t-on $|H| = |C_{D_n}(H)| = n$? C'est vrai bien sûr si $H = \langle \sigma \rangle$. Et sinon? Que dire si H contient $\tau\sigma^k$ pour un certain $k \in \llbracket 0, n-1 \rrbracket$? Dans ce cas, H étant distingué dans D_n :

$$\sigma^2 = \sigma^{-k} \tau \sigma^{-1} \tau \sigma^{k+1} = (\tau \sigma^k)^{-1} (\tau \sigma^k)^\sigma \in H,$$

puis H étant abélien : $\tau \sigma^{k-2} = \sigma^2 (\tau \sigma^k) = (\tau \sigma^k) \sigma^2 = \tau \sigma^{k+2}$, donc $\sigma^4 = 1$, ce qui est impossible car $n \neq 4$. Conclusion : $\langle \sigma \rangle$ est le seul sous-groupe μ -maximal de D_n , donc n'est autre que son sous-groupe de Chermak-Delgado.

■ 4.2 GROUPE DES QUATERNIONS

Le groupe des quaternions Q_8 peut être écrit $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ avec les règles usuelles :

$$i^2 = j^2 = k^2 = -1, \quad ij = k, \quad jk = i, \quad ki = j \quad \text{et} \quad ji = -k, \quad kj = -i, \quad ik = -j.$$

Ses sous-groupes sont $1, Z(Q_8) = \langle -1 \rangle, \langle i \rangle, \langle j \rangle, \langle k \rangle$ et Q_8 . Quant à ses centralisateurs, ce sont $C_{Q_8}(-1) = Q_8, C_{Q_8}(i) = \langle i \rangle, C_{Q_8}(j) = \langle j \rangle$ et $C_{Q_8}(k) = \langle k \rangle$. Aussitôt :

$$\mu(1) = 1 \times 8 = 8, \quad \mu(\langle -1 \rangle) = 2 \times 8 = 16, \quad \mu(\langle i \rangle) = \mu(\langle j \rangle) = \mu(\langle k \rangle) = 4 \times 4 = 16 \quad \text{et} \quad \mu(Q_8) = 8 \times 2 = 16.$$

Le sous-groupe de Chermak-Delgado de Q_8 , qui est aussi son plus petit sous-groupe μ -maximal, est ainsi clairement son centre $\langle -1 \rangle$.

4.3 GROUPES SYMÉTRIQUES

- 1) Les sous-groupes distingués de S_4 sont $1, K = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}, A_4$ et S_4 , mais seuls 1 et K sont abéliens. Le sous-groupe de Chermak-Delgado de S_4 est ainsi l'un de ces deux sous-groupes, et il est au moins clair que $\mu(1) = 1 \times 24 = 24$. Ensuite, $C_{S_4}(K) = K$ donc $\mu(K) = 4 \times 4 = 16$. Comme voulu, le sous-groupe de Chermak-Delgado de S_4 est trivial.
- 2) Comme G est transitif sur $\llbracket 1, n \rrbracket$, l'orbite de 1 sous G est l'ensemble $\llbracket 1, n \rrbracket$ tout entier. Ainsi $n = |G : S|$ si nous notons S le stabilisateur de 1 dans G . Or que vaut ce stabilisateur ? Soit $s \in S$. Pour tout $k \in \llbracket 1, n \rrbracket$, $k = g(1)$ pour un certain $g \in G$ par transitivité de G , donc G étant abélien : $s(k) = s(g(1)) = g(s(1)) = g(1) = k$. En d'autres termes $s = \text{Id}$, et finalement $S = 1$. Comme voulu $n = |G : S| = |G|$.
- 3) Soit $n \geq 3$. Pour calculer p_n , intéressons-nous à une partition (n_1, \dots, n_r) « maximale » de n , i.e. une partition de n pour laquelle $p_n = n_1 \dots n_r$.
 - Il n'est pas possible que l'un des entiers n_1, \dots, n_r soit égal à 1 , car si on avait par exemple $n_r = 1$, l'inégalité $n_{r-1} + 1 > n_{r-1} \times 1$ ferait de $(n_1, \dots, n_{r-1} + 1)$ une partition de n de produit strictement supérieur à p_n .
 - Il n'est pas possible que l'un des entiers n_1, \dots, n_r soit supérieur ou égal à 5 , car si on avait par exemple $n_r \geq 5$, l'inégalité $2(n_r - 2) > n_r$ ferait de $(n_1, \dots, n_{r-1}, n_r - 2, 2)$ une partition de n de produit strictement supérieur à p_n .
 - Les égalités $2 + 2 = 4$ et $2 \times 2 = 4$ permettent de remplacer dans (n_1, \dots, n_r) toute apparition de l'entier 4 par une apparition deux fois de l'entier 2 sans que cela affecte le produit $n_1 \dots n_r$.
 - Il n'est pas possible que l'entier 2 apparaisse plus de deux fois dans (n_1, \dots, n_r) , car si on avait par exemple $n_{r-2} = n_{r-1} = n_r = 2$, l'inégalité $3 \times 3 > 2 \times 2 \times 2$ ferait de $(n_1, \dots, n_{r-3}, 3, 3)$ une partition de n de produit strictement supérieur à p_n .

Notre partition (n_1, \dots, n_r) a finalement l'une des formes $(3, \dots, 3), (2, 3, \dots, 3)$ ou $(2, 2, 3, \dots, 3)$ où l'entier 3 apparaît k fois. Il en découle que $p_n = 3^k$ si $n = 3k$, $p_n = 2 \cdot 3^k$ si $n = 3k + 2$ et $p_n = 4 \cdot 3^k$ si $n = 3k + 4$.

- 4) Soit G un sous-groupe abélien de S_n . Notons O_1, \dots, O_r les orbites de $\llbracket 1, n \rrbracket$ sous G .
 - Pour tous $k \in \llbracket 1, r \rrbracket$ et $g \in G$, $g|_{O_k}$ est une permutation de O_k , et l'application $g \mapsto g|_{O_k}$ un morphisme de groupes de G dans S_{O_k} dont nous noterons G_k l'image. Nos hypothèses sur G font de G_k un sous-groupe abélien transitif de S_{O_k} , donc $|G_k| = |O_k|$ d'après 2).
 - Ensuite, l'application $g \mapsto (g|_{O_1}, \dots, g|_{O_r})$ est un morphisme de groupes injectif de G dans $G_1 \times \dots \times G_r$ — injectif car une permutation qui fixe O_1, \dots, O_r fixe leur réunion $\llbracket 1, n \rrbracket$. En particulier, $|G| \leq |G_1| \dots |G_r|$ donc $|G| \leq |O_1| \dots |O_r|$. Remarquons pour finir que $|O_1| + \dots + |O_r| = n$. Ainsi, $|G| \leq p_n$ par définition de p_n .
 - Faisons maintenant l'hypothèse que $|G| = p_n$. Est-ce seulement possible ? Que dire de G dans ce cas ? Plaçons-nous d'abord dans le cas où $n = 3k$ pour un certain $k \in \mathbb{N}^*$. D'après 3), $|G| = 3^k$ et la seule partition « maximale » de n est la famille $(3, \dots, 3)$ dans laquelle l'entier 3 apparaît k fois. Le groupe G est alors un conjugué du groupe engendré par les 3-cycles disjoints $(1\ 2\ 3), (4\ 5\ 6), \dots, (3n-2\ 3n-1\ 3n)$, donc isomorphe à \mathbb{Z}_3^n .

Dans le cas où $n = 3k + 1$ pour un certain $k \in \mathbb{N}^*$, d'après 3), $|G| = 4 \cdot 3^{k-1}$ et les seules partitions « maximales » de n possibles sont $(2, 2, 3, \dots, 3)$ et $(4, 3, \dots, 3)$ à l'ordre des termes près, dans lesquelles l'entier 3 apparaît $k - 1$ fois. Le groupe G est alors un conjugué du groupe engendré :

- soit par le 4-cycle $(1\ 2\ 3\ 4)$ et les 3-cycles $(5\ 6\ 7), \dots, (3n-1\ 3n\ 3n+1)$, donc isomorphe à $\mathbb{Z}_4 \times \mathbb{Z}_3^{k-1}$,
- soit par les transpositions $(1\ 2)$ et $(3\ 4)$ et les 3-cycles $(5\ 6\ 7), \dots, (3n-1\ 3n\ 3n+1)$, donc isomorphe à $\mathbb{Z}_2^2 \times \mathbb{Z}_3^{k-1}$.

Dans le cas enfin où $n = 3k + 2$ pour un certain $k \in \mathbb{N}^*$, d'après 3), $|G| = 2 \cdot 3^k$ et la seule partition « maximale » de n est $(2, 3, \dots, 3)$ à l'ordre des termes près, dans laquelle l'entier 3 apparaît k fois. Le groupe G est alors un conjugué du groupe engendré par la transposition $(1\ 2)$ et les 3-cycles $(3\ 4\ 5), \dots, (3n\ 3n+1\ 3n+2)$, donc isomorphe à $\mathbb{Z}_2 \times \mathbb{Z}_3^k$.

4.4 GROUPES LINÉAIRES

- 1) Ce sont des résultats très classiques. Pour la première égalité, le groupe $\text{GL}_n(\mathbb{F}_q)$ agit librement et transitivement sur l'ensemble des bases du \mathbb{F}_q -espace vectoriel \mathbb{F}_q^n , lesquelles, construites de proche en proche vecteur par vecteur, sont au nombre de $(q^n - 1)(q^n - q) \dots (q^n - q^{n-1}) = q^{1+2+\dots+(n-1)} \prod_{k=1}^n (q^k - 1) = q^{\frac{n(n-1)}{2}} \prod_{k=1}^n (q^k - 1)$. Pour la seconde égalité, $Z(\text{GL}_n(\mathbb{F}_q)) = \mathbb{F}_q^* I_n$ donc $|Z(\text{GL}_n(\mathbb{F}_q))| = q - 1$.

2) a) Soit $r \in \llbracket 1, n-1 \rrbracket$. L'essentiel est dans les relations suivantes, valables pour toutes matrices $M, N \in \mathcal{M}_{r, n-r}(\mathbb{F}_q)$:

$$\begin{pmatrix} I_r & M \\ 0 & I_{n-r} \end{pmatrix} \begin{pmatrix} I_r & N \\ 0 & I_{n-r} \end{pmatrix} = \begin{pmatrix} I_r & M+N \\ 0 & I_{n-r} \end{pmatrix} = \begin{pmatrix} I_r & N \\ 0 & I_{n-r} \end{pmatrix} \begin{pmatrix} I_r & M \\ 0 & I_{n-r} \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} I_r & M \\ 0 & I_{n-r} \end{pmatrix}^{-1} = \begin{pmatrix} I_r & -M \\ 0 & I_{n-r} \end{pmatrix}.$$

b) Pour tout $r \in \llbracket 1, n-1 \rrbracket$, on peut prolonger a) en remarquant que les matrices $\begin{pmatrix} \lambda I_r & M \\ 0 & \lambda I_{n-r} \end{pmatrix}$, λ décrivant \mathbb{F}_q^* et M décrivant $\mathcal{M}_{r, n-r}(\mathbb{F}_q)$, forment un sous-groupe abélien de $\text{GL}_n(\mathbb{F}_q)$ d'ordre $|\mathcal{M}_{r, n-r}(\mathbb{F}_q)| \cdot |\mathbb{F}_q^*| = q^{r(n-r)}(q-1)$. Il nous reste à montrer qu'on peut effectivement atteindre la borne $q^{\lfloor \frac{n^2}{4} \rfloor} (q-1)$ en choisissant bien r .

— Or si n est pair, alors pour $r = \frac{n}{2}$: $r(n-r) = r^2 = \lfloor \frac{n^2}{4} \rfloor$.

— Et si n est impair, alors pour $r = \frac{n-1}{2}$: $r(n-r) = r^2 + r = \lfloor r^2 + r + \frac{1}{4} \rfloor = \lfloor \frac{n^2}{4} \rfloor$.

3) Pour commencer : $\frac{q^2-1}{q-1} = q+1 > q = q^{\lfloor \frac{2^2}{4} \rfloor}$ et $\frac{q^3-1}{q-1} = q^2+q+1 > q^2 = q^{\lfloor \frac{3^2}{4} \rfloor}$.

Ensuite, pour tout entier pair $n = 2p$ avec $p \geq 2$: $\lfloor \frac{n^2}{4} \rfloor = \lfloor p^2 \rfloor = p^2 \geq 2p = n$, et pour tout entier impair

$n = 2p+1$ avec $p \geq 2$: $\lfloor \frac{n^2}{4} \rfloor = \lfloor p^2 + p + \frac{1}{4} \rfloor = p^2 + p \geq 2p+1 = n$, donc $\lfloor \frac{n^2}{4} \rfloor \geq n$ pour tout $n \geq 4$. Enfin :

$$\frac{q^n-1}{q-1} \leq q^n - 1 < q^n \leq q^{\lfloor \frac{n^2}{4} \rfloor}.$$