Proposition de corrigé TD1 CM

Maxence Caucheteux

October 30, 2023

Exercice 2

Q1

$SL_n(k)$ est un sous-groupe de $GL_n(k)$ (vérifications élémentaires). Pour $A \in GL_n(k)$ et $B \in SL_n(k)$, $\det(ABA^{-1}) = \det(B) = 1$ donc $ABA^{-1} \in SL_n(k)$. Donc $SL_n(K) \triangleleft GL_n(k)$. L'application

$$\begin{array}{cccc} \phi & : & GL_n(k)/SL_n(k) & \to & k^* \\ & & \bar{M} & \mapsto & \det(M) \end{array}$$

est bien définie et est un isomorphisme de groupes.

Preuve :

> Il est clair qu'elle est bien définie (image indépendante du choix du représentant et bien à valeur dans k^*) et que c'est un morphisme de groupes.
>
> Si $\phi(\bar{M}) = \det(M) = 1$, alors $M \in SL_n(k)$ et $\bar{M} = SL_n(k)$, donc ϕ est injective. Pour $x \in k^*$, on pose $M = D(x, 1_k, ..., 1_k) \in GL_n(k)$, de sorte que $\phi(\bar{M}) = \det(M) = x$, ce qui montre la surjectivité de ϕ.

Ainsi $GL_n(k)/SL_n(k) \cong k^*$

Q2 Soit τ une transposition de H (il en existe une par hypothèse). On note $\tau = (i\ j)$. On a :

$$\forall \sigma \in S_n,\ \sigma\tau\sigma^{-1} = (\sigma(i)\ \sigma(j))$$

Cela prouve que H contient toutes les transpositions de S_n. Comme les transpositions engendrent S_n, on a $H = S_n$

Exercice 3 - Centre

Q1 Les f_g $(g \in G)$ sont des automorphismes.

Morphismes : $\forall g \in G$, $\forall x_1, x_2 \in G$,

$$f_g(x_1x_2) = gx_1x_2g^{-1} = (gx_1g^{-1})(gx_2g^{-1}) = f_g(x_1)f_g(x_2)$$

Bijectifs : Les morphismes f_g admettent pour réciproque :

$$\begin{array}{cccc} \phi & : & G & \to & G \\ & & x & \mapsto & g^{-1}xg \end{array}$$

Ainsi $\mathrm{Int}(G) \subset \mathrm{Aut}(G)$.

$\mathrm{Int}(G)$ est un sous-groupe de $\mathrm{Aut}(G)$.

$\mathrm{id}_G = f_{e_g}$ donc $\mathrm{id}_G \in \mathrm{Int}(G)$

Si $g_1, g_2 \in G$, pour $x \in G$,

$$f_{g_1} \circ f_{g_2}(x) = f_{g_1}(g_2 x g_2^{-1}) = g_1 g_2 x g_2^{-1} g_1^{-1} = (g_1 g_2) x (g_1 g_2)^{-1} = f_{g_1 g_2}(x)$$

Donc $f_{g_1} \circ f_{g_2} \in \mathrm{Int}(G)$.

Si $g \in G$, $f_g^{-1} = f_{g^{-1}}$ donc $f_g^{-1} \in \mathrm{Int}(G)$.

$Z(G)$ est un sous-groupe normal de G.

Preuve :

C'est bien un sous-groupe de G (vérifications élémentaires) et il est distingué car pour $g \in G$ et $h \in Z(G)$, pour tout $x \in G$, $ghg^{-1}x = gg^{-1}hx = hx$ et $xghg^{-1} = xhgg^{-1} = xh = hx$. Donc $ghg^{-1} \in Z(G)$, ce qui conclut.

Q2 On note $(\bar{g}_i)_{i \in I}$ les classes d'équivalence distinctes ($g_i \in G$). On définit :

$$\begin{array}{rccc} \phi & : & G/Z(G) & \to & \mathrm{Int}(G) \\ & & \bar{g}_i & \mapsto & f_{g_i} \end{array}$$

ϕ est bien définie. En effet, pour $i \in I$ et $z \in Z(G)$,

$$\forall x \in G,\ f_{g_i z}(x) = (g_i z) x (g_i z)^{-1} = g_i x g_i^{-1}$$

(image indépendante du représentant choisi)

Pour $i, j \in I$,

$$\phi(\bar{g}_i \bar{g}_j) = \phi(\overline{g_i g_j}) = f_{g_i g_j} = f_{g_i} \circ f_{g_j} = \phi(\bar{g}_i) \circ \phi(\bar{g}_j)$$

Donc ϕ est un morphisme.

Si $\bar{g}_i$ ($i \in [1, k]$) vérifie $\phi(\bar{g}_i) = \mathrm{id}_G$ ie :

$$\forall x \in G,\ g_i x = x g_i$$

Donc $g_i = Z(G)$ et $\bar{g}_i = Z(G)$. ϕ est donc injective.

Soit $f_g \in \mathrm{Int}(G)$ (avec $g \in G$), on a alors $\phi(\bar{g}) = f_g$. Donc ϕ est surjective.

Bilan : ϕ est un isomorphisme donc

$$G/Z(G) \cong \mathrm{Int}(G)$$

Q3 Si $G/Z(G)$ est est monogène. $G/Z(G)$ s'écrit $G/Z(G) =< gZ(G) >$. Soient $g_1, g_2 \in G$. Alors $g_1 = g^{k_1} z_1$ et $g_2 = g^{k_2} z_2$ avec $z_1, z_2 \in Z(G)$.

Ainsi :

$$g_1 g_2 = g^{k_1} z_1 g^{k_2} z_2 = g^{k_1} g^{k_2} z_1 z_2 = g^{k_2} g^{k_1} z_2 z_1 = g^{k_2} z_2 g^{k_1} z_1 = g_2 g_1$$

Donc G est abélien.

Exercice 4 - Décomposition directe

On définit :

$$\begin{array}{rcrcl}\phi & : & H \times K & \to & G \\ & & (h,k) & \mapsto & hk\end{array}$$

ϕ est un morphisme de groupes.

Preuve :

On montre d'abord que pour $(h,k) \in H \times K$, $hk = kh$. Comme $H \lhd G$, $kh^{-1}k^{-1} \in H$ puis $hkh^{-1}k^{-1} \in H$. De même, comme $K \lhd G$, $hkh^{-1} \in K$ puis $hkh^{-1}k^{-1} \in K$. Ainsi, $hkh^{-1}k^{-1} \in H \cap K = \{e_G\}$. Donc $hk = kh$.

Ainsi, pour $(h_1,k_1),(h_2,k_2) \in H \times K$, on a :

$$\phi(h_1h_2, k_1k_2) = h_1h_2k_1k_2 = h_1k_1h_2k_2 = \phi(h_1,k_1)\phi(h_2,k_2)$$

ϕ est donc un morphisme de groupes.

Il est surjectif car $HK = G$.

Si $(h,k) \in H \times K$ vérifie $\phi(h,k) = hk = e_G$, alors $h = k^{-1} \in H \cap K = \{e_G\}$ donc $h = k = e_G$. Cela montre l'injectivité de ϕ.

ϕ est donc un isomorphisme : $G \cong H \times K$

Exercice 5 - Groupe dérivé

Q1 Pour $g \in G$, $z = [x,y] \in D(G)$ (avec $x, y \in G$), on remarque que :

$$gzg^{-1} = [gxg^{-1}, gyg^{-1}] \in D(G)$$

Pour $z \in D(G)$, z s'écrit sous la forme $z = z_1...z_k$ où les z_i sont des commutateurs. Alors pour tout $g \in G$, par ce qui précède :

$$gzg^{-1} = gz_1...z_kg^{-1} = (gz_1g^{-1})...(gz_kg^{-1}) \in D(G)$$

On a donc montré que $D(G) \lhd G$.

Q2

Sens indirect : Si $D(G) \subset H$. Alors $[g_1^{-1}, g_2^{-1}] \in H$ ie $g_1^{-1}g_2^{-1}g_1g_2 \in H$, puis $g_1g_2 \in g_2g_1H$. Donc $(g_1g_2)H \subset (g_2g_1)H$.

Par symétrie des rôles entre g_1 et g_2, l'inclusion réciproque est vraie et on a $(g_1g_2)H = (g_2g_1)H$. Ainsi G/H est abélien.

Sens indirect : Si G/H est abélien. Soient $x, y \in G$. On veut montrer que $[x,y] \in H$. On écrit $x = g_1h_1$ et $y = g_2h_2$ avec $g_1, g_2 \in G$ et $h_1, h_2 \in H$. Alors :

$$[x,y] = g_1h_1g_2h_2(g_2h_2g_1h_1)^{-1}$$

Or, comme G/H est abélien, il existe $\tilde{h}, \tilde{\tilde{h}} \in H$ tels que $g_1h_1g_2h_2 = g_2g_1h_1\tilde{h}$ et $g_2h_2g_1h_1 = g_1g_2h_2\tilde{\tilde{h}}$. De sorte que :

$$[x,y] = g_2g_1h_1\tilde{h}\tilde{\tilde{h}}^{-1}h_2^{-1}g_2^{-1}g_1^{-1}$$

Comme G/H est abélien, il existe $h \in H$ tel que $g_1 g_2 = g_2 g_1 h$. Ainsi, par ce qui précède et puisque $H \rhd G$, on a :

$$[x, y] = (g_1 g_2)(h^{-1} h_1 \tilde{h} \tilde{\tilde{h}}^{-1} h_2^{-1})(g_1 g_2)^{-1} \in H$$

Donc $D(G) \subset H$.

Exercice 6 - Groupe résoluble, Galois

Q2

Sens direct

Si G est résoluble, il existe $n_0 \in \mathbb{N}^*$ tel que :

$$G_0 = \{e\} \lhd G_1 \lhd ... \lhd G_{n_0} = G$$

avec $\forall i \in [0, n_0 - 1],\ G_{i+1}/G_i$ abélien.

Par Ex5, comme G_{i+1}/G_i est abélien, on a :

$$\forall i \in [0, n_0 - 1],\ D(G_{i+1}) \subset G_i$$

Une récurrence immédiate montre alors que :

$$D^{n_0}(G) \subset \{e\}$$

Donc $D^{n_0}(G) = \{e\}$, ce qui conclut.

Sens indirect

Si $(D^n(G))_{n \in \mathbb{N}}$ stationne à $\{e\}$. Soit n_0 un entier tel que $D^{n_0}(G) = \{e\}$. Alors :

$$G_0 = \{e\} \lhd G_1 \lhd ... \lhd G_{n_0} = G$$

et en vertu de Ex5, $\forall i \in [0, n_0 - 1],\ D^{i+1}(G)/D^i(G)$ est abélien.

Donc G est résoluble.

Exercice 7 - Exemples de groupes résolubles

Q2 Comme $rs = sr^{-1}$, des calculs élémentaires montrent que $D(D_n) =< r^2 >$. Ce dernier groupe étant abélien, $D^2(D_n) = \{e\}$. Par Ex6 Q2, D_n est donc résoluble.

Exercice 8 - Groupe simple

Q1 Tout sous-groupe H d'un groupe abélien G est distingué. Ainsi, les groupes abéliens simples sont les groupes G admettant exactement deux sous-groupes, à savoir $\{e_G\}$ et G.

Or les seuls groupes G non triviaux dont les seuls sous-groupes sont $\{e_G\}$ et G sont les groupes cycliques d'ordre p premier (ce sont donc les groupes isomorphes à un $\mathbb{Z}/p\mathbb{Z}$ avec p premier).

Preuve :

> Sens indirect immédiat par théorème de Lagrange. Pour le sens direct, si G est non trivial dont les seuls sous-groupes sont triviaux, avec $x \in G$ différent de e_G, on a alors $< x >= G$. G est donc monogène. Si par l'absurde il était infini, il serait isomorphe à $\mathbb{Z}$, ce qui n'est pas possible car $\mathbb{Z}$ admet des sous-groupes stricts. G est donc cyclique.

G est en fait d'ordre premier. En effet, si par l'absurde il ne l'est pas, avec $1 < d < |G|$ un diviseur de $|G|$, un lemme connu montre alors qu'il existe un élément $x \in G$ d'ordre d. Ainsi le groupe $< x >$ est un sous-groupe strict de G, ce qui est absurde.

Q2 Si G et simple est résoluble, il est abélien. Il est donc isomorphe à un $\mathbb{Z}/p\mathbb{Z}$ avec p premier par $Q1$.

Exercice 10

On définit :

$$\begin{array}{cccc} \phi & : & H & \rightarrow & \mathrm{Aut}(N) \\ & & h & \mapsto & \phi_h : n \mapsto hnh^{-1} \end{array}$$

ϕ est bien défini car N est distingué dans G et c'est un morphisme de groupes (vérifications élémentaires).

On définit alors :

$$\begin{array}{ccccc} f & : & N \rtimes_f H & \rightarrow & G \\ & & (n, h) & \mapsto & nh \end{array}$$

Des vérifications élémentaires montrent que f est un morphisme de groupes. C'est en fait un isomorphisme de groupes. L'injectivité est vraie grâce à $N \cap H = \{e_G\}$ et la surjectivité provient du fait que $NH = G$.

Ainsi, $N \rtimes_f H \cong G$.

Exercice 11

Q1 On note $C = \{(x, y) \in G^2 \mid xy = yx\}$. La probabilité recherchée est $\frac{|C|}{|G \times G|} = \frac{|C|}{|G|^2}$. On a :

$$\begin{aligned} C &= \bigsqcup_{x \in G} \{x\} \times C_x & (1) \\ &= (\bigsqcup_{x \in Z(G)} \{x\} \times C_x) \bigsqcup (\bigsqcup_{x \notin Z(G)} \{x\} \times C_x) & (2) \\ &= (\bigsqcup_{x \in Z(G)} \{x\} \times G) \bigsqcup (\bigsqcup_{x \notin Z(G)} \{x\} \times C_x) & (3) \end{aligned}$$

Puis, en cardinaux :

$$\begin{aligned} C &= |Z(G)|.|G| + \sum_{x \notin Z(G)} |C_x| & (4) \\ &= zn + \sum_{x \notin Z(G)} |C_x| & (5) \\ &\leq zn + (|G| - |Z(G)|) \max_{x \notin Z(G)} |C_x| & (6) \end{aligned}$$

Or, les C_x sont des sous-groupes de G (vérifications élémentaires). Pour $x \notin Z(G)$, ce sont des sous-groupes stricts de G. Par théorème de Lagrange, on a donc :

$$\forall x \notin Z(G),\ |C_x| \leq \frac{n}{2}$$

Puis :

$$|C| \leq \frac{zn}{2} + \frac{n^2}{2}$$

Q2 Comme G n'est pas abélien, via contraposée de Ex3, $G/Z(G)$ n'est pas monogène. On peut montrer que tous les groupes d'ordre $1, 2, 3$ sont cycliques. Ainsi, $|G/Z(G)| \geq 4$, puis $z \leq \frac{n}{4}$

Q3 Par suite :

$$|C| \leq \frac{n^2}{8} + \frac{n^2}{2} = \frac{5n^2}{8}$$

Puis :

$$\frac{|C|}{|G|^2} \leq \frac{5}{8}$$

Remarque Si G est abélien, la probabilité recherchée vaut 1.