Devoir sur table

(samedi 7 novembre 2015)

Exercices groupes (cours).

1. *cf.* cours
2. *cf.* cours
3. *cf.* cours. Le noyau cherché est le centre de G et son image est l'ensemble de ses automorphismes intérieurs (= conjugaisons).
4. Le groupe de gauche contient $2 \times 4 \times 2 = 15$ éléments involutifs (piocher n'importe quel élément dans $\mathbf{Z}/2$, Id ou n'importe laquelle des trois transpositions de $\mathfrak{S}_3$, n'importe quel élément dans $\mathfrak{S}_2$) ; or aucun n'élément de $\left\{\pm\overline{1}\right\} \times D_8$ n'est involutif à cause de son abscisse, ce qui ne laisse que $\mathrm{Card}\left(\left\{\overline{0}\right\} \times D_8\right) = 8$ possibilités. Les deux groupes n'ont donc pas le même nombre d'involutifs : ils ne sauraient être isomorphes.
5. Définissons $\left\{\begin{array}{ccc} \mathbf{R}_+ & \longrightarrow & \mathbf{R} \\ t & \overset{\varphi}{\longmapsto} & e^t - 1 \end{array}\right.$. La fonction φ croît strictement, donc induit une bijection de $\mathbf{R}_+$ sur son image $[\lim_0 \varphi, \lim_\infty \varphi[= [0, \infty[= \mathbf{R}_+$ (on pourrait expliciter la réciproque $t \mapsto \ln(1+t)$). On observe alors pour tous réels $a, b > 0$ les égalités

$$\begin{array}{rcl} \varphi(a \boxplus b) & = & e^a + e^b - 2 = (e^a - 1) + \left(e^b - 1\right) = \varphi(a) + \varphi(b) \\ \text{et } \varphi(a \boxtimes b) & = & e^{a+b} - e^a - e^b + 1 = (e^a - 1)\left(e^b - 1\right) = \varphi(a)\,\varphi(b)\,. \end{array}$$

   Ainsi les lois $\boxplus$ *et* $\boxtimes$ sont-elles les transportées *via* la bijection φ de l'addition et de la multiplication usuelles sur $\mathbf{R}_+$, d'où toutes les propriétés demandées.
6. Soit φ un un tel morphisme. Puisque $GL_{42}(\mathbf{R})$ est engendré par ses transvections et dilatations, φ est déterminée par l'image de ces dernières. Comme en cours, la finitude du groupe but neutralise toutes les transvections et toutes les dilatations de rapport positifs (celles dont on peut extraire dans $\mathbf{R}$ une racine huitième). Soit enfin $a < 0$ et notons $h := \varphi\begin{pmatrix} 1_{41} & 0 \\ 0 & a \end{pmatrix}$. Élever au carrré donne une dilatation positive, donc (par ce qui précède) dans $\mathrm{Ker}\,\varphi$, ce qui s'écrit $h^2 = 1$. Consulter la table de $\mathbf{H}_8$ montre qu'il y a deux involutifs exactement : ± 1, d'où deux morphismes candidats.

   Réciproquement, le morphisme trivial (constamment égal à 1) convient (c'est le cas $h = 1$) et on vérifie aisément (en distinguant les quatre cas) que l'application $x \mapsto \left\{\begin{array}{l} 1 \text{ si } \det x > 0 \\ -1 \text{ si } \det x < 0 \end{array}\right.$ est un morphisme comme voulu.

Exercices anneaux (cours).

1. *cf.* cours (attention pour l'intégrité et les corps à ne pas oublier *ni* la commutativité *ni* la non-nullité)
2. Soit I un idéal de $\mathbf{Q}[X]$. S'il est nul, rien à faire. Supposons le contraire : la partie $D := \{\deg i \ ; \ i \in I \setminus \{0\}\}$ est alors non vide, donc avec un minimum. Soit $\mu \in I$ tel que $\deg \mu \leq D$. Montrons $I := (\mu)$. L'inclusion $\supset$ est immédiate vu que I est stable par multiplication par n'importe quoi. Soit $i \in I$: puisque μ est non nul, on peut effectuer une division euclidienne $i = q\mu + r$. Alors le reste s'écrit $i - q\mu$, ce qui reste dans I (ce dernier étant stable par "combinaison linéaire"), donc ou bien est nul (et on a gagné) ou bien a un degré minoré par $\min D$, ce qui est impossible vu l'hypothèse sur le reste euclidien $\deg r < \deg \mu$.
3. Son noyau est un idéal d'un corps, donc ou bien $\{0\}$ (et on gagné) ou bien tout le corps K (mais alors 1 est envoyé sur 0 et sur 1, forçant la nullité de A, exclue par hypothèse.
4. *cf.* cours.
5. *cf.* cours. Justifions le caractère "auto". L'application $x \mapsto x^c$ est injective vu les implications

$$x \in \mathrm{Ker}\,(x \mapsto x^c) \Longrightarrow x^c = 0 \overset{K \text{ intègre}}{\Longrightarrow} x = 0$$

   et elle en devient bijective puisque l'ensemble but et source sont finis (ils sont K).

6. Il s'agit de calculer $\varphi(18!)$. On commencer par décomposer $18! = 2^{16}\cdot 3^8\cdot 5^3\cdot 7^2\cdot 11\cdot 13\cdot 17$, puis on appliquer les règles vues en cours, ce qui donne :

$$\begin{aligned}\varphi(18!) &= \varphi\left(2^{16}\cdot 3^8\cdot 5^3\cdot 7^2\cdot 11\cdot 13\cdot 17\right)\\ &= \varphi\left(2^{16}\right)\varphi\left(3^8\right)\varphi\left(5^3\right)\varphi\left(7^2\right)\varphi(11)\varphi(13)\varphi(17)\\ &= 2^{15}1\cdot 3^7 2\cdot 5^2 4\cdot(7\cdot 6)\cdot 10\cdot 12\cdot 16\\ &= 2^{26}3^9 5^3 7.\end{aligned}$$

7. Notons A l'ensemble formée des matrices de la formes $\begin{pmatrix} a & -b\\ b & a\end{pmatrix}$ pour (a,b) décrivant $\mathbf{R}^2$.

(a) Soient a,b,α,β dans $\mathbf{R}$.

Montrons que A est un sous-groupe additif de $M_2(\mathbf{R})$. La matrice nulle $\begin{pmatrix} 0 & -\boxed{0}\\ \boxed{0} & 0\end{pmatrix}$ a la forme voulue, la somme $\begin{pmatrix} a & -b\\ b & a\end{pmatrix}+\begin{pmatrix} \alpha & -\beta\\ \beta & \alpha\end{pmatrix} = \begin{pmatrix} a+\alpha & -\boxed{b+\beta}\\ \boxed{\text{b+}\beta} & a+\alpha\end{pmatrix}$ aussi tout comme l'opposé $-\begin{pmatrix} a & -b\\ b & a\end{pmatrix} = \begin{pmatrix} -a & -\boxed{-b}\\ \boxed{-b} & -a\end{pmatrix}$.

Montrons que $A\setminus\{0\}$ est un sous-groupe multiplicatif de $M_2(\mathbf{R})^\times$. La matrice identité $\begin{pmatrix} 1 & -0\\ 0 & 1\end{pmatrix}$ a la forme voulue, tout comme le produit $\begin{pmatrix} a & -b\\ b & a\end{pmatrix}\begin{pmatrix} \alpha & -\beta\\ \beta & \alpha\end{pmatrix} = \begin{pmatrix} a\alpha-b\beta & a(-\beta)-b\alpha\\ b\alpha+a\beta & b(-\beta)+a\alpha\end{pmatrix} = \begin{pmatrix} a\alpha-b\beta & -\boxed{(a\beta+b\alpha)}\\ \boxed{a\beta+b\alpha} & a\alpha-b\beta\end{pmatrix}$. Supposons enfin $\begin{pmatrix} a & -b\\ b & a\end{pmatrix}$ non nulle, ce qui s'écrit aussi $a^2+b^2\neq 0$ (nous sommes dans $\mathbf{R}$) : son inverse s'exprime alors par $\frac{1}{\det\begin{pmatrix} a & -b\\ b & a\end{pmatrix}}\begin{pmatrix} a & b\\ -b & a\end{pmatrix} = \begin{pmatrix} \frac{a}{a^2+b^2} & -\boxed{\frac{-b}{a^2+b^2}}\\ \boxed{\frac{-b}{a^2+b^2}} & \frac{a}{a^2+b^2}\end{pmatrix}$, ce qui a bien la forme attendue.

(b) Notons φ la bijection donnée. Soient $c,\gamma\in\mathbf{C}$, soient $a,b,\alpha,\beta\in\mathbf{R}$ tels que $\begin{cases} c=a+ib\\ \gamma=\alpha+i\beta\end{cases}$. On a les égalités

$$\begin{aligned}\varphi(c+\gamma) &= \varphi\begin{pmatrix} a+\alpha\\ +i(b+\beta)\end{pmatrix} = \begin{pmatrix} a+\alpha & -(b+\beta)\\ b+\beta & a+\alpha\end{pmatrix} = \begin{pmatrix} a & -b\\ b & a\end{pmatrix}+\begin{pmatrix} \alpha & -\beta\\ \beta & \alpha\end{pmatrix}\\ &= \varphi(c)+\varphi(\gamma)\\ \text{et } \varphi(c\gamma) &= \varphi\begin{pmatrix} a\alpha-b\beta\\ +i(a\beta+b\alpha)\end{pmatrix} = \begin{pmatrix} a\alpha-b\beta & -(a\beta+b\alpha)\\ a\beta+b\alpha & a\alpha-b\beta\end{pmatrix} \underset{\text{précédent}}{\overset{cf/\text{ un calcul}}{=}} \begin{pmatrix} a & -b\\ b & a\end{pmatrix}\begin{pmatrix} \alpha & -\beta\\ \beta & \alpha\end{pmatrix}\\ &= \varphi(c)\varphi(\gamma),\end{aligned}$$

ce qui montre que φ respecte l'addition et la multiplication : la structure du corps $\mathbf{C}$ se trouve ainsi transportée sur A.

Exercice 1.

Supposons $G\times H$ cyclique

Un groupe cyclique étant fini, G et H doivent être finis.

Soient ensuite $G'\subset G$ et $H'\subset H$ deux sous-groupes : alors (*cf.* cours) le produit $G'\times H'$ est un sous-groupe de $G\times H$, donc est cyclique. En particulier, si $H'=\{1_H\}$, le sous-groupe $G\times\{1_G\}$, qui est isomorphe à G, est cyclique. Bien sûr, par symétrie, l'on obtient la cyclicité de H.

On cherche donc une CNS sur deux entiers $u,v\geq 1$ pour que, en posant $C_n := {}^{\mathbf{Z}}\!/_{n}$ pour tout entier $n\geq 1$, le produit $C_u\times C_v$ soit encore de la forme C_w. Lorsque u et v sont premiers entre eux, c'est le cas d'après le lemme chinois. Montrons la réciproque.

Soit par l'absurde p un premier divisant u et v. Alors C_u et C_v ont tous deux un sous-groupe d'ordre p (prendre les multiples de $\frac{u}{p}$ et $\frac{v}{p}$), donc le groupe $C_p \times C_p$ sera cyclique comme sous-groupe d'un groupe cyclique. Mais cela est impossible car les éléments de $C_p \times C_p$ sont tous d'ordre au plus p (raisonner sur chaque coordonnée) tandis que la cyclicité de $C_p \times C_p$ lui impose d'avoir un élément d'ordre $2p$, d'où la contradiction.

Finalement, $G \times H$ est cyclique ssi G et H sont cycliques d'ordres étrangers.

Exercice 2.

Un morphisme de G vers $\mathbf{C}^*$ est en particulier une application de G vers $\mathbf{C}^*$, qui peut alors très bien être vue (par corestriction) comme une application de G vers $\mathbf{C}$, ce que l'on voulait.

Soit par l'absurde une partie de $\mathrm{Hom}\,(G, \mathbf{C}^*)$ qui est liée dans le $\mathbf{C}$-espace vectoriel $\mathbf{C}^G$. Par définition de la liaison, cette partie contient une sous-partie liée *finie* ; l'ensemble $\left\{ \begin{array}{c|cc} & A \subset \mathrm{Hom}\,(G, \mathbf{C}^*) & \\ |A| & ; & A \text{ liée dans } \mathbf{C}^G \\ & & A \text{ finie} \end{array} \right\}$ est alors non vide, donc admet un minumum. Notons n ce dernier. Soient alors $\varphi_1, \varphi_2, ..., \varphi_n \in \mathrm{Hom}\,(G, \mathbf{C}^*)$ qui sont liés. Soit $\overrightarrow{\lambda} \in \mathbf{C}^n$ non nul tel que $\sum_{i=1}^n \lambda_i \varphi_i = 0$. Alors, pour tous x, y dans G, on a

$$0 = \left[\sum_i \lambda_i \varphi_i\right](xy) = \left[\sum_i \lambda_i \varphi_i(x)\, \varphi_i\right](y),$$

d'où pour tout indice j l'égalité des applications (à $x \in G$ fixé)

$$\sum_i \lambda_i \left(\varphi_i(x) - \varphi_j(x)\right) \varphi_i = \underbrace{\sum_i \lambda_i \varphi_i(x)\, \varphi_i}_{\substack{=0 \text{ par ce qui précède} \\ \text{à } x \text{ fixé et à } y \text{ quantifié}}} - \varphi_j(x) \underbrace{\sum_i \lambda_i \varphi_i}_{\substack{=0 \text{ par hypothèse} \\ \text{de liaison}}} = 0 - 0 = 0.$$

Par minimalité de n (remarquer qu'on a tué l'un des scalaires devant les φ_i), on doit avoir pour tous i, j

$$\lambda_i \left(\varphi_i(x) - \varphi_j(x)\right) = 0.$$

En particulier, pour un i tel que $\lambda_i \neq 0$ et pour un $j \neq i$ (possible si $n \geq 2$), on obtient $\varphi_i(x) - \varphi_j(x) = 0$, et ce pour tout x de G, *i. e.* $\varphi_i = \varphi_j$, *absurde* car les φ_i sont distintcs.

Pour $n = 1$, s'il y a un $\lambda \in K$ tel que $\lambda\varphi = 0$, évaluer φ sur le neutre du groupe renvoit le neutre 1 de K^*, d'où $\lambda = 0$, *CQFD*.

Pour $n = 0$, la liberté devient tautologique (la famille vide est libre).

Problème. Soient p un premier et u un naturel.

1.

(a) La partie $K \subset \mathbf{F}_{p^u}$ est finie, donc le corps K est finie et le cours s'applique. Noter la non-nullité de l'exposant v car un corps contient toujours au moins deux éléments.

(b) Le sous-corps $K \subset \mathbf{F}_{p^u}$ en est un sous-groupe additif, donc un résultat de Lagrange s'applique : $|K|$ divise $|\mathbf{F}_{p^u}|$, *i. e.* $q^v \mid p^u$; puisque v est non nul, cela force $q = p$.

(c) Voyons $\mathbf{F}_{p^u}$ comme un K-espace-vectoriel et notons $d := \dim_K \mathbf{F}_{p^u}$. On a alors un isomorphisme $\mathbf{F}_{p^u} \overset{\text{e. v.}}{\simeq} K^d$, d'où en prenant les cardinaux l'égalité $p^u = (p^v)^d$, *i. e.* $u = vd$ (prendre la valuation p-adique), ce qui conclut.

2.

(a) Soient a et b dans $\mathbf{N}^*$.

Si $a = b$, il n'y a rien à faire. On suppose donc $a > b$. On effectue alors la division euclidienne de a par b ($a = bq + r$), ce qui permet d'écrire

$$X^a - 1 = X^{bq}X^r - 1 = X^{bq}X^r - X^r + X^r - 1 = X^r\left(X^{bq} - 1\right) + (X^r - 1) = X^r A\left(X^b - 1\right) + (X^r - 1)$$

(où A est un polynôme *non fractionnaire*), ce qui montre que le reste de la division euclidienne de $X^a - 1$ par $X^b - 1$ est $X^r - 1$. Les termes successifs de l'algorithme d'Euclide "passent" donc à la puissance X et, en réitérant le procédé, on trouve que le dernier reste non nul est bien $X^{a \wedge b} - 1$.

On en déduit les équivalences

$$\begin{aligned} & X^a - 1 \mid X^b - 1 \\ \iff \quad & (X^a - 1) \wedge \left(X^b - 1\right) = X^a - 1 \\ \iff \quad & X^{a \wedge b} - 1 = X^a - 1 \\ \iff \quad & a \wedge b = b \\ \iff \quad & a \mid b, \text{ ce qui conclut.} \end{aligned}$$

(b) Soit λ dans le groupe multiplicatif $\mathbf{F}_{p^d}^*$. Il est envoyé sur 1 au bout de $\left|\mathbf{F}_{p^d}^*\right| = p^d - 1$ itérations, ce qui s'écrit aussi $\lambda^{p^d-1} = 1$, *i. e.* $\lambda^{p^d} = \lambda$, ou encore "λ est racine du polynôme $X^{p^d} - X$ de $\mathbf{F}_{p^d}[X]$". En rajoutant la racine triviale nulle, on a trouvé p^d racines *distinctes* pour le polynôme $X^{p^d} - X$ qui est de degré p^d, d'où la factorisation annoncée (à un scalaire multiplicatif près que l'on voit tout de suite valoir 1 en regardant le coefficient dominant).

L'ensemble K étant l'ensemble des racines de $X^{p^d} - X$ que l'on vient de prouver simplement scindé, son cardinal vaut $\deg\left(X^{p^d} - X\right) = p^d$.

(c) Il est trivial que 0 et 1 sont dans K. Soient a et b dans K.

La stabilité par produit est immédiate : on a $(ab)^{p^d} = a^{p^d} b^{p^d} = ab$.

Pour la somme, on raisonne comme dans le cours où l'on montrait que le Frobenius était un morphisme additif : écrire $(a+b)^{p^d} = ((a+b)^p)^{p^{d-1}} = (a+b)^{p^{d-1}} = \cdots = (a+b)^{p^0} = a + b$.

Lorsque p est impair on aura $(-a)^{p^d} = -a^{p^d} = -a$ et lorsque $p = 2$ on aura $(-a)^{p^d} = a^{p^d} = a = -a$ (puisque $-1 = 1$), d'où la stabilité par opposition.

Enfin, si a est non nul, on a alors $\left(\frac{1}{a}\right)^{p^d} = \frac{1}{a^{p^d}} = \frac{1}{a}$, d'où la stabilité par inversion.