Rapport sur l'épreuve écrite de mathématiques (filière MP, épreuve commune Paris-Lyon)

Régis de la Bretèche, Stéphane Fischler, Olivier Guichard, David Harari

Le but du problème était d'introduire les notions de base de cohomologie galoisienne (cocycles, ensembles de cohomologie) associées à l'action d'un groupe Γ sur un autre groupe G; on y démontrait notamment le théorème 90 de Hilbert, qui est l'annulation de l'ensemble de cohomologie $H^1(\Gamma, G)$ (noté $\mathcal{H}(\Gamma, G)$ dans le problème) quand G est le groupe des matrices inversibles $\mathrm{GL}_n(L)$ (à valeurs dans un corps L) et Γ le groupe des automorphismes de L laissant fixe un sous-corps K de L. On voyait également au cours du problème un morceau de la suite exacte longue de cohomologie associée à une suite exacte courte de groupes, et on déduisait de tout cela quelques applications, notamment à des théorèmes de finitude.

Le problème avait été conçu pour tester plusieurs parties du programme (groupes, algèbre linéaire, polynômes, topologie et calcul différentiel), et aussi pour étaler au mieux les notes. En ce sens il semble avoir plutôt bien rempli son rôle, puisqu'à coté de certaines copies très faibles, on trouve une copie ayant bien traité l'intégralité du problème à l'exception de deux questions, performance tout à fait étonnante et proche de la perfection; une dizaine de copies ont bien traité au moins les trois quarts du problème, et encore une centaine de copies (sur environ 800 au total) ont résolu correctement au moins la moitié des questions. Toutes les questions ont été résolues par au moins un candidat.

Dans l'ensemble le niveau nous a paru plutôt satisfaisant. Un nombre raisonnable de candidats ont bien assimilé les notions et les raisonnements de base en algèbre, ce qui leur a permis d'aller assez loin dans le problème. La partie plus analytique (essentiellement les questions II.2 et II.3) a en revanche posé de grosses difficultés à la grande majorité des candidats, mais il faut dire qu'elle était sans doute nettement plus difficile que le reste. Les rares candidats qui ont su résoudre (même partiellement) certaines de ces questions ont donc été substantiellement récompensés; nous avons été impressionnés par le candidat qui a su traiter parfaitement l'intégralité de cette difficile partie II.

Les critiques porteront cette année plus sur la forme que sur le fond. Trop de candidats perdent bêtement des points par négligence, par exemple en ne vérifiant pas complètement toutes les propriétés demandées dans les (très faciles) premières questions, ou encore en omettant de préciser qu'ils travaillent avec un polynôme non nul en III.2.b. et III.2.c. Des assertions précises comme "les translations sont des bijections dans un groupe" sont trop souvent remplacées par des phrases fumeuses du genre "les indices décrivent le même ensemble" pour la question IV.3.a. La présentation des copies laisse également parfois à désirer, certaines étant quasi-illisibles. A ce titre il n'est pas inutile de rappeler que dans une épreuve qui dure 6 heures, les candidats ont le temps de faire des essais au brouillon avant d'écrire sur leur copie.

Notons que quelques candidats perdent inutilement du temps à répondre à des questions non posées (par exemple montrer qu'un groupe dans lequel tout élément x vérifie $x^2 = 1$ est commutatif : merci à ceux qui nous ont rappelé ce fait, que nous n'ignorions pas, mais dont nous n'avons pas voulu demander la démonstration en II.1 pour ne pas avantager ceux qui connaissaient ce résultat classique); certains redémontrent (parfois avec des erreurs !) l'énoncé admis dans le préambule; certains invoquent des notions compliquées dont l'intérêt dans ce problème était pour le moins obscur (on a vu des "applications étales" et des "polynômes interpolateurs" par exemple). Enfin d'autres croient voir des erreurs là où il n'y en avait (une fois n'est pas coutume ?) pas, par exemple en V.2.a) où il s'agissait bien du groupe orthogonal complexe, et non pas unitaire (lequel n'est d'ailleurs pas commutatif !) comme ils le pensaient (sans doute l'idée de considérer un groupe orthogonal sur un corps autre que $\mathbf{R}$ est-elle traumatisante...).

Ces remarques générales étant faites, voyons le déroulement du problème.

Partie I.

A l'exception de la question I.4.b), cette première partie était très facile et permettait aux candidats de rentrer en douceur dans l'épreuve. Signalons quand même que très peu de candidats ont pensé en I.1. à écrire que $\mathrm{Aut}\, G$ était un sous-groupe du groupe des permutations de G, alors que le premier critère à essayer pour montrer qu'un ensemble (muni d'une loi interne) est un groupe est toujours de regarder s'il n'est pas sous-groupe d'un groupe connu. Nous avons été surpris de constater qu'en I.4.b), beaucoup de candidats se sont contentés d'écrire que l'inclusion pouvait sans doute être stricte sans chercher un exemple de cette situation. Parmi ceux qui ont essayé de le faire, très peu y sont parvenus alors qu'il suffisait de considérer l'action définie en

I.3. dans le cas le plus simple $n = 1$.

Partie II.

La question II.1. a été bien faite dans l'ensemble, à part d'honteuses erreurs de comptage ($2n$ ou n^2 au lieu de 2^n pour les matrices diagonales à coefficients dans ± 1...) et le manque de clarté dans l'application des théorèmes de diagonalisation.

La question II.2. était sans doute la plus difficile du problème puisqu'elle nécessitait à la fois de comprendre un point subtil (U n'était pas un ouvert de $\mathrm{GL}_n(\mathbf{C})$ mais seulement de A), de se ramener à une application entre ouverts d'e.v.n. réels en utilisant φ, puis d'appliquer le théorème d'inversion locale à l'application ainsi obtenue. [1]

La question II.3.a) était également difficile, et seuls deux ou trois candidats ont compris qu'il s'agissait d'éliminer une variable dans l'équation $\det M = 1$ pour obtenir la situation de II.2. avec $p = n^2 - 1$ (et non pas n, n^2, ou $2n$ comme on l'a trouvé dans certaines copies). II.3.b) était plus abordable à condition d'avoir un peu compris les résultats qui précédaient et réalisé que dans le groupe G, les translations étaient des homéomorphismes.

Partie III.

La question III.1.a) a été fréquemment très mal rédigée. Les candidats se sont souvent embarqués dans des calculs longs et compliqués au lieu de chercher simplement des complexes de module 1 en dehors du spectre de A; du coup leurs preuves étaient incomplètes (par exemple ils ne vérifiaient pas que $\bar{\lambda}/\lambda$ prenait bien une infinité de valeurs pour λ complexe non nul). III.1.b) demandait juste d'appliquer le résultat précédent, ce que pas mal de candidats ont vu.

III.2. a également été plutôt bien faite, mais trop de solutions sont peu soigneuses (le polynôme P doit être non nul, le fait qu'on ne considère que les automorphismes qui laissent fixe K est essentiel), voire fausses (en III.2.c. il ne suffit pas de dire que pour un élément donné x de L, il n'y a qu'un nombre fini de $\gamma(x)$ possibles).

III.3. a été souvent abordée, mais rarement bien terminée, les candidats se perdant dans des calculs qui n'aboutissaient pas au lieu de traduire simplement la propriété de morphisme.

[1] Ici, *mea culpa*, il semble qu'un ahurissant allègement ait rendu la forme générale de ce théorème hors-programme en ne laissant que sa forme "globale", qu'on ne peut évidemment démontrer sans la forme locale. Dans la mesure où ces résultats sont de toute façon admis, on ne peut qu'être étonné d'une telle aberration, d'autant que le théorème des fonctions implicites ne semble pas avoir été explicitement supprimé du programme...

III.4) a été en général bien traitée par les candidats qui l'ont abordée; signalons quand même les sempiternelles confusions entre complémentaire et supplémentaire en III.4.b) qui sont indignes d'un bon élève de MP*.

Partie IV.

IV.1. était juste une vérification immédiate. IV.2. demandait l'utilisation de III.1.b), ce qu'un nombre raisonnable de candidats a vu.

Nous avons été agréablement surpris du fait qu'un nombre non négligeable de candidats ait su traiter IV.4. en appliquant correctement III.4.c), même s'il y a eu quelques cafouillages dans les calculs.

IV.4. et IV.5.a) étaient très faciles et récompensaient les candidats qui avaient réussi à digérer les notations pour arriver jusque-là.

IV.5.b) et IV.5.c) étaient évidemment bien plus délicates, et n'ont été résolues que par peu de candidats.

Partie V.

V.1.a) demandait juste de se rappeler des résultats de II. et a permis à nombre de candidats de grapiller quelques points. V.1.b) nécessitait de reprendre la définition d'un cocycle; plusieurs candidats ont ici donné une réponse erronée en oubliant que le b donnant l'équivalence avec le cocyle trivial devait rester dans G. Seuls les tout meilleurs candidats ont réussi à faire la synthèse pour traiter V.1.c).

V.2.) a été peu abordée, certains candidats écrivant des choses tout à fait fantaisistes en mélangeant les groupes orthogonaux réels et complexes.

V.3.a) était facile; V.3.b) a été faite par quelques bons candidats qui ont vu l'argument de conjugaison des deux 3-cycles de $\mathcal{S}_3$, qui ne sont évidemment pas conjugués dans le groupe (abélien) qu'ils engendrent.

En conclusion, si le niveau d'ensemble de ceux qui ont passé cette épreuve nous a paru fort correct, beaucoup de candidats pourraient gagner un nombre de points appréciable en soignant la rédaction et la présentation.

Corrigé de l'épreuve de mathématiques commune Paris-Lyon (filière MPI)

Partie I

I.1 $\operatorname{Aut} G$ est un sous-ensemble du groupe $(\mathcal{S}(G), \circ)$ des bijections de G dans G. Comme pour tous f, g de $\operatorname{Aut} G$, $f \circ g$ et f^{-1} sont encore des morphismes, $(\operatorname{Aut} G, \circ)$ est un sous-groupe de $(\mathcal{S}(G), \circ)$.

I.2 Comme $\Phi(\gamma)$ est un morphisme, on a ${}^{\gamma}(g_1 g_2) = {}^{\gamma} g_1 \, {}^{\gamma} g_2$ et aussi ${}^{\gamma} e_G = e_G$, ${}^{\gamma}(g^{-1}) = ({}^{\gamma} g)^{-1}$. D'autre part $\Phi : G \to \operatorname{Aut} G$ est un morphisme, d'où ${}^{(\gamma_1 \gamma_2)} g = {}^{\gamma_1} ({}^{\gamma_2} g)$ et ${}^{e_\Gamma} g = g$.

I.3 L'identité et la conjugaison sont des automorphismes du groupe multiplicatif $\mathrm{GL}_n(\mathbf{C})$, donc Φ est bien à valeurs dans $\operatorname{Aut} G$. C'est un morphisme car la conjugaison est une involution. On a immédiatement $\mathrm{GL}_n(\mathbf{C})^{\Gamma_2} = \mathrm{GL}_n(\mathbf{R})$.

I.4 a) Si $\gamma \in \Gamma$ et $x \in G^{\Gamma}$, alors ${}^{\gamma}(u(x)) = u({}^{\gamma} x) = u(x)$ d'où $u(x) \in H^{\Gamma}$.

b) Non : prendre l'action par conjugaison de $\Gamma_2 = \{\pm 1\}$ sur $\mathbf{C}^* = \mathrm{GL}_1(\mathbf{C})$, et $u : \mathbf{C}^* \to \mathbf{C}^*, x \mapsto x^2$. Alors la restriction $\mathbf{R}^* \to \mathbf{R}^*$ de u n'est pas surjective.

Partie II

II.1 Tout élément de G est diagonalisable car il annule le polynôme scindé à racines simples $X^2 - 1 = (X-1)(X+1)$. D'après le résultat rappelé dans l'introduction, il existe une matrice P dans $\mathrm{GL}_n(\mathbf{C})$ telle que $M_g := P g P^{-1}$ soit diagonale pour tout g de G. Comme $M_g^2 = I_n$, l'ensemble des M_g pour g dans G est inclus dans l'ensemble des matrices diagonales dont les éléments diagonaux sont 1 ou -1. En particulier M_g (et donc G) est fini de cardinal au plus 2^n.

II.2 Déjà f est bien définie car si x, y sont dans V_1, alors $\varphi^{-1}(x)$ et $\varphi^{-1}(y)$ sont dans U, donc leur produit est dans A, or $\varphi(A) = V$. D'autre part, comme φ est un homéomorphisme et U est un ouvert de A, V_1 est un ouvert de V (donc de $\mathbf{R}^p$).

Soit $a = \varphi(I_n)$. Alors $a \in V_1$ et les applications partielles $x \mapsto f(x, a)$ et $y \mapsto f(a, y)$ en (a, a) sont toutes deux égales à l'identité de V_1. La différentielle en a de l'application $\theta : V_1 \to V$ définie par $\theta(x) = f(x, x)$ est donc $2\mathrm{id}_{\mathbf{R}^p}$. Par le théorème d'inversion locale, l'image W de θ est un voisinage de $\theta(a) = \varphi(I_n)$ dans V. Comme φ est un homéomorphisme, $\varphi^{-1}(W)$ est un voisinage dans A de $\varphi^{-1}(a) = I_n$. Or par définition $\varphi^{-1}(W)$

est l'ensemble des $(\varphi^{-1}(x))^2$ pour x dans V_1, i.e. l'ensemble des M^2 pour M dans U.

II.3 a) Soit $M = (a_{ij})$ dans $M_n(\mathbf{C})$, alors en développant par rapport à la première colonne on obtient $\det M = a_{11}P(a_{22}, ..., a_{nn}) + Q(a_{12}, ..., a_{nn})$, où P et Q sont des polynômes en les coefficients de M ne dépendant pas de a_{11}. Soit A l'ouvert de $\mathrm{SL}_n(\mathbf{R})$ défini par $P(a_{22}, ..., a_{nn}) \neq 0$. Alors l'application φ de A dans $\mathbf{R}^{n^2-1}$ définie par $\varphi(M) = (a_{ij})_{(i,j)\neq(1,1)}$ est un homéomorphisme de A sur l'ouvert V de $\mathbf{R}^{n^2-1}$ défini par $P(a_{22}, ..., a_{nn}) \neq 0$, la réciproque étant définie en associant à $(a_{ij})_{(i,j)\neq(1,1)}$ la matrice dont le terme d'indice $(1,1)$ est $1 - Q((a_{ij}))/P(a_{22}, ..., a_{nn})$ et le terme d'indice (i,j) (pour $(i,j) \neq (1,1)$) est a_{ij}.

Par continuité, on dispose d'un ouvert U de A contenant I_n tel que pour M, N dans U, on ait $MN \in A$ car A est un ouvert de $\mathrm{SL}_n(\mathbf{R})$ contenant $I_n = I_n.I_n$. Alors l'application f définie comme en II.2 est bien C^1 car ses composantes sont des fonctions rationnelles. [1]

b) Soit ψ l'application $M \mapsto M^2$ de G dans G, c'est un morphisme de groupes car G est commutatif. D'autre part d'après II.2, l'image J de ψ contient un ouvert U de G avec $I_n \in U$. Si maintenant $a = \psi(M_0)$ est dans J, alors a est dans l'ouvert[2] aU de G, qui est lui-même inclus dans J vu que tout x de U s'écrit $\psi(M)$ avec $M \in G$, d'où $ax = \psi(M_0M)$. Finalement J est bien un ouvert de G. Comme c'est le complémentaire dans G de la réunion des $M_0.J$ pour M_0 non dans J (car J est un sous-groupe de G), J est également fermé dans G.

Partie III

III.1 a) Il suffit de prendre λ de module 1 tel que $-\bar{\lambda}/\lambda$ ne soit pas valeur propre de A; c'est possible car le polynôme caractéristique de A n'a qu'un nombre fini de racines, tandis que pour t réel et $\lambda = e^{it}$, $-\bar{\lambda}/\lambda = -e^{-2it}$ prend une infinité de valeurs.

b) On cherche B sous la forme $B = \lambda I_n + \bar{\lambda}A$. Alors l'égalité voulue s'écrit $M\overline{B} = B$, soit $\bar{\lambda}M + \lambda M\overline{A} = \lambda I_n + \bar{\lambda}A$.

On prend donc $A = M$, alors $M\overline{A} = I_n$, et on applique le a) pour trouver λ tel que B soit inversible.

III.2 a) Si $\gamma \in \Gamma$, l'image de i par γ doit avoir un carré égal à -1, donc être i ou $-i$. Comme $\gamma(a+ib) = a+\gamma(i)b$ pour a, b réels, on obtient que γ est l'identité ou la conjugaison complexe. Réciproquement ces deux applications

[1] L'axiome (L) correspond en gros au fait que G soit un groupe de Lie.

[2] Noter que la multiplication par a est un homéomorphisme de G sur lui-même.

sont bien des isomorphismes de corps de $\mathbf{C}$ dans $\mathbf{C}$ qui induisent l'identité sur $\mathbf{R}$.

b) Le K-ev engendré par $(1, x, ..., x^n, ...)$ est inclus dans L, donc il est de dimension finie. Par conséquent, la famille précédente est liée, ce qui donne $P \in K[X]$ non nul avec $P(x) = 0$. Si $P = \sum_{i=0}^{n} a_i X^i$ avec $a_i \in K$, alors $\gamma(P(x)) = P(\gamma(x))$ car $\gamma(a_i) = a_i$ et γ est un automorphisme du corps L. Ainsi $\gamma(x)$ est racine de P.

c) Soit $\gamma \in \Gamma$. Soit $(x_1, ...x_n)$ une base du K-ev L. On vient de voir que pour chaque i, $\gamma(x_i)$ ne peut prendre qu'un nombre fini de valeurs. Comme l'application $\gamma : L \to L$ est K-linéaire, elle est déterminée par ses valeurs sur $x_1, ..., x_n$. Finalement Γ est fini.

III.3 Pour $r = 1$, c'est clair. Supposons le résultat vrai pour $r - 1$. Si on a $\sum_{i=1}^{r} \lambda_i \rho_i = 0$ avec $\lambda_i \in L$, alors pour tous x, y de L^*, on a

$$\sum_{i=1}^{r} \lambda_i \rho_i(x) = 0$$

et en remplaçant x par xy :

$$\sum_{i=1}^{r} \lambda_i \rho_i(x) \rho_i(y) = 0$$

vu que les ρ_i sont des morphismes. En multipliant la première équation par $\rho_1(y)$, puis en retranchant la deuxième, on obtient

$$\sum_{i=2}^{r} \lambda_i (\rho_1(y) - \rho_i(y)) \rho_i(x) = 0$$

Si on fixe y, cette égalité est vraie pour tout x. Comme par hypothèse de récurrence les ρ_i pour $2 \leq i \leq r$ sont linéairement indépendants, on en tire que $\lambda_i(\rho_1(y) - \rho_i(y)) = 0$ pour tout i et tout $y \in L^*$. Pour chaque $i \geq 2$, on peut trouver un y tel que $\rho_1(y) - \rho_i(y)$ soit non nul car $\rho_1 \neq \rho_i$ par hypothèse. Ainsi les λ_i pour $i \geq 2$ sont nuls, et evidemment aussi λ_1.

III.4 a) Si $\theta(b(x)) = 0$ pour tout x de L^n, alors $\theta(b(hx)) = 0$ pour tout x de L^n et tout h de L^*. Ceci s'écrit

$$\sum_{\gamma \in \Gamma} [\theta(f(\gamma)\gamma(x))] \gamma(h) = 0$$

Les $h \mapsto \gamma(h)$ pour $\gamma \in \Gamma$ sont des morphismes deux à deux distincts de L^* dans L^*. Pour x fixé, l'égalité précédente est vraie pour tout h de L^*, et III.3 implique alors que $\theta(f(\gamma)\gamma(x)) = 0$ pour tout $\gamma \in \Gamma$, x étant arbitraire dans

L^n. Il en résulte que θ est nulle car $x \mapsto f(\gamma)\gamma(x)$ est bijective de L^n dans L^n, $f(\gamma)$ étant une matrice inversible et γ induisant une bijection de L^n sur L^n vu que c'est un automorphisme du corps L.

b) Sinon on aurait un supplémentaire $H \neq \{0\}$ de $F := \mathrm{Vect}\,(b(x)_{x \in L^n})$ dans L^n. On recolle alors une base $(e_1, ..., e_r)$ de F et une base $(e_{r+1}, ..., e_n)$ de H pour obtenir une base de L^n. La forme linéaire θ définie par $\theta(e_i) = 0$ pour $1 \leq i \leq r$, $\theta(e_i) = 1$ pour $r+1 \leq i \leq n$ contredit alors III.4 a).

c) Le i-ième vecteur colonne de $B(M)$ est $b(x_i)$, donc les vecteurs colonnes de $B(M)$ engendrent L^n, i.e. $B(M)$ est inversible.

Partie IV

IV.1 $f \sim f$ en prenant $b = e$. Si $f \sim f'$, alors $f' \sim f$ en changeant b en b^{-1}. Si $f \sim g$ et $g \sim h$, alors en écrivant $f(\gamma) = b^{-1} g(\gamma)^\gamma b$ et $g(\gamma) = c^{-1} h(\gamma)^\gamma c$ pour tout $\gamma \in \Gamma$, on obtient $f(\gamma) = b^{-1} c^{-1} h(\gamma)^\gamma c^\gamma b = (cb)^{-1} h(\gamma)^\gamma (cb)$ donc $f \sim h$. [3]

IV.2 Ici $Z(\Gamma, G)$ est l'ensemble des $f : \{\pm 1\} \to \mathrm{GL}_n(\mathbf{C})$ telles que $f(1) = I_n$ et $f(-1.-1) = f(-1)\overline{f(-1)}$, i.e. $M\overline{M} = I_n$, où $M := f(-1)$. D'après III.1.b), une telle M s'écrit $M = B\overline{B}^{-1}$ avec $B \in \mathrm{GL}_n(\mathbf{C})$, donc $f(\gamma) = C^{-1}.{}^\gamma C$ pour tout $\gamma \in \Gamma$, où $C := B^{-1}$. Ainsi f est équivalent au cocycle trivial.

IV.3 a) Soit $f : \Gamma \to \mathrm{GL}_n(L)$ un cocycle. Alors d'après III.4.c), il existe une matrice $M \in M_n(L)$ telle que la matrice

$$B := \sum_{\delta \in \Gamma} f(\delta)\delta(M)$$

soit inversible. On calcule alors, pour $\gamma \in \Gamma$,

$${}^\gamma B = \sum_{\delta \in \Gamma} {}^\gamma f(\delta).({}^{\gamma\delta} M) = \sum_{\delta \in \Gamma} f(\gamma)^{-1} f(\gamma\delta).({}^{\gamma\delta} M)$$

car f est un cocycle. La dernière somme vaut $f(\gamma)^{-1} B$ car $\delta \mapsto \gamma\delta$ est une bijection de Γ sur lui-même. Finalement $f(\gamma) = C^{-1}.{}^\gamma C$ pour tout γ de Γ, où $C := B^{-1}$, et f est équivalent au cocycle trivial. [4]

b) On retrouve IV.2, qui est donc un cas particulier élémentaire du résultat précédent.

[3] L'ensemble $\mathcal{H}(\Gamma, G)$ est l'*ensemble de cohomologie* pour l'action de Γ sur G. Il a une structure canonique de groupe abélien si G est commutatif, mais en général ce n'est qu'un ensemble pointé par 0.

[4] Ce résultat est le théorème 90 de Hilbert.

IV.4 a) Si f est un cocycle, alors pour tous γ_1, γ_2 de Γ, on a $({}^u f)(\gamma_1\gamma_2) = u[f(\gamma_1).{}^{\gamma_1}f(\gamma_2)] = u(f(\gamma_1)).{}^{\gamma_1}f(\gamma_2)$, la dernière égalité résultant de ce que u est un Γ-morphisme. On obtient bien que ${}^u f$ est un cocycle.

b) Si $f \sim f'$, alors on a un b dans G tel que pour tout $\gamma \in \Gamma$: $({}^u f)(\gamma) = u(b^{-1}.f'(\gamma).{}^\gamma b) = u(b)^{-1}.({}^u f)(\gamma).{}^\gamma(u(b))$ d'où ${}^u f \sim^u f'$ via l'élément $u(b)$ de H.

IV.5 a) Si $a \in A$, alors $u(a) = e$ donc $u({}^\gamma a) ={}^\gamma u(a) = \gamma(e) = e$ pour tout $\gamma \in \Gamma$. Ainsi ${}^\gamma a \in A$.

b) Soit $f \in Z(\Gamma, B)$. Dire que $[f] \in \operatorname{Ker} \tilde{u}$, c'est dire qu'il existe $c \in C$ tel que $u(f(\gamma)) = c^{-1}.{}^\gamma c$ pour tout $\gamma \in \Gamma$. Si $[f]$ est dans l'image de $\tilde{i}$, alors il existe un représentant de $[f]$ (et on peut supposer que c'est f) qui est à valeurs dans A; alors $u(f(\gamma)) = e$ et ${}^u f$ est le cocycle trivial.

En sens inverse, si $u(f(\gamma)) = c^{-1}.{}^\gamma c$ pour tout $\gamma \in \Gamma$, alors on écrit $c = u(b)$, $b \in B$, en utilisant la surjectivité de u. On en tire $u(f(\gamma)) = u(b^{-1}.{}^\gamma b)$, soit $f(\gamma) = b^{-1}a(\gamma){}^\gamma b$ avec $a(\gamma) := bf(\gamma){}^\gamma b^{-1}$. On remarque que $a(\gamma) \in A$ et $\gamma \mapsto a(\gamma)$ est dans $Z(\Gamma, A)$. L'égalité précédente montre que $[f] = \tilde{i}(a)$, donc f est dans l'image de $\tilde{i}$.

c) Soit $f : \Gamma \to A$ un cocycle avec $[f] \in \operatorname{Ker} \tilde{i}$. Alors par définition il existe $b \in B$ tel que $f(\gamma) = b^{-1}.{}^\gamma b$ pour tout $\gamma \in \Gamma$. Comme $f(\gamma) \in A$, on a $u(f(\gamma)) = e$ soit $u(b) \in C^\Gamma$. Mais d'après l'hypothèse supplémentaire, on a $u(b) = u(b')$ avec $b' \in B^\Gamma$ d'où $b = b'a$ avec $a \in A$, soit $f(\gamma) = a^{-1}.{}^\gamma a$ car ${}^\gamma b' = b'$. Finalement $[f] = 0$. [5]

Partie V

V.1 a) D'après II.3.b), l'image de u est ouverte et fermée dans G. Elle est donc égale à G tout entier puisque G est connexe.

b) Si $f : \Gamma_2 \to G$ est un cocycle, alors $\tilde{u}([f])$ est la classe du cocycle g qui à γ associe $f(\gamma)^2$. Ainsi $g(-1) = M^2$, où $M = f(-1)$ vérifie $M\overline{M} = I_n$. Du coup $g(1) = I_n$ et $g(-1) = M\overline{M}^{-1}$ ce qui implique $[g] = 0$ comme on l'a déjà vu en IV.2.

c) On pose $B = C = G$ et on applique IV.5.b) à $u : B \to C$, $M \mapsto M^2$ qui est surjective d'après a). Par IV.5.b) et V.1.b), $\tilde{i}$ est surjective. Mais sa source est $\mathcal{H}(\Gamma_2, A)$; or A est fini par II.1. donc comme Γ_2 est fini, $Z(\Gamma_2, A)$ aussi, et a fortiori $\mathcal{H}(\Gamma_2, A)$. Ainsi le but de $\tilde{i}$, i.e. $\mathcal{H}(\Gamma_2, G)$, est fini. [6]

[5] Les deux questions précédentes constituent une partie de la *suite exacte de cohomologie* associée à la suite exacte courte $0 \to A \to B \to C \to 0$.

[6] C'est une version très élémentaire du théorème de finitude de Borel-Serre en cohomologie galoisienne.

V.2 a) On vérifie immédiatement que $SO_2(\mathbf{C})$ est l'ensemble des matrices de la forme

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

avec a, b complexes vérifiant $a^2 + b^2 = 1$. L'application qui envoie une telle matrice sur $(a + ib, a - ib)$ est un homéomorphisme de $SO_2(\mathbf{C})$ sur le sous-ensemble de $\mathbf{C}^2$ défini par $uv = 1$, lequel est à son tour homéomorphe à $\mathbf{C}^*$ via $(u, v) \mapsto u$. Il est alors immédiat que $SO_2(\mathbf{C})$ vérifie (L).

b) On a tout de suite $A = \{\pm I_2\}$ donc comme A est commutatif et l'action de Γ_2 sur A est triviale, on obtient que $\mathcal{H}(\Gamma_2, A)$ est simplement l'ensemble des homomorphismes de groupes de Γ_2 dans A, qui est de cardinal 2.

c) On vérifie par le calcul que l'élévation au carré u dans $SO_2(\mathbf{C})$ est surjective (on peut aussi appliquer V.1.a) et V.2.a) si on sait que $SO_2(\mathbf{C})$ est connexe par arcs). Mais u induit également une surjection de $SO_2(\mathbf{R})$ sur lui-même (calcul facile, ou interprétation géométrique avec les rotations du plan). D'après IV.5.c), le noyau de $\tilde{i}$ est réduit à 0 et $\tilde{i}$ est injective puisqu'elle envoie 0 sur 0, et son ensemble de départ est de cardinal 2 d'après b). Par V.1.b), $\tilde{u} = 0$ donc $\tilde{i}$ est surjective par IV.5.b). On en conclut que le cardinal cherché est 2.

V.3 a) i est clairement un Γ-morphisme. Le noyau de $\tilde{i}$ est réduit à 0 car la signature est un morphisme surjectif sur H de noyau G, et on applique IV.5.c).

b) Un cocycle de $Z(\Gamma, G)$ est simplement un morphisme de groupes de Γ dans G. Les deux cocycles obtenus en envoyant la classe $\bar{1}$ respectivement sur $\bar{1}$ et sur $-\bar{1}$ ne sont pas équivalents dans $Z(\Gamma, G)$ car G est commutatif. Mais leurs images dans $Z(\Gamma, H)$ le sont car elles sont conjuguées dans le groupe H.[7]

[7] Le point est que les ensembles de cohomologie n'ont pas de structure naturelle de groupe quand G n'est pas commutatif. Et les résultats de IV ne donnent donc des renseignements que sur les noyaux de $\tilde{i}$, $\tilde{u}$, pas sur les relations d'équivalence qui leurs sont associées...