Université Pierre et Marie Curie
Master de Mathématiques
Professeur: J. Oesterlé

Année 2013-2014
MM002 Algèbre et théorie de Galois

E. Lepage

Feuille 1 - Solutions

Solution 1 On a $(x_1x_2\dots x_s) = (x_1x_2)(x_2x_3)\dots(x_{s-1}x_s)$. La signature d'un s-cycle est donc $(-1)^{s-1}$. Si σ est le produit de r cycles de supports disjoints de longueur respective $(s_i)_{1\leq i\leq r}$, on a $\sum_{i=1}^{r} s_i = n$, et la signature de σ est

$$\prod_{i=1}^{r}(-1)^{s_i-1} = (-1)^{\sum_{i=1}^{r} s_i - r} = (-1)^{n-r}.$$

Solution 2

a)

	Id	(12)	(23)	(13)	(123)	(132)
Id	Id	(12)	(23)	(13)	(123)	(132)
(12)	(12)	Id	(123)	(132)	(23)	(13)
(23)	(23)	(132)	Id	(123)	(13)	(12)
(13)	(13)	(123)	(132)	Id	(12)	(23)
(123)	(123)	(13)	(12)	(23)	(132)	Id
(132)	(132)	(23)	(13)	(12)	Id	(123)

b) Le groupe $\mathfrak{S}_3$ a trois classes de conjugaison. La première est $\{Id\}$. La deuxième est formée des trois transpositions (d'ordre 2) (12), (13) et (23). La troisième est formée des deux 3-cycles (d'ordre 3) (123) et (132).

Il y a cinq classes de conjugaison dans Le groupe $\mathfrak{S}_4$. La première est $\{Id\}$. La deuxième est formée des six transpositions (d'ordre 2) (12), (13), (14), (23), (24) et (34). La troisième est formée des huit 3-cycles (d'ordre 3) (123), (132), (124), (142), (134), (143), (234) et (243). La quatrième est formée des six 4-cycles (d'ordre 4) (1234), (1243), (1324), (1342), (1423) et (1432). Enfin la cinquième est formée des trois produits de deux transpositions à supports disjoints (d'ordre 2) (12)(34), (13)(24) et (14)(23).

c) Le groupe $\mathfrak{S}_3$ a 6 sous-groupes : $\{Id\}$, $\mathfrak{A}_3 = \{Id, (123), (132)\}$ et $\mathfrak{S}_3$ sont distingués, $\{Id, (12)\}$, $\{Id, (13)\}$ et $\{Id, (23)\}$ ne le sont pas.

Le groupe $\mathfrak{A}_4$ a 10 sous-groupes : $\{Id\}$, le groupe de Kein

$$\mathfrak{V}_4 = \{Id, (12)(34), (13)(24), (14)(23)\}$$

et $\mathfrak{A}_4$ sont distingués, $\{Id, (12)(34)\}$, $\{Id, (13)(24)\}$, $\{Id, (14)(23)\}$, ainsi que $\{Id, (123), (132)\}$, $\{Id, (124), (142)\}$, $\{Id, (134), (143)\}$ et $\{Id, (234), (243)\}$ ne le sont pas.

Solution 3

a) On a $(x_1x_2\dots x_{k-1}x_k) = (1x_1)(1x_k)(1x_{k-1})\dots(1x_2)(1x_1)$ si 1 ne fait pas partie des x_i et $(1x_2\dots x_{k-1}x_k) = (1x_k)(1x_{k-1})\dots(1x_2)$, donc les transpositions données engendrent tous les cycles, et $\mathfrak{S}_n$ tout entier. Si on oublie la transposition $(1i)$, on ne peut obtenir que des permutations qui laissent i fixe, le groupe engendré n'est donc pas $\mathfrak{S}_n$ tout entier.

b) On a $(1i) = (12)(23)\dots((i-2)(i-1))((i-1)i)((i-2)(i-1))\dots(23)(12)$ donc les $(1i)$ sont dans le groupe engendré. Or on a vu à la question précédente que les $(1i)$ engendraient $\mathfrak{S}_n$. Donc les $(i(i+1))$ engendrent $\mathfrak{S}_n$. Si on omet la transposition $(i(i+1))$, toute permutation du groupe engendré laisse stable l'ensemble $\{1\dots i\}$, ce ne peut donc pas être $\mathfrak{S}_n$ entier.

c) Si on pose $\sigma = (12\dots n)$ et $\tau = (12)$, on a $(i(i+1)) = \sigma^{i-1}\tau\sigma^{1-i}$. D'après la question précédente, le groupe engendré est $\mathfrak{S}_n$. La minimalité est ici évidente.

d) Notons $\tau = (x_1x_2)$ la transposition et posons $y_1 = x_1$. Le n-cycle peut être noté $\sigma = (y_1y_2\dots y_n)$. Il existe un $k \in [2,n]$ tel que $y_k = x_2$. Puisque n est premier, la permutation $\sigma' = \sigma^{k-1}$ est un n-cycle et on peut écrire $\sigma' = (x_1x_2\dots x_n)$. L'application $x : i \mapsto x_i$ est une permutation de $[1,n]$. D'après la question précédente le groupe G' engendré par $(12\dots n)$ et (12) est $\mathfrak{S}_n$. Il en est donc de même du groupe $xG'x^{-1}$ qui est engendré par τ et σ'.

Solution 4

a) Le groupe alterné $\mathfrak{A}_n$ est, par définition, engendré par les produits de deux transpositions. Il y a trois cas possibles :

1. Les deux transpositions sont égales : $(xy)(xy) = Id$.
2. Les supports des deux transpositions ont un élément commun : $(xy)(xz) = (xzy)$.
3. Les supports des deux transpositions sont disjoints : $(xy)(zt) = (xzt)(xyt)$, comme on l'a vu à l'exercice précédent.

Dans tous les cas, un produit de deux transpositions appartient au groupe engendré par les 3-cycles, d'où le résultat.

b) Soit H un sous-groupe de $\mathfrak{S}_n$ d'ordre $n!/2$, c'est-à-dire d'indice 2. Le sous-groupe H est distingué dans $\mathfrak{S}_n$ et $\mathfrak{S}_n/H \simeq \{\pm 1\}$. Si H contenait une transposition, il les contiendrait toutes puisqu'elles sont conjuguées entre elles. Comme les transpositions engendrent $\mathfrak{S}_n$, on aurait $H = \mathfrak{S}_n$, une contradiction. On a donc montré que toutes les transpositions ont pour image -1 dans G/H. Les produits d'un nombre pair de transpositions ont pour image 1 et sont donc dans H. On en déduit $\mathfrak{A}_n \subset H$ et $\mathfrak{A}_n = H$.

Solution 5

a) On a

$$(25)(56)(13254) = (1354)(26)$$

et

$$(123)(124) = (13)(24).$$

b) On trouve

$$(19)(28)(37)(46).$$

c) On a

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 7 & 8 & 3 & 2 & 1 & 9 & 4 & 6 \end{pmatrix} = (152796)(384)$$

Solution 6

a) Pour toute permutation (paire) différente de Id, notons $m(\sigma)$ le plus grand entier m tel que $\sigma(m) = k \neq m$. Remarquons que $k < m$. Montrons par récurrence sur $m(\sigma)$ que σ s'écrit comme produit de $\sigma_i = (12i)$. Si $m(\sigma) \leq 2$, comme σ est pair, σ est en fait Id. Supposons donc $m = m(\sigma) > 2$. On pose

$$\tau = \begin{cases} (1m2)(12k)\sigma & \text{si } k = \sigma(m) > 2, \\ (12m)\sigma & \text{si } k = 2, \\ (1m2)\sigma & \text{si } k = 1. \end{cases}$$

Dans tous les cas, on a $\tau(m) = m$ et $\tau = Id$ ou $m(\tau) < m(\sigma)$. D'après l'hypothèse de récurrence, τ appartient au groupe engendré par les $(12i)$. Il en est donc de même de σ. Remarquons que ceci fournit une autre preuve de la première question de l'exercice précédent.

b) On a $(124) = (123)(243)$, puis

$$(12(i+2)) = (i(i+2)(i+1))(12i)(i(i+1)(i+2))$$

pour $i \geq 3$, donc les $(12i)$ appartiennent au groupe engendré, qui est $\mathfrak{A}_n$ d'après la question précédente.

c) Si dans le premier système générateur on oublie le 3-cycle $(12i)$, le groupe engendré ne peut obtenir que des permutations qui laissent i fixe, et ne peut donc être $\mathfrak{A}_n$ tout entier. Par contre, la relation

$$(234) = (345)(132)(354)(123)$$

montre que l'on peut omettre (234) du second système générateur si $n \geq 5$.

Solution 7 Le noyau de l'action de G sur X est un sous-groupe distingué H de G. Puisque G est simple, on a $H = G$ ou $H = \{e\}$. Si $H = G$, G agit trivialement sur X. Les orbites ont un seul élément et l'action ne peut être transitive puisque $|X| > 1$. On a donc $H = \{e\}$, c'est-à-dire que l'action est fidèle.

Solution 8

a) On a vu que si $\sigma = (x_1 \dots x_n)$ est un n-cycle et τ une permutation, $\tau\sigma\tau^{-1} = (\tau(x_1) \dots \tau(x_n))$ est aussi un n-cycle. Dire que σ et τ commutent, c'est dire que ce cycle est en fait σ. Ceci signifie que les éléments $(\tau(x_1), \dots, \tau(x_n))$ sont les éléments $(x_1, \dots, x_n)$ pris dans le même ordre, mais peut-être non pas à partir de l'élément numéro 1, mais à partir du numéro k, c'est-à-dire que $\tau = \sigma^k$.

b) Dans le cas général, écrivons sur une ligne les cycles de σ, y compris les k_1 qui sont de longueur 1. Pour que $\tau\sigma\tau^{-1} = \sigma$ il faut que τ permute les supports des cycles de σ. Comme on ne peut permuter que les cycles de même longueur, il y a $k_i!$ choix possibles pour les cycles de longueur i. Une fois la correspondance entre les cycles choisie, il y a i choix possibles pour chaque cycle de longueur i, donc i^{k_i} choix pour l'ensemble des cycles de longueur i. La formule

$$|C_{\mathfrak{S}_n}(\sigma)| = \prod_{i=1}^{n} k_i! i^{k_i}.$$

en découle.

Plus formellement, considérons sur $Y := \{1, \cdots, n\}$ la relation d'équivalence définie par $x \sim y$ si et seulement si il existe $k \in \mathbb{Z}$ tel que $x = \sigma^k(y)$ (les classes d'équivalence sont les orbites pour l'action de $\langle\sigma\rangle$) et considérons $X := Y/\sim$.

Soit $\tau \in C_{\mathfrak{S}_n}(\sigma)$. Si $x \sim y$, alors $\tau(x) \sim \tau(y)$ (en effet si $x = \sigma^k(y)$, $\tau(x) = \tau\sigma^k(y) = \sigma^k(\tau(y))$ car σ et τ commute). On peut donc définir $\bar{\tau} : X \to X$ par $\bar{\tau}(\bar{x}) = \overline{\tau(x)}$. On obtient ainsi un morphisme de groupe $\varphi : C_{\mathfrak{S}_n}(\sigma) \to \mathfrak{S}(X)$ défini par $\varphi(\tau) = \bar{\tau}$.

De plus si Z est une classe d'équivalence de $(Y, \sim)$, $\tau(Z)$ est une classe d'équivalence de même cardinal puisque τ est bijective. En notant, pour tout entier i, $X_i \subset X$ l'ensemble des classes d'équivalence de cardinal i, on a donc $\bar{\tau}(X_i) = X_i$, et donc l'image de φ est inclue dans $\prod_i \mathfrak{S}(X_i)$.

Choisissons arbitrairement un représentant $s(\bar{x})$ de chaque classe $\bar{x} \in X$ (i.e. , s est une section de la projection $X \to Y/\sim$. Alors tout élément x de Y s'écrit de façon unique $x = \sigma^k(x)(s(\bar{x}))$ avec $k(x) \in \mathbb{Z}/i\mathbb{Z}$ où i est tel que $\bar{x} \in X_i$. Soit $t = (t_i)_i \in \prod_i \mathfrak{S}(X_i)$, et définissons $\tau \in \mathfrak{S}_n$ par $\tau(x) = \sigma^k(x)(s(t_i(\bar{x})))$. Alors, comme $\overline{\sigma(x)} = \bar{x}$ et $k(\sigma(x)) = k(x) + 1$, on obtient $\tau\sigma(x) = \sigma^{k(x)+1}(s(t_i(\bar{x}))) = \sigma\tau(x)$: donc $\tau \in C_{\mathfrak{S}_n}$ et $\varphi(\tau) = t$, donc $\varphi : C_{\mathfrak{S}_n} \to \prod_i \mathfrak{S}(X_i)$ est surjective (plus précisément, l'application $t \mapsto \tau$ ainsi définie est un morphisme de groupe définissons une section de φ ; $C_{\mathfrak{S}_n}$ est donc isomorphe à un produit semi-direct de $\prod_i \mathfrak{S}(X_i)$ par $\mathrm{Ker}(\varphi)$.

Etudions maintenant $\mathrm{Ker}(\varphi)$. Soit $\tau \in \mathrm{Ker}(\varphi)$, alors pour toute classe d'équivalence $Z \in X_i$, $\tau(Z) = Z$ d'où par restriction un élément $\tau_Z \in \mathfrak{S}(Z)$. De plus comme σ et τ commutent, leurs restrictions σ_Z et τ_Z commutent aussi. Or σ_Z est un i-cycle, donc la question 1 nous dit que $\tau_Z \in \langle\sigma_Z\rangle \simeq \mathbb{Z}/i\mathbb{Z}$. On en déduit que $\mathrm{Ker}(\varphi)$ est isomorphe à $\prod_{Z\in X}\langle\sigma_Z\rangle \simeq \prod_i (\mathbb{Z}/i\mathbb{Z})_i^k$ et est donc de cardinal $\prod_i i^{k_i}$.

Le cardinal de $C_{\mathfrak{S}_n}$ est le produit des cardinaux de $\prod_i \mathfrak{S}(X_i)$ et de $\mathrm{Ker}(\varphi)$, qui est donc $\prod_i i^{k_i} k_i!$.

c) Le cardinal de l'orbite d'un élément x sous l'action d'un groupe G est l'indice du stabilisateur de x. Dans le cas de l'action par conjugaison, le cardinal de la classe de conjugaison de x dans G est l'indice dans G du centralisateur de x.

Notons X la classe de conjugaison de σ dans $\mathfrak{S}_n$ et $Y \subset X$ sa classe dans $\mathfrak{A}_n$. On vient de voir que $|X| = \frac{n!}{|C_{\mathfrak{S}_n}(\sigma)|}$ et $|Y| = \frac{n!}{2|C_{\mathfrak{A}_n}(\sigma)|}$.

- Dans le premier cas, la relation $C_{\mathfrak{A}_n}(\sigma) = C_{\mathfrak{S}_n}(\sigma)$ est évidente. On en déduit $|X| = 2|Y|$. Soit $\sigma' = \tau\sigma\tau^{-1} \in \mathfrak{A}_n$ un élément de X qui n'est pas dans Y. Il est évident que τ est impaire et que $C_{\mathfrak{A}_n}(\sigma') = \tau C_{\mathfrak{A}_n}(\sigma)\tau^{-1} = \tau C_{\mathfrak{S}_n}(\sigma)\tau^{-1} = C_{\mathfrak{S}_n}(\sigma')$. La classe de conjugaison Y' de σ' dans $\mathfrak{A}_n$ a donc même cardinal que Y, c'est le complémentaire de Y dans X.

- Dans le deuxième cas, soit $\tau \in C_{\mathfrak{S}_n}(\sigma)$ une permutation impaire. Soit $x = g\sigma g^{-1}$ un élément de X. Si la permutation g est paire, alors $x \in Y$. Si elle est impaire, $x = (g\tau)\sigma(g\tau)^{-1}$ est encore dans Y puisque $g\tau$ est paire. On a donc $Y = X$ et la formule ci-dessus montre que l'indice de $C_{\mathfrak{A}_n}(\sigma)$ dans $C_{\mathfrak{S}_n}(\sigma)$ est 2.

d) Si σ a un cycle τ de longueur paire, τ lui-même est une permutation impaire qui commute avec σ. On est donc alors dans le deuxième cas. De même, si $(x_1x_2\ldots x_i)$ et $(y_1y_2\ldots y_i)$ sont deux cycles de même longueur impaire i, le produit $\tau = (x_1y_1)\ldots(x_iy_i)$ est une permutation impaire qui commute avec σ et on est encore dans le deuxième cas. Reste le cas où σ est produit de cycles de longueurs impaires distinctes, c'est-à-dire $k_i = 0$ pour i pair et $k_i \leq 1$ pour i

impair. Dans ce cas le cardinal $|C_{\mathfrak{S}_n}| = \prod_i (k_i!) i^{k_i}$ est impair, donc $C_{\mathfrak{S}_n}(\sigma) \subset \mathfrak{A}_n$ et on est dans le premier cas.

e) Comme $\mathfrak{A}_3$ est commutatif d'ordre 3, il a trois classes de conjugaison (une est une classe de $\mathfrak{S}_3$, les autres sont les deux moitiés de la classe paire de $\mathfrak{S}_3$).

Les classes $\{Id\}$ et $\{(12)(34), (13)(24), (14)(23)\}$ de $\mathfrak{S}_4$ restent des classes de $\mathfrak{A}_4$. Par contre la classe de (123), qui a 8 éléments, se décompose en deux classes dans $\mathfrak{A}_4$: $\{(123),(134),(142),(243)\}$ et $\{(124), (132), (143), (234)\}$.

Solution 9

a) Si $(abcd\dots)$ est un cycle de σ et $\tau = (abc)$, alors

$$\sigma\tau^{-1}\sigma^{-1} = (\sigma(c)\sigma(b)\sigma(a)) = (dcb)$$

et $\tau\sigma\tau^{-1}\sigma^{-1} = (dab)$ est un 3-cycle.

b) Si $(abc)(de)$ apparaît dans σ et $\tau = (ab)(de)$, alors

$$\sigma\tau^{-1}\sigma^{-1} = (\sigma(a)\sigma(b))(\sigma(d)\sigma(e)) = (bc)(de)$$

et $\tau\sigma\tau^{-1}\sigma^{-1} = (abc)$ est un 3-cycle.

Si $(abc)(d)(e)$ apparaît dans σ et $\tau = (ade)$, alors

$$\sigma\tau^{-1}\sigma^{-1} = (\sigma(e)\sigma(d)\sigma(a)) = (edb)$$

et $\tau\sigma\tau^{-1}\sigma^{-1} = (adb)$ est un 3-cycle.

Si $(ab)(c)$ apparaît dans σ et $\tau = (abc)$, alors

$$\sigma\tau^{-1}\sigma^{-1} = (\sigma(c)\sigma(b)\sigma(a)) = (cab)$$

et $\tau\sigma\tau^{-1}\sigma^{-1} = (acb)$ est un 3-cycle.

c) Si $(abc)(def)$ apparaît dans σ et $\tau = (abd)$, alors

$$\sigma\tau^{-1}\sigma^{-1} = (\sigma(d)\sigma(b)\sigma(a)) = (ecb)$$

et $\tau\sigma\tau^{-1}\sigma^{-1} = (abfde)$ est un 5-cycle.

d) Si $(ab)(cd)(ef)$ apparaît dans σ et $\tau = (ace)$, alors

$$\sigma\tau^{-1}\sigma^{-1} = (\sigma(e)\sigma(c)\sigma(a)) = (fdb)$$

et $\tau\sigma\tau^{-1}\sigma^{-1} = (ace)(fdb)$ est un produit de deux 3-cycles disjoints.

e) Soit G un sous-groupe distingué de $\mathfrak{A}_n$, avec $n \geq 5$, et $\sigma \neq Id$ un élément non neutre de G. Si σ est dans un des cas couverts par les questions a) et b), le groupe G contient un 3-cycle. Le c) ramène au a) et le d) ramène au c). Restent les cas où σ a un seul 3-cycle et au plus un point fixe ou deux 2-cycles et pas de point fixe, qui ne peuvent arriver que pour $n \leq 4$. Dans tous les cas G contient un 3-cycle, donc tous les 3-cycles puisqu'ils sont conjugués entre eux dans $\mathfrak{A}_n$ et $G = \mathfrak{A}_n$ puisque les 3-cycles engendrent $\mathfrak{A}_n$. Donc $\mathfrak{A}_n$ est simple pour $n \geq 5$.

Solution 10 Le groupe $\mathfrak{S}_n$ agit par translation à gauche sur l'ensemble quotient $X = \mathfrak{S}_n/H$ qui a n éléments. On en déduit un homorphisme ρ de $\mathfrak{S}_n$ dans $\mathfrak{S}_X \simeq \mathfrak{S}_n$. Le noyau K de ce morphisme est un sous-groupe distingué de

$\mathfrak{S}_n$, c'est donc $\mathfrak{S}_n$, $\mathfrak{A}_n$ ou $\{Id\}$, sauf dans le cas $n = 4$ où la possibilité supplémentaire $\mathfrak{V}_4$ existe. L'image $\rho(\mathfrak{S}_n) \simeq \mathfrak{S}_n/K$ a donc pour cardinal 1, 2, $n!$ (ou 6 dans le cas $n = 4$). Comme l'orbite de H est X tout entier, le cardinal de l'image est un multiple de n. La seule possibilité est donc $K = \{Id\}$ et ρ est un isomorphisme. Le stabilisateur de H dans l'action est H lui-même, donc son image par ρ est le stabilisateur d'un point dans $\mathfrak{S}_X$, lequel est isomorphe à $\mathfrak{S}_{n-1}$. Attention, on n'a pas prouvé que H était le stabilisateur d'un point dans $\mathfrak{S}_n$; il existe d'ailleurs un contre-exemple pour $n = 6$.

Solution 11 Le groupe G agit par translation à gauche sur G/H. Le stabilisateur de H est H lui-même, et le stabilisateur de xH est xHx^{-1}. Le noyau de cette action est donc $K = \cap_{x\in G} xHx^{-1}$. On a donc un homomorphisme injectif de G/K dans $\mathfrak{S}(G/H) \simeq \mathfrak{S}_p$. L'indice de K dans G est un diviseur commun à n et $p!$, il vaut donc 1 ou p. Comme K est contenu dans H, ce n'est pas 1. On en conclut que l'indice vaut p, donc $K = H$ et H, comme K, est distingué.

Solution 12 Notons φ l'application composée, qui est un morphisme de groupes. Il est clair que son noyau est $\ker\varphi = H\cap K$, qui est un sous-groupe distingué de K. On a donc bien $\mathrm{Im}\varphi \simeq K/(H \cap K)$.

Solution 13 Notons P_1, P_2, P_3 et P_4 les sommets du tétraèdre. Comme les trois vecteurs $\overrightarrow{OP_1}$, $\overrightarrow{OP_2}$ et $\overrightarrow{OP_3}$ sont indépendants, l'action de $G(T)$ est fidèle. On a donc bien une injection de $G(T)$ dans $\mathfrak{S}_4$. Montrons qu'elle est surjective. En effet, la réflexion orthogonale par rapport au plan engendré par $\overrightarrow{OP_3}$ et $\overrightarrow{OP_4}$ appartient à $G(T)$ et échange P_1 et P_2. L'image de $G(T)$ contient donc la transposition (12), et de même toutes les transpositions, donc $\mathfrak{S}_4$ tout entier. Pour montrer que l'image de $G^+(T)$ est $\mathfrak{A}_4$, on peut remarquer que ce doit être un sous-groupe d'indice 2 de $\mathfrak{S}_4$. On peut aussi expliciter les rotations qui interviennent : (123) correspond à la rotation d'un tiers de tour d'axe $\overrightarrow{OP_4}$ et (12)(34) au demi-tour dont l'axe joint les milieux des segmentsP_1P_2 et P_3P_4.

Solution 14

a) Notons D_1, D_2, D_3 et D_4 les quatre diagonales de C. Un endomorphisme qui fixe D_i a le vecteur directeur de D_i comme vecteur propre. Comme trois quelconques de ces vecteurs sont indépendants, un tel endomorphisme est un scalaire. S'il est orthogonal, c'est ±1, et -1 n'est pas une rotation de $\mathbb{R}^3$. L'action de $G^+(C)$ sur les diagonales est donc fidèle, d'où une injection $\beta : G^+(C) \to \mathfrak{S}_4$. Une rotation d'un quart de tour dans le plan engendré par D_3 et D_4 échange D_1 et D_2. L'image de β contient donc la transposition (12) et les autres transpositions. Donc β est surjective. Le morphisme naturel $\{\pm1\} \times G^+(C) \to G(C)$ est un isomorphisme (la réciproque est $u \mapsto (\det u, \det u.u)$), ce qui achève la démonstration.

b) On obtient les matrices des éléments de $G(C)$ en parcourant les matrices de permutation et en changeant arbitrairement les signes des coefficients non nuls.

$$\begin{pmatrix} \pm1 & 0 & 0 \\ 0 & \pm1 & 0 \\ 0 & 0 & \pm1 \end{pmatrix}, \begin{pmatrix} 0 & \pm1 & 0 \\ 0 & 0 & \pm1 \\ \pm1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & \pm1 \\ \pm1 & 0 & 0 \\ 0 & \pm1 & 0 \end{pmatrix},$$

$$\begin{pmatrix} \pm1 & 0 & 0 \\ 0 & 0 & \pm1 \\ 0 & \pm1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & \pm1 \\ 0 & \pm1 & 0 \\ \pm1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \pm1 & 0 \\ \pm1 & 0 & 0 \\ 0 & 0 & \pm1 \end{pmatrix}.$$

On obtient ainsi une suite exacte :

$$1 \longrightarrow \{\pm 1\}^3 \longrightarrow G(C) \longrightarrow \mathfrak{S}_3 \longrightarrow 1$$

liée à l'action sur les trois axes (de coordonnées) passant par les milieux des faces du cube.

Solution 15 La situation est exactement la même que dans la deuxième partie de l'exercice précédent. Le groupe $G(C(n))$ agit sur l'ensemble des n axes de coordonnées. Le noyau de cette action est formé des applications orthogonales qui ont chaque élément de la base canonique comme vecteur propre. La valeur propre étant ± 1, le noyau est isomorphe à $\{\pm 1\}^n$. On a donc encore la suite exacte :

$$1 \longrightarrow \{\pm 1\}^n \longrightarrow G(C(n)) \longrightarrow \mathfrak{S}_n \longrightarrow 1$$

La surjectivité vient de ce que les matrices de permutation (qui forment un sous-groupe isomorphe à $\mathfrak{S}_n$) sont bien dans $G(C(n))$. Tout élément de $G(C(n))$ s'écrit de manière unique

$$u = M_\sigma.\mathrm{diag}(\varepsilon_1, \ldots, \varepsilon_n),$$

avec $\sigma \in \mathfrak{S}_n$ et $\varepsilon_i \in \{\pm 1\}$. Si $v = M_\tau.\mathrm{diag}(\eta_1, \ldots, \eta_n)$ est un autre élément de $G(C(n))$, on a

$$u.v = M_{\sigma\tau}.\mathrm{diag}(\varepsilon_{\tau(1)}\eta_1, \ldots, \varepsilon_{\tau(n)}\eta_n).$$

Solution 16

a) Une rotation non triviale $\rho \in G \setminus \{Id\}$ a un axe unique, et cet axe porte deux vecteurs unitaires. La première projection $Z \to G \setminus \{Id\}$ est donc surjective et chaque élément de $G \setminus \{Id\}$ a deux antécédents dans Z. On a donc bien $|Z| = 2|G \setminus \{Id\}| = 2(n-1)$.

b) Soit $x \in P$, $\rho \in G \setminus \{Id\}$ tel que $\rho(x) = x$, et $\sigma \in G$. En posant $y = \sigma(x)$ et $\tau = \sigma\rho\sigma^{-1}$, on a bien $|y| = 1$, $\tau \in G \setminus \{Id\}$ et $\tau(y) = \sigma(x) = y$, donc (τ, y) appartient à Z et y appartient à P.

c) L'ensemble des rotations qui ont x comme pôle est isomorphe au groupe $O^+(2)$ des rotations du plan perpendiculaire à x. Il est isomorphe à $\mathbb{R}/\mathbb{Z}$ et ses seuls sous-groupes finis sont cycliques. Par définition d'un pôle, son stabilisateur n'est pas trivial, donc $n_x > 1$. Le reste des affirmations est vrai pour toute action de groupe.

d) La i-ème orbite a $\frac{n}{n_i}$ éléments, et chacun d'eux a $(n_i - 1)$ antécédents dans Z. On a donc

$$|Z| = \sum_{i=1}^{r}(n_i - 1)\frac{n}{n_i} = n\sum_{i=1}^{r}(1 - \frac{1}{n_i}).$$

e) On a $1 \leq 2 - \frac{2}{n} < 2$ et $1 > 1 - \frac{1}{n_i} \geq \frac{1}{2}$. On en déduit $2 \leq r \leq 3$. Si $r = 2$, l'équation devient $2 = \frac{n}{n_1} + \frac{n}{n_2}$. Comme $\frac{n}{n_i}$ est le cardinal de la i-ème orbite, il y a exactement deux pôles opposés, et $G = G_{x_1}$ est cyclique.

f) L'équation s'écrit maintenant

$$\frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} = 1 + \frac{2}{n}.$$

Si l'on avait $n_1 \geq 3$ ou $n_1 = 2$ et $n_2 \geq 4$ le premier membre serait majoré par 1, une contradiction. Si $n_3 = 2$ l'équation devient $n = 2n_3$. La troisième orbite est formée de deux pôles S et N et G_S est d'indice 2, donc distingué. On en déduit $G_S = G_N$ et N et S sont diamétralement opposés. Les éléments de $G \setminus G_S$ échangent S et N : ce sont donc des demi-tours d'axe perpendiculaire à l'axe SN. Les deux autres orbites sont donc dans ce plan et sont deux $n/2$-gones réguliers.

g) L'équation s'écrit maintenant

$$\frac{1}{n_3} = \frac{1}{6} + \frac{2}{n}$$

d'où immédiatement $n_3 < 6$. En substituant les valeurs de n_3 on trouve :

- Si $n_3 = 3$, $n = 12$, la deuxième orbite est l'ensemble des sommets d'un tétraèdre régulier T (la troisième aussi) et $G = G(T) \simeq \mathfrak{A}_4$.
- Si $n_3 = 4$, $n = 24$, la deuxième orbite est l'ensemble des sommets d'un cube C (la troisième est un octaèdre) et $G = G(C) \simeq \mathfrak{S}_4$.
- Si $n_3 = 5$, $n = 60$, la deuxième orbite est l'ensemble des sommets d'un dodécaèdre régulier D (la troisième est un icosaèdre) et $G = G(D) \simeq \mathfrak{A}_5$. Dans ces trois cas, les axes de la première orbite passent par les milieux des arêtes du polyèdre régulier.

Solution 17

a) On a $(\sigma^a)^k = 1 \Leftrightarrow \sigma^{ak} = 1 \Leftrightarrow n \,|\, ak \Leftrightarrow \frac{ak}{n} \in \mathbb{Z}$. Le plus petit entier $k \geq 1$ qui satisfait cette condition est le dénominateur de $\frac{a}{n}$.

b) L'application

$$\{a \in [1, n];\ \sigma^a \text{ est d'ordre } d\} \to \{b \in [1, d];\ b \text{ est premier avec } d\}$$

qui à a fait correspondre le numérateur b de $\frac{a}{n}$ est une bijection dont la réciproque est $b \mapsto \frac{bn}{d} = b.\frac{n}{d}$. Les deux ensembles ont même cardinal, et $\varphi(d)$ est par définition le cardinal du second.

Solution 18 L'ordre (additif) de l'élément 1 de R est un diviseur de 4 autre que 1.

1) Si c'est 4, les éléments 0, 1, $2 = 1+1$ et $3 = 1+1+1$ de R sont tous distincts. La table d'addition de R est celle de $\mathbb{Z}/4\mathbb{Z}$ et la table de multiplication aussi puisque elle découle de celle d'addition par distributivité. On a donc dans ce cas $R = \mathbb{Z}/4\mathbb{Z}$, $R^\times = \{\pm 1\}$ et $GA_1(R)$ est le groupe diédral à huit éléments D_8.

Dans la suite, l'ordre additif de 1 est 2 et le groupe additif de R est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$. On a $R = \{0, 1, \alpha, \beta = \alpha + 1\}$. Reste la structure multiplicative. A priori α^2 peut valoir 0, 1, α ou β. Toutes les autres valeurs des produits en découlent par associativité et distributivité.

2) Si $\alpha^2 = \alpha$, on a $\alpha\beta = 0$ et $\beta^2 = \beta$. L'anneau R est isomorphe à $\mathbb{F}_2 \times \mathbb{F}_2$ par $\alpha \mapsto (1, 0)$ et $\beta \mapsto (0, 1)$. La seule unité est 1 et le groupe affine est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$. Il agit *librement* sur R, c'est-à-dire que les éléments de $GA_1(R)$ autres que l'identité n'ont aucun point fixe. On en déduit que $GA_1(R)$ s'identifie au groupe de Klein $\mathfrak{V}_4$.

3) Si $\alpha^2 = \beta$, on a $\alpha\beta = 1$ et $\beta^2 = \alpha$. L'anneau R est le corps à quatre éléments $\mathbb{F}_4$. Le groupe des unités $\mathbb{F}_4^*$ est cyclique d'ordre 3 et $GA_1(R)$ est un sous-groupe à 12 éléments de $\mathfrak{S}_4$: c'est $\mathfrak{A}_4$.

4) Si $\alpha^2 = 0$ (respectivement 1), on a $\alpha\beta = \alpha$ (respectivement β) et $\beta^2 = 1$ (respectivement 0). L'application $\varepsilon \mapsto \alpha$ (respectivemet β) induit un isomorphisme de $\mathbb{F}_2[\varepsilon]$ sur R. Le groupe des unités de $\mathbb{F}_2[\varepsilon]$ a deux éléments, 1 et $1+\varepsilon$ et le groupe affine a 8 éléments. C'est donc encore un groupe diédral D_8.

Solution 19

a) Le premier vecteur est non nul, il y a $q^m - 1$ possibilités. Le deuxième n'appartient pas à la droite engendrée par le premier, soit $q^m - q$ possibilités. De façon générale, le i-ème vecteur n'appartient à l'espace de dimension $i-1$ engendré par les $i-1$ précédents. Il y a $q^m - q^{i-1}$ possibilités. On a montré

$$L(m,k,q) = \prod_{i=1}^{k}(q^m - q^{i-1}) = q^{\frac{k(k-1)}{2}} \prod_{i=1}^{k}(q^{m-i+1} - 1).$$

b) La représentation matricielle donne une bijection de $GL_m(\mathbb{F}_q)$ avec l'ensemble des bases de $\mathbb{F}_q^m$. On a donc

$$|GL_m(\mathbb{F}_q)| = L(m,m,q) = q^{\frac{m(m-1)}{2}} \prod_{i=1}^{m}(q^i - 1).$$

c) L'image de 0 est un élément quelconque de $\mathbb{F}_q^m$. On a

$$|GA_m(\mathbb{F}_q)| = q^m |GL_m(\mathbb{F}_q)| = q^{\frac{m(m+1)}{2}} \prod_{i=1}^{m}(q^i - 1).$$

d) Les matrices scalaires forment un sous-groupe de $GL_m(\mathbb{F}_q)$ isomorphe à $\mathbb{F}_q^*$. On a donc

$$|PGL_m(\mathbb{F}_q)| = \frac{|GL_m(\mathbb{F}_q)|}{|\mathbb{F}_q^*|} = q^{\frac{m(m-1)}{2}} \prod_{i=2}^{m}(q^i - 1).$$

e) Le déterminant est un homomorphisme surjectif de $GL_m(\mathbb{F}_q)$ sur $\mathbb{F}_q^*$. Donc

$$|SL_m(\mathbb{F}_q)| = \frac{|GL_m(\mathbb{F}_q)|}{|F_q^*|} = |PGL_m(\mathbb{F}_q)| = q^{\frac{m(m-1)}{2}} \prod_{i=2}^{m}(q^i - 1).$$

f) Notons $X_m(\mathbb{F}_q)$ le groupe des matrices scalaires d'ordre m de déterminant 1. Il est en bijection avec le groupe des solutions dans $\mathbb{F}_q$ de l'équation $x^m = 1$. Comme $\mathbb{F}_q^*$ est cyclique d'ordre q, on a $|X_m(\mathbb{F}_q)| = \text{pgcd}(m, q-1)$ et

$$|PSL_m(\mathbb{F}_q)| = \frac{|SL_m(\mathbb{F}_q)|}{|X_m(\mathbb{F}_q)|} = q^{\frac{m(m-1)}{2}} \frac{\prod_{i=2}^{m}(q^i - 1)}{\text{pgcd}(m, q-1)}.$$

g) Chacun de ces espaces a $|GL_k(\mathbb{F}_q)|$ bases, chacune de ces bases est une k-famille libre de $\mathbb{F}_q^m$. On en déduit

$$EV(k,m,q) = \frac{L(m,k,q)}{|GL_k(\mathbb{F}_q)|} = \frac{\prod_{i=1}^{k}(q^{m-i+1} - 1)}{\prod_{i=1}^{k}(q^i - 1)}$$

et l'expression ci-dessus est bien un entier.

h) Tout espace affine de dimension k est un translaté par un vecteur u de $\mathbb{F}_q^m$ d'un espace vectoriel de dimension k et un seul. Deux translatés du même espace F sont égaux si et seulement si les vecteurs u et v de translation vérifient $u-v \in F$, ce qui, à u fixé, arrive pour q^k valeurs de v. On a donc

$$EA(k,m,q) = \frac{q^m}{q^k} EV(k,m,q) = q^{m-k} \frac{\prod_{i=1}^{k}(q^{m-i+1}-1)}{\prod_{i=1}^{k}(q^i-1)}.$$

b') L'application det : $M_m(\mathbb{R}) \to \mathbb{R}$ est continue, donc $GL_m(\mathbb{R}) = \det^{-1}(\mathbb{R}^*)$ est un ouvert de $M_m(\mathbb{R})$. Sa dimension est donc m^2.

c') Il faut en plus spécifier l'image de 0, à valeur dans $\mathbb{R}^m$, on trouve donc m^2+m paramètres.

d',e') Chaque élément de $PGL_m(\mathbb{R})$ a un représentant unique dont le déterminant est 1 ou -1. On en déduit que $PGL_m(\mathbb{R})$ et $SL_m(\mathbb{R})$ ont même dimension. La fonction det a une différentielle qui ne s'annulle en aucun point de $GL_m(\mathbb{R})$, Donc, d'après le théorème des fonctions implicites appliqué à $\det(A) = 1$, $SL_m(\mathbb{R})$ est une variété de codimension 1 de $M_m(\mathbb{R})$. Sa dimension est m^2-1.

f') Selon que m est impair ou pair, $PSL_m(\mathbb{R})$ est homéomorphe à $SL_m(\mathbb{R})$ ou à $SL_m(\mathbb{R})/\{\pm 1\}$. Dans les deux cas, la dimension est donc encore m^2-1.

g') L'espace des k-familles libres de $\mathbb{R}^m$ est de dimension km (c'est un ouvert de $(\mathbb{R}^m)^k$). Le groupe $GL_k(\mathbb{R})$ est une variété de dimension k^2 qui agit librement sur cet espace. Le quotient a donc pour dimension $km - k^2 = k(m-k)$.

h') En plus d'un espace vectoriel E de dimension k, il faut spécifier un élément de l'espace affine, unique à un élément de E près, donc dépendant de $m-k$ paramètres. On trouve donc $k(m-k) + (m-k) = (k+1)(m-k)$.

Solution 20

a) Le noyau de ρ est le centre de $\mathbb{H}^*$, c'est-à-dire $\mathbb{R}^*$. Comme l'application composée $\det \circ \rho : \mathbb{H}^* \to \{\pm 1\}$ est continue et $\mathbb{H}^*$ est connexe, l'image de ρ est incluse dans $SO(3)$. Soit $\vec{u} = b\vec{i} + c\vec{j} + d\vec{k}$ un vecteur unitaire et $\theta \in \mathbb{R}$. Posons $q = \cos(\theta) + b\sin(\theta)i + c\sin(\theta)j + d\sin(\theta)k$. On vérifie que $\rho(q)$ est la rotation d'angle θ autour de l'axe $\vec{u}$. L'image de ρ est donc $SO(3)$ tout entier.

b) Voici une liste de représentants dans $\mathbb{H}^*$ des éléments de $\rho^{-1}(G^+(C))$:
- $\{1, i, j, k\}$ pour $\mathfrak{V}_4$,
- $\{1 \pm i \pm j \pm k\}$ pour les 3-cycles,
- $\{1 \pm i, 1 \pm j, 1 \pm k\}$ pour les 4-cycles,
- $\{i \pm j, i \pm k, j \pm k\}$ pour les transpositions.

On aurait pu choisir des représentants de norme 1 mais pour les permutations impaires cela aurait nécessité de diviser par $\sqrt{2}$.

c) Les applications $\alpha \mapsto 1 + \alpha^2$ et $\beta \mapsto -\beta^2$ prennent chacune $\frac{p+1}{2}$ valeurs distinctes dans $\mathbb{F}_p$ qui a p éléments. Il y a donc au moins une valeur prise par les deux applications et une solution à l'équation $1 + \alpha^2 = -\beta^2$.

d) La vérification est immédiate. L'unique algèbre de quaternions sur $\mathbb{F}_p$ est (isomorphe à) $M_2(\mathbb{F}_p)$, la conjugaison est le passage à la comatrice, et la norme réduite est le déterminant.

e) Notons G l'image naturelle dans $PGL_2(\mathbb{F}_p)$ des 24 matrices

$$\{1, I, J, K, \frac{1 \pm I \pm J \pm K}{2}, 1 \pm I, 1 \pm J, 1 \pm K, I \pm J, I \pm K, J \pm K\}.$$

L'ensemble G est un sous-groupe de $PGL_2(\mathbb{F}_p)$ isomorphe à $G^+(C) \simeq \mathfrak{S}_4$. La réciproque sera β_p. Le déterminant est 1 pour les 12 premières matrices qui constituent $\beta_p(\mathfrak{A}_4)$ et 2 pour les 12 autres.

f) L'image réciproque de PSL_2 dans GL_2 est formée des matrices dont le déterminant est un carré. On a donc bien $G \subset PSL_2(\mathbb{F}_p) \Leftrightarrow \sqrt{2} \in \mathbb{F}_p \Leftrightarrow p \equiv \pm 1 \pmod 8$.

g) On a vu

$$|PGL_2(\mathbb{F}_5)| = 5.(25-1) = 120$$

et

$$|PSL_2(\mathbb{F}_7)| = 7.\frac{49-1}{\text{pgcd}(2,6)} = 168.$$

Comme $2 \equiv 3^2 \pmod 7$, on a bien $\beta_p(\mathfrak{S}_4) \subset G_p$ et $|X_p| = \frac{|G_p|}{|\beta_p(\mathfrak{S}_4)|} = \frac{|G_p|}{24} = p$. Le noyau K_p de l'action de G_p sur X_p est un sous-groupe distingué de G_p inclus dans $\beta_p(\mathfrak{S}_4)$. Si $p = 7$, comme G_p est simple, on en conclut directement $K_p = \{1\}$. Pour $p = 5$, l'intersection de K_p et $PSL_2(\mathbb{F}_5)$ est triviale. Comme $PSL_2(\mathbb{F}_5)$ est d'indice 2 dans G_p, l'ordre de K_p est au plus 2. Comme il est distingué dans $\beta_5(\mathfrak{S}_4 \simeq \mathfrak{S}_4$, on a encore $K_p = \{1\}$. On a une action fidèle de G_p sur un ensemble à p éléments, c'est-à-dire un plongement de G_p dans $\mathfrak{S}_{X_p} \simeq \mathfrak{S}_p$.

Solution 21 On calcule $|GL_3(\mathbb{F}_2)| = (2^3-1)(2^3-2)(2^3-2^2) = 2^3.7.3 = 168$. Le groupe $GL_3(\mathbb{F}_2)$ agit naturellement sur l'ensemble X des vecteurs non nuls de $\mathbb{F}_2^3$, qui a 8-1 = 7 éléments. Le noyau de cette action est formé des endomorphismes qui laissent fixe chaque vecteur de $\mathbb{F}_2^3$. Il est donc réduit à $\{1\}$ et l'action est fidèle, d'où un plongement de G dans $\mathfrak{S}_X \simeq \mathfrak{S}_7$.

Solution 22 Il est clair que $p(Z)$ est un sous-groupe de X/Y et que $p^{-1}(T)$ est un sous-groupe de X contenant Y. Les deux applications sont donc bien définies. Comme p est surjectif, on a toujours $p(p^{-1}(T)) = T$. Soit Z un sous-groupe de X contenant Y. Montrons que $Z = p^{-1}(p(Z))$. On a toujours $Z \subset p^{-1}(p(Z))$. D'autre part, si $x \in p^{-1}(p(Z))$, alors $p(x) \in p(Z)$, c'est-à-dire qu'il existe $z \in Z$ tel que $p(x) = p(z)$. On a donc $xz^{-1} \in Y \subset Z$. On en déduit $x \in Z$ et $Z = p^{-1}(p(Z))$. Les deux applications sont donc bien des bijections réciproques l'une de l'autre.