Quelques indications pour les questions de Debarre et Laszlo

1. Dénombrement, groupes

(1.1) • Une première réponse : on note x_{2n+1} le nombre de chemins de longueur exactement $2n+1$ sur les arêtes d'un cube joignant deux sommets opposés (il faut remarquer que ce nombre est nécessairement impair...), on a alors $x_{2n+1} = \frac{27}{4}9^{n-1} - \frac{3}{4}$.
En effet, on introduit la matrice d'adjacence A relatif au graphe dont les sommets sont les 8 sommets du cube (couplés de la sorte : $(1,7)$, $(2,8)$, $(3,5)$, $(4,6)$), et dont les arêtes sont les arêtes du cube. On obtient la matrice A suivante :

$$A = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}$$

Si on regarde le nombre de chemins joignant 1 à 7 de longueur exactement $2n+1$, il s'agit du terme de la 1ère colonne et de la 7ème ligne de la matrice A^{2n+1}, qui est donc x_{2n+1} (merci la théorie des graphes et les matrices d'adjacence !).
En observant la tête des différentes puissances de A, on s'aperçoit que la 1ère colonne de A^{2n+1} est
${}^t\begin{pmatrix} 0 & 1+x_{2n+1} & 0 & 1+x_{2n+1} & 1+x_{2n+1} & 0 & x_{2n+1} & 0 \end{pmatrix}$
Le terme x_{2n+3} est donné par le produit de la 7ème ligne de A^2, qui est $\begin{pmatrix} 0 & 2 & 0 & 2 & 2 & 0 & 3 & 0 \end{pmatrix}$, et de la 1ère colonne de A^{2n+1}, ce qui donne $x_{2n+3} = 9\,x_{2n+1} + 6$. On a affaire à une suite arithmético-géométrique ; ainsi, $x_{2n+1} = (6 + \frac{3}{4})9^{n-1} - \frac{3}{4}$.

Donnons quelques puissances de A :

$$A^2 = \begin{pmatrix} 3 & 0 & 2 & 0 & 0 & 2 & 0 & 2 \\ 0 & 3 & 0 & 2 & 2 & 0 & 2 & 0 \\ 2 & 0 & 3 & 0 & 0 & 2 & 0 & 2 \\ 0 & 2 & 0 & 3 & 2 & 0 & 2 & 0 \\ 0 & 2 & 0 & 2 & 3 & 0 & 2 & 0 \\ 2 & 0 & 2 & 0 & 0 & 3 & 0 & 2 \\ 0 & 2 & 0 & 2 & 2 & 0 & 3 & 0 \\ 2 & 0 & 2 & 0 & 0 & 2 & 0 & 3 \end{pmatrix}, \quad A^4 = \begin{pmatrix} 21 & 0 & 20 & 0 & 0 & 20 & 0 & 20 \\ 0 & 21 & 0 & 20 & 20 & 0 & 20 & 0 \\ 20 & 0 & 21 & 0 & 0 & 20 & 0 & 20 \\ 0 & 20 & 0 & 21 & 20 & 0 & 20 & 0 \\ 0 & 20 & 0 & 20 & 21 & 0 & 20 & 0 \\ 20 & 0 & 20 & 0 & 0 & 21 & 0 & 20 \\ 0 & 20 & 0 & 20 & 20 & 0 & 21 & 0 \\ 20 & 0 & 20 & 0 & 0 & 20 & 0 & 21 \end{pmatrix},$$

$$A^5 = \begin{pmatrix} 0 & 61 & 0 & 61 & 61 & 0 & 60 & 0 \\ 61 & 0 & 61 & 0 & 0 & 61 & 0 & 60 \\ 0 & 61 & 0 & 61 & 60 & 0 & 61 & 0 \\ 61 & 0 & 61 & 0 & 0 & 60 & 0 & 61 \\ 61 & 0 & 60 & 0 & 0 & 61 & 0 & 61 \\ 0 & 61 & 0 & 60 & 61 & 0 & 61 & 0 \\ 60 & 0 & 61 & 0 & 0 & 61 & 0 & 61 \\ 0 & 60 & 0 & 61 & 61 & 0 & 61 & 0 \end{pmatrix}, \quad A^7 = \begin{pmatrix} 0 & 547 & 0 & 547 & 547 & 0 & 546 & 0 \\ 547 & 0 & 547 & 0 & 0 & 547 & 0 & 546 \\ 0 & 547 & 0 & 547 & 546 & 0 & 547 & 0 \\ 547 & 0 & 547 & 0 & 0 & 546 & 0 & 547 \\ 547 & 0 & 546 & 0 & 0 & 547 & 0 & 547 \\ 0 & 547 & 0 & 546 & 547 & 0 & 547 & 0 \\ 546 & 0 & 547 & 0 & 0 & 547 & 0 & 547 \\ 0 & 546 & 0 & 547 & 547 & 0 & 547 & 0 \end{pmatrix}.$$

On s'aperçoit que x_2 et x_4 sont bien nuls, et que $x_5 = 60$, $x_7 = 546$, comme le donne la formule de récurrence : $x_5 = 9^{2-1}\frac{27}{4} - \frac{3}{4} = 60$ et $x_7 = 9^{3-1}\frac{27}{4} - \frac{3}{4} = 546$.
• Voici une réponse plus élégante de Meu. Partageons les sommets en deux paquets : le paquet 1 comprend le sommet A et le sommet diamétralement opposé ; le paquet 2 comprend les six autres sommets. De chaque sommet du paquet 1 partent 3 arêtes, toutes vers le paquet 2. De chaque sommet du paquet 2 partent 3 arêtes, 1 vers le paquet 1 et 2 vers le paquet 2. Par conséquent, le nombre de chemins de longueur n allant de A au paquet 1 est le coefficient d'indice $(1,1)$ de la puissance n-ème de la matrice $M = \begin{pmatrix} 0 & 3 \\ 1 & 2 \end{pmatrix}$. Si n est pair, tous ces chemins arrivent en A, et si n est impair ils arrivent au sommet diamétralement opposé. La matrice M se

diagonalise facilement : $M = P \begin{pmatrix} 3 & 0 \\ 0 & -1 \end{pmatrix} P^{-1}$, avec $P = \begin{pmatrix} 1 & 3 \\ 1 & -1 \end{pmatrix}$, ce qui permet d'obtenir le coefficient d'indice (1,1) de M^n : $(3^n + (-1)^n \times 3)/4$.
Bilan : Il existe $\frac{1}{4}\left[3^n + (-1)^n \times 3\right]$ chemins de longueur n :
- allant d'un sommet à lui-même si n est pair, et
- d'un sommet au sommet diamètralement opposé si n est impair.
On pourra également regarder ici pour une méthode probabiliste.

(1.2) Pour l'étude de $\mathfrak{A}_5$, voir [Ort] page 35.

(1.3) Pour $n = 2$, c'est effectivement le cas, sinon, il s'agit "seulement" d'un produit semi-direct (cf [Per], page 23).

(1.4) L'isomorphisme $\mathfrak{S}_n \simeq D_m$ est valable pour $n = 3$, $m = 3$ (faire agir le groupe des isométries d'un triangle équilatéral sur ses sommets) ; mais, sinon, ce n'est pas le cas puisque D_m contient un sous-groupe d'indice 2 cyclique, donc abélien, alors que le seul sous-groupe d'indice 2 de $\mathfrak{S}_n$ est $\mathfrak{A}_n$ qui n'est pas abélien pour $n > 3$.

(1.5) Le nombre de dérangements de $\mathfrak{S}_n$ est $n!\left(\sum_{k=0}^{n} \frac{(-1)^k}{k!}\right)$. Voir [FGN1], page 8.

(1.6) D'après Meu : si on note e le cardinal de E et f celui de F (e et f tous les deux $\geqslant 2$, sinon ce n'est pas drôle), les réponses sont (sauf erreur) :

$$\mathrm{sign}(\sigma)^f \times \mathrm{sign}(\tau)^e$$

et

$$\mathrm{sign}(\sigma)^{(f^e - f^{e-1})/2} \times \mathrm{sign}(\tau)^{(f^e - (f-2)^e)/2}\ .$$

(1.7) Le groupe des automorphismes de corps de $\mathbb{F}_q$ ($q = p^n$) est cyclique engendré par le Frobenius $\mathcal{F}$ défini par $x \to x^p$. En effet, il n'est pas difficile de montrer que l'ordre de $\mathcal{F}$ est n, et comme $\#\ \mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_p) \leqslant [\mathbb{F}_q : \mathbb{F}_p] = n$ (conséquence de l'indépendance linéaire des morphismes de Dedekind), $\mathcal{F}$ engendre $\mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_p)$. Voir [Goz], page 86.

(1.8) Signature du Frobenius : le cas p premier impair se traite de différente façon (avec le théorème de Frobenius-Zolotarev ou avec les polynômes irréductibles) et le cas $p = 2$ reste encore à élucider pour moi !
Références sur le net :
http ://agreg-maths.univ-rennes1.fr/documentation/docs/SignFrob.pdf
http ://www-pequan.lip6.fr/ graillat/papers/SignFrob.pdf
http ://objagr.gforge.inria.fr/documents/files/signature-frobenius.pdf

(1.9) Ceci repose sur le théorème de Frobenius-Zolotarev qui affirme que si $u \in GL_n(\mathbb{F}_p)$ avec p premier impair, alors $\varepsilon(u) = \left(\frac{\det u}{p}\right)$ (cf [OA], page 251). Si on pose $q = p^s$ alors $M \in GL_{ns}(\mathbb{F}_p)$ et on a alors $\varepsilon(M) = \left(\frac{\det M}{p}\right)$ (toujours pour p impair).
Voir aussi : http ://www-pequan.lip6.fr/ graillat/agregation/FrobZol.pdf

(1.10) Comme $\mathbb{F}_{p^n}$ est un $\mathbb{F}_p$-ev de dim n, il est isomorphe à $\mathbb{F}_p^n$, et on peut donc considérer une matrice de $GL_n(\mathbb{F}_p)$ comme une bijection linéaire de $\mathbb{F}_{p^n}$. Ainsi pour montrer que $\mathrm{GL}_n(\mathbb{F}_p)$ contient un élément d'ordre $p^n - 1$, il suffit de considérer l'endomorphisme de $\mathbb{F}_{p^n}$ suivant $u : x \longrightarrow ax$, où a est un générateur de $\mathbb{F}_{p^n}^*$.

(1.11) Réponse donnée par Ritchie : on représente $\mathbb{F}_q$ par $\mathbb{F}_p[X]/\langle R\rangle$ où R est un certain polynôme irréductible sur $\mathbb{F}_p$ de degré n. Alors la multiplication par d est en fait la multiplication par un élément $\overline{D}$ de $\mathbb{F}_p[X]/\langle R\rangle$. On remarque tout d'abord que l'endomorphisme de multiplication par $\overline{X}$ a pour matrice, dans la base $(1, \overline{X}, \ldots, \overline{X}^{p^{n-1}})$, la matrice compagnon de R, notée $\mathcal{C}$. Dans cette même base, l'endomorphisme de multiplication par $\overline{D}$ a donc pour matrice $D(\mathcal{C})$. Comme les valeurs propres de $\mathcal{C}$ sont les racines de R qui sont $\overline{X}, \mathcal{F}(\overline{X}), \ldots, \mathcal{F}^{n-1}(\overline{X})$, on a $\det D(\mathcal{C}) = D(\overline{X})D(\mathcal{F}(\overline{X}))\ldots D(\mathcal{F}^{n-1}(\overline{X})) = D(\overline{X})\mathcal{F}(D(\overline{X}))\ldots\mathcal{F}^{n-1}(D(\overline{X})) = D(\overline{X})^{1+p+\ldots+p^{n-1}} = \overline{D}^{\frac{q-1}{p-1}}$.

(1.12) Soit φ un morphisme de $\mathfrak{S}_n$ dans $\mathbb{C}^*$. Si on regarde l'image d'une transposition τ par φ alors $\varphi(\tau)^2 = \varphi(\tau^2) = \varphi(id) = 1 \Rightarrow \varphi(\tau) \in \{\pm 1\}$. Comme les transpositions sont conjuguées et que $\mathbb{C}^*$ est commutatif, φ vaut -1 sur toutes les transpositions. Il y a donc deux morphismes : le morphisme trivial, et celui valant -1 sur les transpositions, c'est-à-dire la signature. Voir [Tau], page 63.

(1.13) C'est la question (1.2).

(1.14) Soit G un groupe fini plongé dans l'ensemble $\mathfrak{S}_G$ de ses permutations. On veut savoir quand cette image est contenue dans $\mathfrak{A}_G$. Soit φ le morphisme de groupes $\varphi : \begin{array}{ccc} G & \longrightarrow & \mathrm{Perm}(G) \simeq \mathfrak{S}_G \\ g & \longrightarrow & m_g : h \to gh \end{array}$
Pour $g \in G$, regardons $\varepsilon(m_g)$. On remarque que m_g se décompose en cycles tous de même longueur égale à $o(m_g)$. En effet, si on pose $r = \dfrac{\#G}{o(g)}$ (qui est le nombre de classes à gauche modulo $\langle g \rangle$), alors $m_g = (e\ g\ g^2 \dots g^{o(g)-1})(h_2\ h_2 g\ h_2 g^2\ \dots\ h_2 g^{o(g)-1}) \dots (h_r\ h_r g\ h_r g^2\ \dots\ h_r g^{o(g)-1})$. Ainsi $\varepsilon(m_g) = (-1)^{(o(g)+1)\frac{\#G}{o(g)}} = (-1)^{\#G}(-1)^{\frac{\#G}{o(g)}}$.
Donc $G \subset \mathfrak{A}_G$ ssi $\begin{cases} \#G \text{ est impair et } \frac{\#G}{o(g)} \text{ est impair } \forall g \in G \text{ (ce qui est équivalent à } \#G \text{ impair)} \\ \text{OU} \\ \#G \text{ pair (de la forme } 2^k\, m) \text{ et les 2-Sylow de } G \text{ ne sont pas cycliques (afin que } o(g) \text{ ne mange} \\ \text{pas toutes les puissances de 2 de } \#G, \text{ ce qui donnera que } \frac{\#G}{o(g)} \text{ reste pair pour tout } g). \end{cases}$
Voir également : http ://www.les-mathematiques.net/phorum/read.php ?3,526472,526472#msg-526472

(1.15) On plonge G dans $\mathfrak{S}_{2n}$ par translation à gauche via φ, et en considérant un élément $g \in G$ d'ordre 2 (qui existe d'après Cauchy), on montre que $\varphi(g)$ est une permutation qui est le produit de n transpositions. Comme n est impair, $\varphi(g) \not\subset \mathfrak{A}_{2n}$. Ainsi $\varphi(G) \cap \mathfrak{A}_{2n}$ est d'indice 2 dans $\varphi(G)$, ce qui fournit un sous-groupe d'ordre n de $\varphi(G)$, que l'on peut ramener dans G par l'injection φ.

(1.16) Les 2-Sylow de $\mathfrak{S}_4$ sont d'ordre 8 et sont en fait des groupes diédraux D_4 ; il y en a 3 (cf [Ort], page 28). On peut les voir sur les groupes du cube (qui est $\mathfrak{S}_4$) : un 2-Sylow est engendré par une rotation d'ordre 4 d'axe passant par les milieux de 2 faces opposées, et par un retournement d'axe passant par les milieux de 2 arêtes opposées.

(1.17) Voir [FGN1], page 17, où l'on donne le cardinal de $\mathrm{SO}_2(\mathbb{F}_p)$.
Réponse donnée par Meu : un groupe cyclique d'ordre $q-1$ si $q \equiv 1 \pmod 4$ et d'ordre $q+1$ si $q \equiv 3 \pmod 4$ (je laisse soigneusement de côté la caractéristique 2). Quelques mots d'explication :
- Si $q \equiv 1 \pmod 4$, alors -1 est un carré dans $\mathbb{F}_q$, et donc $(\mathbb{F}_q)^2$ muni de la forme quadratique $x^2 + y^2$ est un plan hyperbolique. Or le groupe spécial orthogonal d'un plan hyperbolique est toujours isomorphe au groupe multiplicatif du corps, donc ici un groupe cyclique d'ordre $q-1$.
- Si $q \equiv 3 \pmod 4$, alors -1 devient un carré dans $\mathbb{F}_{q^2}$ et $\mathrm{SO}_2(\mathbb{F}_q)$ est isomorphe au sous-groupe du groupe multiplicatif de $\mathbb{F}_{q^2}$ formé des éléments de norme 1 sur $\mathbb{F}_q$ (penser à S^1 dans $\mathbb{C}$). C'est donc un sous-groupe d'indice $q-1$ d'un groupe cyclique d'ordre q^2-1, ce qui fait bien un groupe cyclique d'ordre $q+1$.
Voici une réponse donnée par Skilveg dans le cas de la caractéristique 2.
On a $\mathrm{SO}_2(\mathbb{F}_{2^n}) \simeq (\mathbb{Z}/2\mathbb{Z})^n$. En effet : La matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est dans le groupe ssi $\begin{cases} ad - bc &= 1 \\ ab + cd &= 0 \\ a^2 + c^2 &= 1 \\ b^2 + d^2 &= 1 \end{cases}$, ce qui donne $(a+c)^2 = 1$ et donc $a + c = 1$; de même $b + d = 1$ et la matrice est de la forme $\begin{pmatrix} a & a+1 \\ b & b+1 \end{pmatrix}$. En regardant le déterminant, on obtient $a + b = 1$, donc la matrice est de la forme $\begin{pmatrix} x+1 & x \\ x & x+1 \end{pmatrix}$. La réciproque est évidente. Donc

$$\mathrm{SO}_2(\mathbb{F}_{2^n}) = \left\{ \begin{pmatrix} x+1 & x \\ x & x+1 \end{pmatrix};\ x \in \mathbb{F}_{2^n} \right\}$$

qui est isomorphe à $\mathbb{F}_{2^n}$ par $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto b$, et donc (en tant que groupe) à $(\mathbb{Z}/2\mathbb{Z})^n$.

(1.18) Pour $p = 2$, on peut donner le groupe diédral à 8 éléments qui est non abélien. Pour p quelconque ? ? Par exemple, le sous-groupe des unipotentes supérieures de $\mathrm{GL}_3(\mathbb{F}_p)$ (i.e. les triangulaires supérieures avec des 1 sur la diagonale). C'est le seul produit semi-direct non trivial $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/p\mathbb{Z}$. Voir [FG], page 23 et sur le forum, en bas de cette page. Voir aussi [Del] exercice 3.4.7, page 99.

(1.19) Dans un groupe cyclique, il existe un unique sous-groupe d'ordre d pour tout d diviseur de $\#G$. Voir [FG], page 3.

(1.20) Il n'existe pas d'injection de $\mathfrak{S}_3$ dans $\mathfrak{A}_4$, car $\mathfrak{A}_4$ ne contient pas de sous-groupe d'ordre 6, voir [Ort], page 23 (sinon H d'ordre 6 serait d'indice 2 donc normal et serait réunion de classes de conjugaison qui sont de cardinal 1, 3 ou 4...). D'une manière générale, il est impossible d'injecter $\mathfrak{S}_n$ dans $\mathfrak{A}_{n+1}$ pour $n \geqslant 2$, bien qu'il soit possible d'injecter $\mathfrak{S}_n$ dans $\mathfrak{A}_{n+2}$, cf [FGN1], page 68. En effet, si une telle injection φ existe, on a alors $n! \mid \frac{(n+1)!}{2}$, i.e. $2 \mid n+1$. Supposons donc n impair et $n \geqslant 5$. Alors on fait

agir $\mathfrak{A}_{n+1}$ par translation à gauche sur les classes à gauche modulo $\varphi(\mathfrak{S}_n) = G$, i.e. on a le morphisme suivant $\psi : \begin{array}{ccc} \mathfrak{A}_{n+1} & \longrightarrow & \mathrm{Perm}((\mathfrak{A}_{n+1}/G)_{gauche}) \simeq \mathfrak{S}_{(n+1)/2} \\ \sigma & \longmapsto & \{\tau G \mapsto \sigma\tau G\} \end{array}$. Comme $\mathfrak{A}_{n+1}$ est simple, $\ker\psi$ vaut $\{id\}$ ou $\mathfrak{A}_{n+1}$. Mais

ψ ne peut être injectif car $(n+1)!/2 > (\frac{n+1}{2})!$. Ainsi $\ker\psi = \mathfrak{A}_{n+1}$ et en regardant la classe de G, on a $\sigma G = G, \forall\sigma \in \mathfrak{A}_{n+1}$, i.e. $\mathfrak{A}_{n+1} \subset G$ et donc $G = \mathfrak{A}_{n+1}$, ce qui est impossible pour une raison de cardinal.

(1.21) On fait agir $\mathrm{GL}_2(\mathbb{F}_2)$ sur les droites vectorielles de $\mathbb{F}_2^3$ qui sont au nombre de $2+1=3$. Comme la seule homothétie de $\mathrm{GL}_2(\mathbb{F}_2)$ est l'identité, on obtient un morphisme injectif de $\mathrm{GL}_2(\mathbb{F}_2)$ dans $\mathfrak{S}_3$. Pour des raisons de cardinal, on a $\mathrm{GL}_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$. (voir [Per], page 106). Comme le groupe dérivé de $\mathfrak{S}_3$ est $\mathfrak{A}_3$, on a $D(\mathrm{GL}_2(\mathbb{F}_2)) = \mathfrak{A}_3$, ce qui montre que l'égalité $D(\mathrm{GL}_n(\mathbb{K})) = \mathrm{SL}_n(\mathbb{K})$ est en défaut pour $n=2$ et $\mathbb{K} = \mathbb{F}_2$.

(1.22) $\mathrm{Aut}(\mathfrak{S}_3) = \mathrm{Int}(\mathfrak{S}_3)$, car l'image d'une transposition est une transposition (ensuite, cf [FGN1], page 74). De plus, $\mathrm{Int}(\mathfrak{S}_n) \simeq \mathfrak{S}_n$ pour $n \geqslant 3$ (il suffit de considérer le morphisme $\begin{array}{ccc} \mathfrak{S}_n & \longrightarrow\!\!\!\!\rightarrow & \mathrm{Int}(\mathfrak{S}_n) \\ \sigma & \longmapsto & \{\tau \to \sigma\tau\sigma^{-1}\} \end{array}$ et de constater que le noyau est trivial puisque le centre de $\mathfrak{S}_n$ est trivial pour $n \geqslant 3$). Voir par exemple, [Per] page 30, [Ort] page 51 ou [Hau] page 75.

(1.23) Quels sont les sous-groupes de $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$? Réponse donnée par Alain : comme $(\mathbb{Z}/p\mathbb{Z})^2$ est un espace vectoriel de dimension 2 (un plan) sur le corps $\mathbb{Z}/p\mathbb{Z}$, les sous-groupes sont des sous-espaces vectoriels. Il y aura donc le le sev nul (le sous-groupe trivial) et l'ev complet (le groupe en entier), puis les sev de dim 1, c'est-à-dire les droites passant par l'origine. En prenant les p^2-1 points différents de l'origine, chaque droite est alors comptée $p-1$ fois, soit $\dfrac{p^2-1}{p-1} = p+1$ droites (sous-groupes propres non triviaux) ; on trouve en effet les droites engendrées par les vecteurs $(\lambda, 1)$ où λ parcourt $\mathbb{F}_p$ et la droite engendrée par $(1,0)$. Soit au total $p+3$ sous-groupes différents dans $(\mathbb{Z}/p\mathbb{Z})^2$. Voir aussi le problème corrigé 2.5.1 page 56 dans le Delcourt.

(1.24) Le groupe $(\mathbb{F}_q, +)$ est isomorphe au groupe $((\mathbb{Z}/p\mathbb{Z})^n, +)$.

(1.25) Le groupe $\mathrm{GL}_2(\mathbb{F}_3)$ opère sur les $3+1=4$ droites vectorielles de $\mathbb{F}_3^2$, et les homothéties opèrent trivialement, donc $\mathrm{PGL}_2(\mathbb{F}_3)$ opère fidèlement sur $\mathbb{P}(\mathbb{F}_3^2)$. Ainsi, $\mathrm{PGL}_2(\mathbb{F}_3)$ s'injecte dans $\mathfrak{S}_4$ et pour des raisons de cardinal, ces deux groupes sont isomorphes. Le groupe $\mathrm{PSL}_2(\mathbb{F}_3)$ est d'indice 2 dans $\mathrm{PGL}_2(\mathbb{F}_3)$, donc $\mathrm{PSL}_2(\mathbb{F}_3)$ est isomorphe à $\mathfrak{A}_4$. Ainsi, $D(\mathrm{PSL}_2(\mathbb{F}_3))$ est le groupe de Klein ([Ort] page 203).

(1.26) Existe-t-il un morphisme surjectif de $\mathfrak{S}_n$ dans $\mathfrak{S}_{n-1}$?
Si un tel morphisme φ existe, alors on a $\mathfrak{S}_n/\ker\varphi \simeq \mathfrak{S}_{n-1}$. Si $n \geqslant 5$, alors φ n'existe pas, puisqu'il n'existe pas de sous-groupe d'ordre n normal dans $\mathfrak{S}_n$ (en effet, $\frac{n!}{2} > n$ et le seul sous-groupe normal est $\mathfrak{A}_n$).
Pour $n=4$ (cf [FGN1], page 70), φ existe et on peut le voir sur le cube en faisant agir le groupe des isométries positives du cube (isomorphe à $\mathfrak{S}_4$) sur les 3 axes passant par les milieux de 2 faces opposées. On a donc le morphisme de groupes :

$$\begin{array}{ccccc} \varphi & : & \mathfrak{S}_4 & \longrightarrow & \mathrm{Perm}(3 \text{ axes principaux}) \simeq \mathfrak{S}_3 \\ & & g & \longmapsto & \{a \mapsto g(a)\} \end{array}$$

Le morphisme φ est surjectif, puisque pour échanger a_1 et a_2, il suffit de considérer la rotation d'axe a_3 et d'angle $\pi/2$; on obtient ainsi toutes les transpositions de $\mathfrak{S}_3$. Pour $n=3$, on peut facilement construire un morphisme surjectif sur $\mathfrak{S}_2$. Il suffit de considérer $\begin{array}{ccccc} \varphi & : & \mathfrak{S}_3 & \longrightarrow & \mathfrak{S}_2 \\ & & \mathrm{transpo} & \longmapsto & (1,2) \\ & & 3-\mathrm{cycle} & \longmapsto & id \end{array}$
Pour $n=2$, on peut prendre le morphisme trivial (et d'ailleurs, il n'y a que cette possibilité !).

(1.27) Le sous-groupe de $\mathfrak{S}_n$ engendré par la transposition $(1,2)$ n'est pas distingué dans $\mathfrak{S}_n$ (sauf si $n = 2...$), car en général, le seul sous-groupe distingué dans $\mathfrak{S}_n$ est $\mathfrak{A}_n$ (attention au cas $n = 4...$), qui n'est pas d'ordre 2. Son normalisateur est constitué des permutations dont la décomposition en cycles à supports disjoints est de la forme $(1,2)^\varepsilon \prod(?, \ldots, ?)$, où $\varepsilon \in \{0,1\}$.

(1.28) Il s'agit de la réciproque du lemme Chinois ; l'isomorphisme a lieu si a et b sont premiers entre eux.

(1.29) $\#\mathrm{PGL}_n(\mathbb{F}_q) = \dfrac{(q^n-1)(q^n-q)\ldots(q^n-q^{n-1})}{q-1}$, donc $\#\mathrm{PGL}_2(\mathbb{F}_4) = \dfrac{(4^2-1)(4^2-4^{2-1})}{4-1} = 60$. On peut montrer (cf [Per], page 106) que $\mathrm{PGL}_2(\mathbb{F}_4)$ est isomorphe à $\mathfrak{A}_5$; en effet, toujours pour les mêmes raisons que (1.25), $\mathrm{PGL}_2(\mathbb{F}_4)$ s'injecte dans $\mathfrak{S}_5$ et est d'indice 2 donc...

(1.30) Le nombre minimal de transpositions qui engendrent $\mathfrak{S}_n$ est $n-1$, cf [FGN1], page 69.

(1.31) Le nombre minimal de générateurs de $\mathfrak{S}_n$ est 2 : on peut engendrer $\mathfrak{S}_n$ avec un n-cycle et une transposition échangeant 2 éléments consécutifs du n-cycle ; et on ne peut guère faire mieux !

(1.32) Par l'opération habituelle ([Per], page 106), on obtient que $\mathrm{PGL}_2(\mathbb{F}_5)$ s'injecte dans $\mathfrak{S}_6$. De plus, $\mathrm{PGL}_2(\mathbb{F}_5)$ est d'indice 6 (car d'ordre 5!), et on sait ([Per], page 30) alors que $\mathrm{PGL}_2(\mathbb{F}_5)$ est en fait isomorphe à $\mathfrak{S}_5$.

2. Congruences, nombres entiers

(2.1) Compter les applications $\{1,\dots,n\} \longrightarrow \{1,\dots,p\}$ strictement croissantes n'est pas difficile. Il suffit de se donner n images distinctes dans $\{1,\dots,p\}$; il y a donc $\binom{p}{n}$ applications strictement croissantes. Pour compter les applications croissantes, c'est un peu plus délicat. En se donnant une application $f : \{1,\dots,n\} \longrightarrow \{1,\dots,p\}$ croissante, on peut construire une application g strictement croissante, en posant $g(k) = f(k) + k - 1$, et g est à valeurs dans $\{1,\dots,p+n-1\}$. On vérifie facilement que l'on construit ainsi une bijection entre les applications croissantes de $\{1,\dots,n\}$ dans $\{1,\dots,p\}$ et les applications strictements croissantes de $\{1,\dots,n\}$ dans $\{1,\dots,p+n-1\}$. Ainsi, le nombre d'applications $\{1,\dots,n\} \longrightarrow \{1,\dots,p\}$ croissante est $\binom{p+n-1}{n}$. On peut retrouver ce résultat directement en remarquant que se donner une application croissante, c'est se donner un p-uplet $(\alpha_1,\dots,\alpha_p)$ où $\alpha_i = \#f^{-1}(\{i\})$ avec $\sum \alpha_i = n$. Ceci revient à dénombrer les façons de ranger n objets dans p boîtes. Si l'on écrit ces objets sur une même ligne, cela revient à insérer $p-1$ séparations parmi les n objets. Il faut donc choisir les places des $p-1$ séparations parmi $n+p-1$ places. D'où $\binom{p+n-1}{p-1}=\binom{p+n-1}{n}$ applications croissantes. Dans le même style, voir [OA], page 195.

(2.2) Réponse de Meu : si k est l'ordre de 10 dans le groupe multiplicatif de $\mathbb{Z}/n\mathbb{Z}$, alors k est une période du développement décimal de $1/n$ et divise $\phi(n)$.

(2.3) Pour $n \in \mathbb{N}$, 2^n-1 premier $\Rightarrow n$ premier. En effet, si $n = mk$ alors $2^n-1 = (2^m)^k-1 = (2^m-1)(1+2^m+2^{2m}+\ldots+2^{m(k-1)})$. On trouve ainsi les nombres de Mersenne premiers. Voir peut-être Demazure (à vérifier). Pour $n \in \mathbb{N}$, 2^n+1 premier $\Rightarrow n = 0$ ou $n \in 2^{\mathbb{N}}$. En effet, si $n = 2^k m$ avec m impair $\geqslant 3$, alors $2^n+1 = 1-(-2^k)^m$ et en posant $a = 2^k$, on a $2^n+1 = (1+a)(1-a+a^2-\ldots-a^m)$ et $1+a$ est un vrai diviseur de 2^n+1. Ici, on trouve les nombres dits de Fermat. Voir [Goz], page 75 ou [FGN1], page 132.

(2.4) L'équation $16x+26y = n$ a une solution ssi n est pair (car $16 \wedge 26 = 2$). Si $n = 2m$, alors une solution particulière de l'équation $8x+13y = m$ est $(5,-3)$ et donc les solutions sont les couples $(5-13k, 8k-3)$ où $k \in \mathbb{Z}$.

(2.5) Voir [FGN1] page 127 pour un exo similaire.

(2.6) Il s'agit de déterminer le reste de la division euclidienne de 7^{3^9} par 10. La suite des puissances de 7 est périodique de période 4. Il s'agit donc de déterminer le reste de la division euclidienne de 3^9 par 4. On a $3 \equiv -1 \pmod 4$, donc $3^9 \equiv -1 \pmod 4$. On trouve ensuite, en déterminant les puissances de 7 modulo 10, que $7^{3^9} \equiv 3 \pmod{10}$.

2.7) Il s'agit de résoudre $777^{401} \equiv ? \pmod{1000}$. Comme $\varphi(1000) = \varphi(2^3)\varphi(5^3) = 2^{3-1}(2-1)5^{3-1}(5-1) = 400$, on a $777^{400} \equiv 1 \pmod{1000}$ et donc $777^{401} \equiv 777 \pmod{1000}$.

(2.8) Pour trouver une racine carrée explicite de -1 dans $\mathbb{Z}/p\mathbb{Z}$ quand $p \equiv 1 \pmod 4$, il s'agit de faire une relecture du théorème de Wilson. Ainsi $\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \pmod 4$, voir [FGN1], page 128-129 ou Duverney, Théorie des nombres, pages 68 et 75.

(2.9) Il s'agit de déterminer l'inverse de $\bar{8}$ dans le corps $\mathbb{Z}/13\mathbb{Z}$, qui est $\bar{5}$. Ainsi, l'ensemble des solutions est $5+13\mathbb{Z}$.

(2.10) Le système $\begin{cases} x \equiv a \pmod m \\ x \equiv b \pmod n \end{cases}$ a une solution ssi $m \wedge n \mid a-b$. En effet, si le système admet une solution x, il existe $k,l \in \mathbb{Z}$ tels que $x = a+km$ et $x = b+ln$. On a alors $a-b = ln-km$ et donc $m \wedge n \mid a-b$. Réciproquement, supposons que $d = m \wedge n \mid a-b$, et posons $b = a+dy$ avec $y \in \mathbb{Z}$. Prenons x une solution de la première équation : $x = a+km$. Pour que x satisfasse à la 2ème équation, il reste à voir s'il existe l tel que $a+km = a+dy+ln$, ou encore en écrivant $m = dm'$ et $n = dn'$ et simplifiant par d : $km' = y+ln'$. Cette équation possède bien une solution l, puisque $m' \wedge n' = 1$. Voir Mignotte, Algèbre concrète, page 62.

(2.11) Les racines de $P = 2X^3-X^2+5X+3$ sont $\frac{-1}{2}, \frac{1+i\sqrt{11}}{2}, \frac{1-i\sqrt{11}}{2}$. On peut commencer par chercher les racines rationelles $\frac{p}{q}$ et on sait alors que $p \mid 3$ et $q \mid 2$. L'étude du polynôme dérivé nous dit que la fonction polynomiale associée est croissante et comme $P(0) > 0$ et $P(-1) < 0$, le seul rationnel qui peut être racine de P est $\frac{-1}{2}$ et c'est bien le cas. Ensuite, il ne reste plus qu'à factoriser et trouver les racines d'un trinôme du second degré ! Cf Eric, Ritchie et ev.

(2.12) On peut se limiter à l'hypothèse $n > ab$ car sinon la solution $(b, 0)$ est évidente. Comme a et b sont premiers entre eux, $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$; donc pour tout entier $n > ab$, il existe (u_0, v_0) dans $\mathbb{Z}$ tels que $au_0 + bv_0 = n$ Et on sait que les couples d'entiers relatifs $(u_0 - kb, v_0 + ka)$ sont aussi solution !
On ne peut avoir u_0 et v_0 tous deux négatifs (car a et b sont positifs). S'ils sont tous deux positifs, alors c'est gagné ! On suppose désormais que $u_0 > 0$ et $v_0 < 0$. Alors $au_0 + bv_0 = n$ avec $bv_0 < 0$ implique $au_0 > n$. Mais puisque $ab < n$, cela implique que $u_0 > b$. On peut alors remplacer le couple (u_0, v_0) par le couple (u_1, v_1) tel que $u_1 = u_0 - b$ et $v_1 = v_0 + a$. Puisque $u_0 > b$, on a forcément $u_1 > 0$. Et on a $v_1 = v_0 + a$ donc $v_1 > v_0$.
Par récurrence, on construit ainsi de proche en proche une suite de couples d'entiers (u_n, v_n) solution de l'équation $au + bv = n$. (u_n) est positive strictement décroissante. (v_n) est négative strictement croissante. Or il n'existe pas de suite strictement décroissante d'entiers positifs, pas plus qu'il n'existe de suite strictement croissante d'entiers négatifs. Donc ou bien il existe un entier P tel que $u_P = 0$ et alors la solution est triviale. Ou bien la suite (u_n) ne s'annule pas, et alors il existe un entier N tel que $v_{N-1} < 0$ et $v_N \geqslant 0$. Ce couple (u_N, v_N) convient !

(2.13) C'est la question (2.10).

3.Polynômes, anneaux, corps

(3.1) De manière générale, l'ensemble des éléments nilpotents d'un anneau commutatif est un idéal (cf [FG] page 41). Si $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ est la décomposition en produit de premiers de n, alors l'idéal des éléments nilpotents de l'anneau $\mathbb{Z}/n\mathbb{Z}$ est engendré par $p_1 p_2 \dots p_r$. Cet idéal est réduit à zéro ssi $\alpha_i = 1, \forall i$.

(3.2) Voir [FGN1] page 90.

(3.3) Voici une réponse donnée par Ritchie : Soit $P = X^4 - 2X^2 + 9$ à décomposer en irréductibles sur $\mathbb{F}_p[X]$.
Si $p = 2$ ou $p = 3$, le résultat est évident : $P = (X + 1)^4$ sur $\mathbb{F}_2$ et $P = X^2(X^2 + 1)$ sur $\mathbb{F}_3$.
Supposons $p > 3$. On remarque que $P = (X^2 - 3)^2 + (2X)^2$. Si P a une racine, alors p divise une somme de deux carrés, dont aucun n'est divisible par p (facile). Cela implique classiquement que $p \equiv 1 \pmod 4$.
Si -1 est un carré, disons $-1 = i^2$, i.e. si $p \equiv 1 \pmod 4$, alors $P = (X^2 - 2iX - 3)(X^2 + 2iX - 3)$.
Si de plus 2 est un carré, i.e. si $p \equiv 1 \pmod 8$, alors $P = (X - i - \sqrt{2})(X - i + \sqrt{2})(X + i - \sqrt{2})(X + i + \sqrt{2})$.
Si 2 n'est pas un carré alors que -1 l'est, i.e. si $p \equiv 5 \pmod 8$, alors $P = (X^2 - 2iX - 3)(X^2 + 2iX - 3)$ est la décomposition en irréductibles de P (penser au discriminant des trinômes).
Il reste les cas $p \equiv 3 \pmod 8$ et $p \equiv 7 \pmod 8$, pour lesquels P n'admet pas de racine.
Dans le premier cas, -2 est un carré, disons $-2 = \alpha^2$, et on peut écrire $P = (X^2 - 1 + 2\alpha)(X^2 - 1 - 2\alpha)$, qui est la décomposition en irréductibles de P, puisqu'il n'a pas de racine.
Dans le second cas, 2 est un carré, et on peut écrire $P = (X^2 + 2\sqrt{2}X + 3)(X^2 - 2\sqrt{2}X + 3)$, qui donc également sa décomposition en irréductibles.

(3.4) Considérons le polynôme $P = X^2 + Y^2 + Z^2$ dans $\mathbb{K}[X, Y][Z]$. Alors P est irréductible ssi $-(X^2 + Y^2)$ est un carré dans $\mathbb{K}[X, Y]$. Ce qui impose que $\mathbb{K}$ est de caractéristique 2. En effet, si $-(X^2 + Y^2) = Q^2$ alors Q est homogène de degré 1, i.e. de la forme $aX + bY$. On a donc, en développant, $-(X^2 + Y^2) = a^2X^2 + 2abXY + b^2Y^2$. D'où $2 = 0$. Bilan : P est irréductible en caractéristique disctincte de 2 et sinon $P = (X + Y + Z)^2$.
Pour $X^m + Y^n + Z^2$, on peut s'en sortir avec les deux remarques de Meu :
1) Si $\mathbb{B}$ est un anneau intègre et $Q \in \mathbb{B}$, alors $Z^2 - Q$ est réductible dans $\mathbb{B}[Z]$ ssi Q est un carré dans $\mathbb{B}$.
2) Si Q est un carré dans $\mathbb{A}[X]$, $\mathbb{A}$ intègre ($\mathbb{A}$ est en fait $\mathbb{K}[Y]$), alors le degré de Q est pair et, si $\mathbb{A}$ est de caractéristique $\neq 2$, Q a ou bien un seul monôme, ou bien au moins trois monômes.
En conclusion : $X^m + Y^n + Z^2$ est irréductible sauf si
- $m = n = 0$ et -2 est un carré dans $\mathbb{K}$,
ou
- $\mathbb{K}$ est de caractéristique 2 et m et n sont pairs.

(3.5) Déterminer le corps $\mathbb{F}_3(\alpha)$, où α est une "vraie" racine 7ème de l'unité (i.e. différente de 1 ! !). Il est clair que α est racine de Φ_7. De plus, Φ_7 est irréductible sur $\mathbb{F}_3$; (on pourra trouver dans Demazure un théorème indiquant la factorisation de polynômes cyclotomiques sur $\mathbb{F}_p$ qui est le suivant : "Sur $\mathbb{F}_p$ avec p un premier ne divisant pas m, Φ_m est produit d'irréductibles tous de même degré d, où d est l'ordre de $\bar{p}$ dans $\mathcal{U}(\mathbb{Z}/m\mathbb{Z})$". Ici, l'ordre de 3 modulo 7 est 6, donc Φ_7 est bien irréductible sur $\mathbb{F}_3$). Ainsi $[\mathbb{F}_3(\alpha) : \mathbb{F}_3] = 6$ et donc le corps en question a 3^6 éléments.

(3.6) Archi-classique, voir par exemple [Per], page 75.

(3.7) Il y a $\dfrac{q+1}{2}$ carrés dans $\mathbb{F}_q$ ([Per], page 74). Ensuite, voir Mignotte page 176.

(3.8) L'anneau $\mathbb{K}[X]$ jouit des mêmes propriétés que l'anneau des entiers $\mathbb{Z}$ et il suffit alors de calquer la preuve bien connue de l'infinitude des nombres premiers dans cet anneau pour en déduire que $\mathbb{K}[X]$ ne peut pas avoir un nombre fini d'irréductibles.

(3.9) Si $n < 4$ c'est trivial, supposons donc $n \geqslant 4$. Notons $f(x) = x^n + pX + q$, on a $f'(x) = nx^{n-1} + p$ et $f''(x) = n(n-1)x^{n-2}$. Si n est impair. $\lim_{x\to-\infty} f(x) = -\infty$ et $\lim_{x\to+\infty} f(x) = +\infty$. De plus si $p \geqslant 0$, f est strictement crosissante sur $\mathbb{R}$ donc f s'annule en un seul point (TVI). Si $p < 0$, f est strictement croissante sur $\left]-\infty, -\sqrt[n-1]{-p/n}\right]$ et sur $\left[\sqrt[n-1]{-p/n}, +\infty\right[$, elle est décroissante sur $\left[-\sqrt[n-1]{-p/n},\ \sqrt[n-1]{-p/n}\right]$ donc f s'annule en au plus trois points. Si n est pair, f convexe sur $\mathbb{R}$ et s'annule donc au plus en deux points. (Réponse de Portland). Voici une autre solution donnée par Ritchie :
Si $n \geqslant 2$ est un entier et p, q deux réels, alors le polynôme $P = X^n + pX + q$ a au plus trois racines réelles. Si P avait au moins 4 racines réelles (distinctes), alors P' au aurait au moins 3, et P'' au moins 2 (Rolle). Mais $P'' = n(n-1)X^{n-2}$ n'a qu'une racine réelle, contradiction.

(3.10) On écrit la division euclidienne : $(\cos\theta + X\sin\theta)^n = Q(X)(X^2+1) + AX + B$, avec A et B réels. D'où $e^{in\theta} = Ai + B$, d'où $A = \sin n\theta$ et $B = \cos n\theta$. (Réponse d'ev).

(3.11) Montrons que $\mathbb{K}[X,Y]/\langle X^2 - Y^3\rangle$ s'injecte dans $\mathbb{K}[T]$.
On considére le morphisme $\varphi : \begin{array}{ccc} \mathbb{K}[X,Y] & \longrightarrow & \mathbb{K}[T] \\ P(X,Y) & \longmapsto & P(T^3, T^2) \end{array}$.
Soit $P \in \ker\varphi$. On effectue dans $\mathbb{K}[Y][X]$ la division euclidienne de P par $X^2 - Y^3$. Alors il existe $A, B \in \mathbb{K}[Y]$ et $Q \in \mathbb{K}[X,Y]$ tels que $P(X,Y) = (X^2 - Y^3)Q(X,Y) + A(Y)X + B(Y)$. En faisant $X := T^3$ et $Y := T^2$, on trouve : $0 = A(T^2)T^3 + B(T^2)$, ce qui est impose pour des raisons de degré $A = B = 0$. Donc $\ker\varphi = \langle X^2 - Y^3\rangle$. Ainsi l'image par φ de $\mathbb{K}[X,Y]/\langle X^2 - Y^3\rangle$ est un sous-anneau de $\mathbb{K}[T]$ et est donc intègre. Remarquons que l'anneau $\mathbb{K}[X,Y]/\langle X^2 - Y^3\rangle$ est en fait isomorphe à l'anneau $\mathbb{K}[T^3, T^2]$, qui est le sous-anneau de $\mathbb{K}[T]$ formé des polynômes sans terme en T.
Montrons que $\overline{X} = x$ est irréductible mais non premier. On a $\varphi(x) = T^3$ et $\varphi(y) = T^2$. Le monôme T^3 est irréductible dans $\mathbb{K}[T^3, T^2]$, puisque $T \notin \mathbb{K}[T^3, T^2]$. On a $T^3 \mid T^6 = T^3T^3$, et T^6 est aussi égal à T^2T^4 ; mais $T^3 \not| T^2$ et $T^3 \not| T^4$ donc T^3 est non premier.
Montrons que x^2 et xy n'ont pas de pgcd, i.e. que T^6 et T^5 n'ont pas de pgcd dans $\mathbb{K}[T^3, T^2]$. Comme $T \notin \mathbb{K}[T^3, T^2]$, le candidat au pgcd est T^3. Or T^2 divise T^6 et T^5. Mais comme T^2 ne divise pas T^3 (toujours car $T \notin \mathbb{K}[T^3, T^2]$), T^3 ne peut pas être pgcd, et il n'y a pas de pgcd. Voir [FG], exo 2.26 page 69.

(3.12) Voir (2.11)

(3.13) Remarquons tout d'abord que si a ne divise pas b, alors le système n'a pas de solution. Supposons donc que a divise b. On écrit les décompositions de a et b en produit d'irréductibles (le $\sim$ est là pour montrer qu'il y a un inversible devant) : $a \sim \prod_{i=1}^{n} p_i^{a_i}$ et $b \sim \prod_{i=1}^{n} p_i^{b_i}$ avec $0 \leq a_i \leq b_i$.
Si x et y sont solutions, alors $xy = ab$, et donc on peut écrire $x \sim \prod_{i=1}^{n} p_i^{x_i}$ et $y \sim \prod_{i=1}^{n} p_i^{y_i}$ avec $0 \leq x_i, y_i$.
La condition $\text{pgcd}(x,y) = a$ implique que pour tout i, $\min(x_i, y_i) = a_i$. De même, pour tout i, $\max(x_i, y_i) = b_i$. Réciproquement, x et y définis de cette façon sont bien solutions.

(3.14) Supposons que $P(a) = 0$ et $Q(b) = 0$ avec $P, Q \in A[X]$ unitaires. Alors le polynôme en X unitaire suivant $\text{res}_Y(P(Y), Q(X-Y))$ annule $a + b$. Moralement, le résultant de F et G est "le produit de G évalué en les racines de F" (si F est unitaire). Pour des détails sur le résultant, on pourra regarder ce document de Michel Coste.

(3.15) Le système est symétrique. Supposons $\{x, y, z\}$ solution. Notons $P = (X-x)(X-y)(X-z) = X^3 + aX^2 + bX + c$. On a $a = -(x+y+z) = -1$, $b = xy + yz + xz = (a^2 - (x^2+y^2+z^2))/2 = 10$, $c = -xyz$, donc si $c \neq 0$, $1/x + 1/y + 1/z = b/c$, d'où $c = -10$. Donc $P = X^3 - X^2 + 10X - 10 = (X-1)(X^2+10)$. Ainsi $\{x, y, z\} = \{-1, \sqrt{10}, -\sqrt{10}\}$. Réciproquement $\{-1, \sqrt{10}, -\sqrt{10}\}$ est solution.

(3.16) On note $F = U/V$. On note également, pour $\sigma \in \mathfrak{S}_n$, U_σ et V_σ les polynômes où l'on a permuté les variables $X_1, \ldots, X_n$ selon σ. Par hypothèse, pour toute permutation σ, on a :
$U/V = U_\sigma/V_\sigma$, et donc $UV_\sigma = VU_\sigma$. En sommant ces égalités pour $\sigma \in \mathfrak{S}_n$, on trouve :
$U\sum_{\sigma\in\mathfrak{S}_n} V_\sigma = V\sum_{\sigma\in\mathfrak{S}_n} U_\sigma$, soit, avec $P = \sum_{\sigma\in\mathfrak{S}_n} U_\sigma$ et $Q = \sum_{\sigma\in\mathfrak{S}_n} V_\sigma$, $F = U/V = P/Q$, et P, Q sont bien des polynômes symétriques. (Réponse donnée par Ritchie)

(3.17) Soit $\phi : x \mapsto \frac{P(x)}{Q(x)}$ un endomorphisme de groupe additif de $(\mathbb{K}, +)$, avec P et Q premiers entre eux. Alors pour tous a, b, $\frac{P(a+b)}{Q(a+b)} - \frac{P(a)}{Q(a)} = \frac{P(b)}{Q(b)}$ donc : $Q(a)Q(b)P(a+b) - Q(b)Q(a+b)P(a) = Q(a)Q(a+b)P(b)$.

Comme cette égalité (polynomiale) est vraie pour une infinité de b ($\mathbb{K}$ infini), on a encore $Q(a)Q(X)P(a+X) - Q(X)Q(a+X)P(a) = Q(a)Q(a+X)P(X)$ et donc :

$$\frac{P(a+X)Q(a) - P(a)Q(a+X)}{Q(a)Q(a+X)} = \frac{P(X)}{Q(X)}$$

et comme le membre de droite de cette égalité est une fraction irréductible, $Q(X)$ divise $Q(a)Q(a+X)$ et donc $Q(X)$ et $Q(a+X)$ sont proportionnels pour tout a ; cela entraîne que Q est constant (sans quoi, soit z une racine de Q dans une extension algébrique de $\mathbb{K}$, alors pour tout a dans $\mathbb{K}$, $z+a$ est encore une racine, Q admet donc une infinité de racines... On peut aussi s'en sortir autrement : en plus d'être proportionnels, $Q(a+X)$ et $Q(X)$ ont le même coefficiant dominant et donc sont égaux, et ce pour tout a. On en déduit aussitôt que Q est constant). On peut donc supposer $Q = 1$. On a encore $P(a+X) - P(a) = P(X)$ et $P(0) = 0$ ce qui entraîne que $P(X)$ est de la forme λX. Le morphisme en question est une homothétie.
Soit maintenant $\psi : x \mapsto \frac{P(x)}{Q(x)}$ un morphisme de $(\mathbb{K}, +)$ dans $(\mathbb{K}^*, \times)$. On a alors (même type de raisonnement que ci-dessus) $\frac{P(a+X)}{Q(a+X)} \cdot \frac{Q(a)}{P(a)} = \frac{P(X)}{Q(X)}$ avec P, Q premiers entre eux. On en déduit encore que Q est constant et on peut encore le supposer égal à 1. On a $P(a+X) = P(a)P(X)$ pour tout a. En examinant les coefficients dominants de ces deux polynômes, on voit que P est constant lui aussi ; donc $P = 1$ car $\psi(1) = 1$.
Réponse de Foys. Référence : [FG], page 197.

(3.18) Il s'agit là d'un "petit théorème de Lüroth". Si $F \in \mathbb{K}(X)$, alors $[\mathbb{K}(X) : \mathbb{K}(F)]$ = hauteur de F, i.e. $\max(\deg(\text{num}(F)), \deg(\text{déno}(F)))$. Pour la démonstration, voir [Goz], page 184. Et aussi P. Samuel, Géométrie projective, page 73.

(3.19) Les polynômes $X^2 - 6X + 8$ et $X - 3$ sont premiers entre eux. On a $-(X^2 - 6X + 8) + (X - 3)(X - 3) = 1$, donc $(X^2 - 6X + 8).(-(X + 5)) + (X - 3).(X - 3)(X + 5) = X + 5$. Les solutions sont les couples $((X - 3)R(X) - (X + 5), -(X^2 - 6X + 8)R(X) + (X - 3)(X + 5))$ où $R \in \mathbb{K}[X]$.

(3.20) Notons $P = c\prod_{i=1}^m (x - a_i)^{\alpha_i} \prod_{i=1}^n (x - b_i)$ avec $\alpha_i > 1$, et les a_i et b_i deux à deux distincts, avec pour convention, si $m = 0$, $\prod_{i=1}^m (x - a_i)^{\alpha_i} = 1$. Notons $Q = P \wedge P'$ et montrons que $Q = \prod_{i=1}^m (x - a_i)^{\alpha_i - 1}$. $\prod_{i=1}^m (x - a_i)^{\alpha_i - 1}$ est un diviseur de P et de P', comme le montre la formule de dérivation d'un produit de polynômes. Supposons que $Q = R\prod_{i=1}^m (x - a_i)^{\alpha_i - 1}$ avec $\deg(R) \geqslant 1$. Soit z une racine de R. Alors il existe i tel que $z = a_i$ ou $z = b_i$. Or les b_i sont des racines simples de P, donc $z = a_i$ ainsi a_i est une racine de P' d'ordre au moins α_i, ce qui implique que a_i est une racine de P d'ordre au moins $\alpha_i + 1$, ce qui contredit l'hypothèse de départ sur P, donc $\deg(R) < 1$. Ainsi $P \wedge P' = \prod_{i=1}^m (x - a_i)^{\alpha_i - 1}$ (Réponse de Portland). Grâce à Ritchie, on peut avoir une preuve plus rapide : Si $P = \prod (X - \lambda_i)^{\alpha_i}$ est la décomposition en irréductibles de P dans $\mathbb{C}[X]$ (les λ_i deux à deux distincts), alors on sait que celle de P' est de la forme $P' = \prod (X - \lambda_i)^{\alpha_i - 1} Q(X)$, avec $Q(\lambda_i) \neq 0$ pour tout i (si $\alpha_i = 1$, alors le terme correspondant vaut 1 dans le produit précédent). En effet, si une racine de P est d'ordre a, alors elle est racine d'ordre $a - 1$ de P'. De là, le pgcd se lit sur les expressions de P et P' : il vaut $\prod (X - \lambda_i)^{\alpha_i - 1}$.

(3.21) C'est la question (4.5)

(3.22) Sans perte de généralité, on peut supposer que l'ouvert non vide contient 0 (sinon, on translate). La formule de Taylor s'écrit $P = \sum_{\nu \in \mathbb{N}^n} \frac{1}{\nu!} (D^{(\nu)}P)(0) X^\nu$, avec pour notation $\nu! = \prod_{i=1}^n \nu_i!$ et $X^\nu = \prod_{i=1}^n X_i^{\nu_i}$. Donc P est le polynôme nul.

(3.23) On a $P(X, X) = 0$ ssi $Y - X$ divise P (utiliser la division euclidienne par $Y - X$, polynôme unitaire en Y). On en déduit que les polynômes antisymétriques de $\mathbb{K}[X_1, \ldots, X_n]$ ($\mathbb{K}$ de caractéristique $\neq 2$) sont divisibles par $\Delta = \prod_{i<j} (X_i - X_j)$, et de là que ce sont exactement les polynômes de la forme ΔS où S est symétrique.

(3.24) On peut trouver cela dans les développements de Sébastien Pellerin et dans le Goblot, Algèbre commutative (page 180).

(3.25) Exo corrigé proposé dans le Goblot, Algèbre commutative. Autre référence, ici et là.

(3.26) Soient z_1, z_2, z_3 les racines complexes de $X^3 + aX^2 + bX + c$. On a $a = -(z_1 + z_2 + z_3)$, $b = z_1z_2 + z_2z_3 + z_3z_1$ et $c = -z_1z_2z_3$. On a $(X - z_1^2)(X - z_2^2)(X - z_3^2) = X^3 + \alpha X^2 + \beta X + \gamma$, avec $\alpha = -(z_1^2 + z_2^2 + z_3^2) = -(a^2 - 2b)$, $\beta = z_1^2z_2^2 + z_2^2z_3^2 + z_3^2z_1^2$ et $\gamma = -(z_1z_2z_3)^2 = -c^2$. Or $\beta = b^2 - 2(z_1z_2z_2z_3 + z_3z_1z_1z_2 + z_2z_3z_3z_1) = b^2 - 2ca$. Le polynôme $X^3 - (a^2 - 2b)X^2 + (b^2 - 2ca)X - c^2$ répond donc à la question.
On peut aussi utiliser le résultant comme le fait Ritchie : le polynôme $\text{Res}_X\left(Y - X^2, P(X)\right)$ convient.

(3.27) Voici une preuve "à coup de résultants" par Ritchie :
D'après le 3.26, on sait construire un polynôme unitaire R_1 de degré 3 dont les racines sont les carrés λ_i^2 de celles de P. On peut supposer que les λ_i^2 sont distincts deux à deux en divisant R_1 par $\text{pgcd}(R_3 - 1, R_1')$. On obtient un polynôme de degré $d_1 \leqslant 3$. D'après la 3.14, on sait également construire un polynôme unitaire R_2

de degré d_1^2 dont les racines sont les sommes $\lambda_i^2+\lambda_j^2$. Il y a des termes en trop. D'abord, les termes pour $i=j$: ils correspondent aux racines $2\lambda_i^2$. On les enlève en divisant par le polynôme dont les racines sont les doubles des carrés de celles de P , il s'agit de $R_1(X/2)$. On obtient un polynôme R_3. Ensuite, on a compté deux fois les termes pour lesquels $i\neq j$: R_3 est un carré $R_3=R_4^2$, et c'est le R_4 le polynôme recherché. Si le jury voulait la fonction polynomiale, c'est fini. Sinon, on sait que les quantités $\lambda_i^2+\lambda_j^2$ sont distinctes deux à deux (d'après la construction de R_1). Il suffit alors de diviser R_3 par $D=\operatorname{pgcd}(R_3,R_3')$ pour obtenir R_4.
Et une preuve un peu calculatoire d'Eric :
On a $\lambda_1+\lambda_2+\lambda_3=\sigma_1=0$, $\lambda_1\lambda_2+\lambda_2\lambda_3+\lambda_3\lambda_1=\sigma_2=p$ et $\lambda_1\lambda_2\lambda_3=\sigma_3=-q$. On cherche un polynôme du troisième degré dont les racines sont $\alpha_{12}=\lambda_1^2+\lambda_2^2$, $\alpha_{23}=\lambda_2^2+\lambda_3^2$ et $\alpha_{31}=\lambda_3^2+\lambda_1^2$. On a :

$$\alpha_{12}+\alpha_{23}+\alpha_{31}=2(\lambda_1^2+\lambda_2^2+\lambda_3^2)=2(\sigma_1^2-2\sigma_2)=-4p,$$

$$\begin{aligned}\alpha_{12}\alpha_{23}+\alpha_{23}\alpha_{31}+\alpha_{31}\alpha_{12}&=3(\lambda_1^2\lambda_2^2+\lambda_1^2\lambda_3^2+\lambda_3^2\lambda_2^2)+\lambda_1^4+\lambda_2^4+\lambda_3^4\\&=\tfrac{3}{2}\left((\lambda_1^2+\lambda_2^2+\lambda_3^2)^2-\lambda_1^4-\lambda_2^4-\lambda_3^4\right)+\lambda_1^4+\lambda_2^4+\lambda_3^4\\&=\tfrac{3}{2}\left((\lambda_1^2+\lambda_2^2+\lambda_3^2)^2\right)-\tfrac{1}{2}\left(\lambda_1^4+\lambda_2^4+\lambda_3^4\right)\\&=6p^2-\tfrac{1}{2}(\sigma_1^4-4\sigma_1^2\sigma_2+2\sigma_2^2+\sigma_1\sigma_3)\\&=6p^2-\tfrac{1}{2}2p^2\\&=5p^2,\end{aligned}$$

et, on tire également $3(\lambda_1^2\lambda_2^2+\lambda_1^2\lambda_3^2+\lambda_3^2\lambda_2^2)+\underbrace{\lambda_1^4+\lambda_2^4+\lambda_3^4}_{2p^2}=5p^2$, ainsi $\lambda_1^2\lambda_2^2+\lambda_1^2\lambda_3^2+\lambda_3^2\lambda_2^2=p^2$, d'où :

$$\begin{aligned}\alpha_{12}\alpha_{23}\alpha_{31}&=(\lambda_1^2+\lambda_2^2)(\lambda_2^2+\lambda_3^2)(\lambda_3^2+\lambda_1^2)+\lambda_1^2\lambda_2^2\lambda_3^2-\lambda_1^2\lambda_2^2\lambda_3^2\\&=(\lambda_1^2+\lambda_2^2+\lambda_3^2)(\lambda_1^2\lambda_2^2+\lambda_2^2\lambda_3^2+\lambda_3^2\lambda_1^2)-\lambda_1^2\lambda_2^2\lambda_3^2\\&=-2p\,p^2-q^2\\&=-2p^3-q^2\end{aligned}$$

Le polynôme cherché est donc $X^3+4pX^2+5p^2X+2p^3+q^2$.

(3.28) Supposons que pour tout $z\in\mathbb{C}$, $|P(z)|\geqslant|\mathrm{Im}(z)|^n$. Soit $z_k=x_k+iy_k$ une racine de P. Comme par hypothèse, $|y_k|^n\leqslant|P(z_k)|=0$, on a $y_k=0$; ainsi P a toutes ses racines réelles. Réciproquement, si P a toutes ses racines réelles (i.e. $z_k=x_k$), on a $|P(x+iy)|=\prod_{k=1}^n|x-x_k+iy|$, où les racines sont comptées avec ordre de multiplicité. Or $|x-x_k+iy|=\sqrt{(x-x_k)^2+y^2}\geqslant|y|$. Ainsi $|P(z)|\geqslant|\mathrm{Im}(z)|^n$.

(3.29) Voici une belle question et une tout aussi belle réponse donnée par Ritchie !
Soit $P=p_nX^n+\cdots+p_{k+2}X^{k+2}+p_kX^k+\cdots+p_0$ tel que $p_kp_{k+2}>0$. Supposons que P ait toutes ses racines réelles. D'après le théorème de Rolle, P' est également scindé sur $\mathbb{R}$, ainsi que toutes les dérivées successives de P. En particulier, $Q=P^{(k)}=q_nX^{n-k}+\cdots+q_{k+2}X^2+q_k$ est scindé sur $\mathbb{R}$, et vérifie $q_kq_{k+2}>0$. On peut même supposer $q_n=1$. Soit $R=X^{n-k}Q\big(1/X\big)=q_kX^{n-k}+q_{k+2}X^{n-k-2}+\cdots+q_n$ le polynôme réciproque de Q. Puisque les racines de Q sont toutes non nulles, R est scindé sur $\mathbb{R}$ (ses racines sont les inverses des racines de Q). Il est en de même de ses dérivées successives, et en particulier de $R^{(n-k-2)}=r_kX^2+r_{k+2}$ qui vérifie lui aussi $r_kr_{k+2}>0$: contradiction.

(3.30) C'est la question (3.24).

(3.31) Pour la table de multiplication de $\mathbb{F}_8$, voir Mignotte, Algèbre concrète, page 147. Pour celle de $\mathbb{F}_4$, voir [Goz], page 58.

(3.32) Voir (3.5).

(3.33) a) Comme $x\in\mathbb{L}$ est entier sur $\mathbb{A}$, il existe $P\in\mathbb{A}[X]$ unitaire tel que $P(x)=0$. Notons $\pi_{x,\mathbb{K}}$ le polynôme minimal de x sur $\mathbb{K}$. On a alors $\pi_{x,\mathbb{K}}\mid P$. Ainsi, les racines x_i de $\pi_{x,\mathbb{K}}$ (dans un sur-corps $\mathbb{L}'$ de $\mathbb{L}$) sont entières sur $\mathbb{A}$ (puisque $P(x_i)=0$). Comme les éléments de $\mathbb{L}'$ entiers sur $\mathbb{A}$ est un sous-anneau de $\mathbb{L}'$, les fonctions symétriques élémentaires en les racines x_i de $\pi_{x,\mathbb{K}}$ sont entières sur $\mathbb{A}$. Or ce sont au signe près les coefficients de $\pi_{x,\mathbb{K}}$...
b) Supposons que $P\in\mathbb{A}[X]$ unitaire ait une décomposition dans $\mathbb{K}[X]$ de la forme FG, où F et G sont unitaires. Montrons alors que F,G sont à coefficients dans $\mathbb{A}$. Toute racine de F est entière sur $\mathbb{A}$, puisque racine de P. Or les coefficients de F sont au signe près les fonctions symétriques élémentaires en ses racines, donc sont entiers sur $\mathbb{A}$. Comme $\mathbb{A}$ est intégralement clos, F appartient à $\mathbb{A}[X]$. De même pour G.

(3.34) Ritchie connaît un corps algébriquement clos contenu strictement dans $\mathbb{C}$ et tout le monde est d'accord avec lui ! Il s'agit du corps des nombres algébriques qui est la clôture algébrique du corps des nombres rationnels.

(3.35) Voir [FGN1], page 194.

(3.36) Si $P = c\prod_{i=1}^{n}(X-\alpha_i)$, on a la décomposition en éléments simples $\frac{1}{P} = \sum_{i=1}^{n} \frac{b_i}{X-\alpha_i}$. Supposons $n > 1$. Alors en multipliant par X et en faisant tendre X vers $+\infty$, on obtient que $\sum_{i=1}^{n} b_i = 0$. D'autre part, en notant $Q_i(X) = \frac{P(X)}{X-\alpha_i}$, on a $\frac{1}{b_i} = Q(\alpha_i) = P'(\alpha_i)$. Ainsi $\sum_{i=1}^{n} \frac{1}{P'(\alpha_i)} = 0$.

(3.37) Voici une réponse donnée par Ritchie : $x^2 + (xy-1)^2$ est partout positif, mais n'atteint pas son infimum ; et une référence par Eric : Makarov, Goluzina, Lodkin, Podkorytov, Problèmes choisis d'analyse réelle, 2nde éd. russe (ce n'est pas dans la première édition).

(3.38) La parole est à Meu :
Il faut un peu interpréter l'énoncé, car le pgcd n'est défini qu'à un facteur constant près. Je comprends donc "pgcd" comme "pgcd unitaire", ce qui permet de le définir sans ambiguïté, si on exclut bien sûr le couple $(0,0)$ de l'espace.
L'endroit où les polynômes P et Q sont tous les deux de degré n et premiers entre eux est un ouvert dense, le pgcd (unitaire) vaut 1 sur un ouvert dense.
Si les polynômes P et Q sont tous les deux de degré $< n$, alors on peut les approcher par $(1-\epsilon X)P$ et $(1-\epsilon X)Q$ (avec $\epsilon \to 0$) qui ont un pgcd non constant.
Par contre si l'un des deux, par exemple P, est de degré n et l'autre, Q, de degré $< n$, alors, si P et Q sont premiers entre eux et si $(\tilde{P}, \tilde{Q})$ est proche de (P, Q), $\tilde{P}$ et $\tilde{Q}$ sont encore premiers entre eux.
Pour justifier cette affirmation, il convient, avec la notation de 3.9 où E désigne l'espace vectoriel des polynômes de degré $\leq n$, de considérer la fonction polynomiale sur $E \times E$ qui à (P, Q) associe leur résultant calculé comme si P et Q étaient toujours de degré n tous les deux (c.-à-d. le déterminant de la fameuse matrice de Sylvester de taille $2n$). Le résultant ainsi calculé s'annule ssi le pgcd de P et Q est non constant ou P et Q sont tous les deux de degré $< n$. Voir tout bon cours sur les résultants, par exemple ce texte de Michel Coste.
La réponse est donc : les points de continuité de la fonction "pgcd unitaire" sur $E \times E \setminus \{(0,0)\}$ sont les couples (P, Q) où P et Q sont premiers entre eux et au moins un des deux polynômes est de degré exactement n. Avec une vision de la droite projective (en homogénéisant les polynômes en formes de degré n en deux variables), on peut dire aussi que ce sont les couples (P, Q) qui n'ont aucune racine commune, y compris à l'infini.

(3.39) L'application qui a (P, Q) associe leur résultant est polynomiale sur $E \times E$. L'endroit où elle ne s'annule pas, i.e. l'endroit où P et Q sont premiers entre eux, est un ouvert dense (que ce soit sur $\mathbb{R}$ ou sur $\mathbb{C}$). Réponse de Meu.

(3.40) Ce sont les fractions rationnelles qui n'ont pas de pôle simple.

(3.41) Voici la démonstration ; on pourra aussi regarder [FGN1], page 302 et [OA], page 144.

4. Algèbre linéaire

(4.1) Appelons A la matrice de $\mathcal{M}_n(\mathbb{K})$ "pleine" de 1. Elle est de rang 1 donc 0 est valeur propre de multiplicité $n-1$. Pour trouver l'autre valeur propre, on peut utiliser : $\mathrm{tr}(A) = n$ ou le fait que le vecteur colonne plein de 1 est vecteur propre pour la valeur propre n puisque la somme de chaque ligne vaut n. Ainsi, si le corps est de caractéristique nulle ou ne divisant pas n, la matrice A est diagonalisable. Sinon, A n'est pas diagonalisable (en revanche trigonalisable, puisque nilpotente : 0 est la seule valeur propre).

(4.2) On peut trouver la réponse ici ; le nombre de classes de conjugaison de matrices nilpotentes $\in \mathcal{M}_n(\mathbb{C})$ est lié aux partitions de l'entier n, via la décomposition de Jordan. On pourra regarder aussi [OA], page 173.

(4.3) Le rang est l'entier maximal pour lequel il existe une matrice extraite $r \times r$ de déterminant non nul. Donc, le rang sur $\mathbb{Q}$ et $\mathbb{C}$ sont les mêmes et le rang sur $\mathbb{F}_p$ est toujours inférieur ou égal au rang sur $\mathbb{Q}$. Maintenant, l'ensemble des p pour lesquels il y a inégalité stricte est fini. En effet, considérons $M_1, \ldots, M_k$ toutes les matrices extraites de taille $r \times r$. Alors il y aura inégalité stricte ssi $\det(M_i) \equiv 0 \pmod{p}$ pour tout i. Ainsi, l'ensemble des p pour lesquels l'inégalité est stricte est l'ensemble des diviseurs premiers de $\mathrm{pgcd}(\det(M_i), i \in [\![1, k]\!])$. Il est donc fini.

(4.4) Cf [FGN1], page 261, ou [Tau-ex], page 4.

(4.5) Cf [FGN1], page 352.

(4.6) Voir [FGN2], page 83.

(4.7) Voir [FGN2], page 117.

(4.8) Question posée par bs ici, et où on trouvera une preuve élémentaire (et élégante !) de Ritchie : Si $A_1, \dots, A_n$ désignent les colonnes de A, et $(e_1, \dots, e_n)$ la base canonique de $\mathbb{R}^n$, alors :

$$\det(A - XI) = \det(A_1 + (-X)e_1, \dots, A_n + (-X)e_n)$$

La multilinéarité du déterminant montre que ce déterminant se calcule en choisissant pour tout i entre A_i et $(-X)e_i$ (et en faisant la somme de tous les termes possibles ainsi formés).
Pour avoir les termes en X^{n-2}, il faut choisir $n-2$ $(-X)e_i$ différents, et deux A_{i_1} et A_{i_2} $(i_1 < i_2)$. On a donc la somme des termes de la forme

$$\det\big((-X)e_1, \dots, (-X)e_{i_1-1}, A_{i_1}, (-X)e_{i_1+1}, \dots, (-X)e_{i_2-1}, A_{i_2}, (-X)e_{i_2+1}, \dots, (-X)e_n\big) = (-X)^{n-2} \det\big(A_{i_1,i_2}\big),$$

où A_{i_1,i_2} est la matrice extraite de A en ne retenant que les lignes et colonnes i_1, i_2.

(4.9) Le nombre de matrices nilpotentes sur $\mathbb{F}_q$ est q^{n^2-n}, voir l'article de la RMS d'octobre 2006 : "Quelques dénombrements dans $\mathcal{M}_n(\mathbb{F}_q)$", de Tosel, retranscrit ici par Ritchie. On pourra aussi s'amuser à compter (plus facile) le nombre de matrices nilpotentes sur $\mathcal{M}_n(\mathbb{F}_q)$ d'indice n.

(4.10) Deux vecteurs entiers sont dans la même orbite ssi les pgcd de leurs coordonnées sont les mêmes. C'est une conséquence de la réduction de Hermite, voir par exemple ce document, proposition 7 page 4.

(4.11) Rang de la comatrice $\mathrm{com}(A)$ qui est le même que le rang de la transposée de la comatrice notée $\widetilde{A}$.
Si $\mathrm{rg}(A) = n$, alors A est inversible et comme $A\widetilde{A} = \det A\, \mathrm{I}_n$ $(\star)$, on en déduit alors que $\widetilde{A}$ est inversible et donc $\mathrm{rg}(\widetilde{A}) = n$.
Si $\mathrm{rg}(A) = n-1$, alors $\dim \ker A = 1$. Or $\mathrm{Im}(\widetilde{A}) \subset \ker A$ (d'après $(\star)$ et le fait que $\det A = 0$). De plus $\widetilde{A}$ est non nulle car il existe un mineur $n-1$ de A non nul (car A est de rang $n-1$). Donc $\mathrm{Im}(\widetilde{A}) = \ker A$ et $\mathrm{rg}(\widetilde{A}) = 1$.
Si $\mathrm{rg}(A) \leqslant n-2$, tous les mineurs de taille $n-1$ sont nuls et donc $\widetilde{A} = 0$.
Voir [Gou], page 147.

(4.12) On a, en notant $A^\sharp$ la transposée de la comatrice de A, $(P^{-1}AP)^\sharp = P^{-1}A^\sharp P$. Le faire d'abord pour les matrices inversibles A, puis appliquer cette égalité à $A - \lambda I_n$ qui est inversible sauf pour un nombre fini de λ. On obtient la nullité des n^2 coefficients de la matrice $(P^{-1}(A-\lambda I_n)P)^\sharp - P^{-1}(A-\lambda I_n)^\sharp P$ qui sont des fonctions polynomiales en λ. Comme $\mathrm{Sp}(A)$ est fini, ces fonctions sont nulles. En faisant $\lambda = 0$, on obtient le résultat, si le corps est infini. Voir [Tau-ex], page 76.

(4.13) Ultra-classique, voir [Gou] page 164.

(4.14) Les transvections d'hyperplan donné H, noyau d'une certaine forme linéaire f, forment un sous-groupe de $\mathrm{GL}_n(\mathbb{K})$. Une transvection $u_{H,a}$ de droite $\mathbb{K}a$ incluse dans l'hyperplan H a pour écriture : $u_{H,a}(x) = x + f(x)a$. On vérifie que la composée de deux transvections d'hyperplan H et de droite respective $\mathbb{K}a$ et $\mathbb{K}b$ est une transvection d'hyperplan H et de droite $\mathbb{K}_{a+b}$. En effet, $u_{H,a} \circ u_{H,b}(x) = u_{H,a}(x + f(x)b) = (x + f(x)a) + f(x)(b + f(b)a) = x + f(x)(a+b)$, puisque $b \in H$ par définition d'une transvection (donc $f(b) = 0$). Ainsi le sous-groupe de $\mathrm{GL}_n(\mathbb{K})$ des transvections d'hyperplan donné est isomorphe au groupe $(\mathbb{K}^{n-1}, +)$, (à une transvection d'hyperplan H, on associe le vecteur directeur de sa droite qui se trouve être dans H).

(4.15) L'espace vectoriel engendré par les matrices nilpotentes est le sev formé des matrices de trace nulle, cf [OA], page 169. On a une inclusion évidente : $\mathrm{vect}(\mathcal{N}) \subset \ker(\mathrm{trace})$. Pour l'inclusion réciproque, on peut montrer que toute matrice de trace nulle est semblable à une matrice à diagonale nulle et est donc somme d'une matrice triangulaire supérieure stricte et d'une matrice triangulaire inférieure stricte, qui sont toutes deux nilpotentes.
L'espace vectoriel engendré par les matrices inversibles est $\mathcal{M}_n(\mathbb{K})$ tout entier, cf [OA], page 150. On peut en effet obtenir une base de $\mathcal{M}_n(\mathbb{K})$ formée de matrices inversibles.

(4.16) C'est la question (1.25).

(4.17) La décomposition de Dunford étant unique, A est semblable à D, i.e. est diagonalisable, ssi sa partie nilpotente N est nulle.
Si A est réelle, D et N le sont aussi. En effet, il suffit d'écrire que $\overline{A} = \overline{D} + \overline{N}$ et remarquer que $\overline{D}$ est diagonalisable et $\overline{N}$ est nilpotente. Ainsi par unicité, on trouve $\overline{D} = D$ et $\overline{N} = N$.
Comme D et N commutent et sont trigonalisables, elles sont cotrigonalisables, et donc les valeurs propres de A sont exactement celles de D, puisque celles de N sont nulles. Ainsi, si A est inversible, D l'est également.

(4.18) Soit $A = D + N$ la décomposition de Dunford de A. Alors comme D et N commutent, la formule du binôme donne : $A^k = D^k + a_{k-1}D^{k-1}N + a_{k-2}D^{k-2}N^2 + \ldots + a_0N^k$. Comme D est diagonalisable, D^k l'est aussi et toujours par commutativité, on montre que $N' = a_{k-1}D^{k-1}N + a_{k-2}D^{k-2}N^2 + \ldots + a_0N^k$ est nilpotente. Ainsi, si on suppose A^k diagonalisable, alors par unicité de la décomposition de Dunford, on a $N' = 0$. Or $N' = a_{k-1}D^{k-1}N(I_n + b_1D^{-1}N + \ldots + b_{k-1}D^{-(k-1)}N^{k-1})$, et d'après la question (4.19), la parenthèse est

inversible puisque de la forme "identité + nilpotent". Ainsi on a $a_{k-1}D^{k-1}N = 0$. Comme A est supposée inversible, D est inversible (question (4.17)), et donc $N = 0$ (puisque $a_{k-1} = k \neq 0$). On a donc montré que $A = D$, i.e. que A est diagonalisable.
Si A n'est plus inversible, le résultat n'est pas vrai ; il suffit de considérer une matrice nilpotente d'indice k...
Si A est réelle, cela n'est pas vrai comme on le voit en considérant une rotation du plan d'angle $\pi/2$ qui n'est pas diagonalisable, bien que sa puissance quatrième le soit...

(4.19) Si N est nilpotente d'ordre p, $(I+N)^{-1} = I - N + N^2 - \cdots + (-1)^{p-1}N^{p-1} = \sum_{i=1}^{p-1}(-1)^i N^i$.
Si A est inversible et commute avec N, alors $A+N$ est nilpotente. En effet, $A+N = A(I_n + A^{-1}N)$. Comme A^{-1} est un polynôme en A et que A commute à N, A^{-1} commute aussi à N, et alors la matrice $A^{-1}N$ est nilpotente et on termine comme dans le 1er cas.

(4.20) Classique, c'est une application de la diagonalisation simultanée. cf [FGN2], page 168 ou [OA], page 205.

(4.21) Soit E l'ev des polynômes de degré $\leqslant n$ à coefficients réels. Alors la base duale de $(1, (X-a), \ldots, (X-a)^n)$ pour le crochet de dualité est $(f_0, \ldots, f_n)$, où : $f_j : E \to \mathbb{R}, P \mapsto \frac{P^{(j)}(a)}{j!}$.
Ainsi la formule de Taylor n'est rien d'autre qu'un cas particulier de la formule $x = \sum_{i=1}^{n} e_i^*(x)e_i$, valable pour tout espace vectoriel E de dimension finie, et toute base $\mathbf{e}$ et sa duale $\mathbf{e}^*$. Réponse de GreginGre.

(4.22) Le dual de E/F s'identifie à l'espace vectoriel des formes linéaires sur E qui s'annulent sur F, que l'on note habituellement $F^\perp$.

(4.23) Cf [FGN1], page 261.

(4.24) Il suffit de prendre n'importe quelle matrice inversible P au hasard pour voir que ça ne marche pas. En fait, N est le produit semi-direct interne de D et de $\mathcal{S}_n$ (vu comme groupe de matrices de permutations). Supposons que $P^{-1}\Delta P$ soit diagonale pour tout Δ diagonale. Choisissons en particulier Δ avec n valeurs propres distinctes. Puisque Δ et $P^{-1}\Delta P$ ont même valeurs propres (distinctes), elles sont donc déduites l'une de l'autre en conjuguant par une matrice de permutation S. Ainsi $S^{-1}\Delta S = P^{-1}\Delta P$, donc PS^{-1} commute avec Δ. Comme Δ n'a que des valeurs propres simples, PS^{-1} est un polynôme en Δ, donc diagonale. Ainsi $P \in D \rtimes \mathcal{S}_n$. La réciproque est claire. Le quotient N/D est donc $\mathcal{S}_n$. Réponse de GreginGre.

(4.25) Cf [FGN2], page 148.

(4.26) Voir la question (1.29).

(4.27) a) S'il existe un sous-espace stable non trivial F, alors en considérant une base adaptée (i.e. une base de F complétée en une base de E), et en considérant la matrice de u dans cette base, on voit que χ_u ne peut pas être irréductible. Réciproquement si $\chi_u = P_1^{\alpha_1} \ldots P_r^{\alpha_r}$ alors il existe un i tel que $P_i^{\alpha_i}(u) \notin \mathrm{GL}(E)$ (sinon cela contredirait Cayley-Hamilton). Ainsi $P_i(u)$ est également non inversible et en considérant un x non nul tel que $P_i(u).x = 0$, on obtient un sous-espace stable non trivial dont une base est $(x, u(x), \ldots, u^{\deg(P_i)-1}(x))$. On trouvera une preuve différente dans [FGN2], page 126.
b) Voir [Gou], page 219.

(4.28) Les conditions (ii) et (iii) sont équivalentes (voir par exemple, [FGN2], page 123) et un endomorphisme vérifiant l'une de ces deux conditions est dit cyclique. Pour montrer le reste de l'équivalence, il faut noter que la restriction d'un endomorphisme cyclique u à un sous-espace stable F est également cyclique. Pour voir ceci, on peut se souvenir que (E, u) est muni d'une structure de $\mathbb{K}[X]$-module via $P.x = P(u).x$ et copier la preuve de la propriété analogue dans le cas des groupes abéliens finis (qui sont des $\mathbb{Z}$-modules), qui revient simplement à dire qu'un sous-groupe d'un groupe cyclique est cyclique ! ! Et la preuve dans le cas des groupes est très simple : si x_0 est un générateur du groupe cyclique G et H un sous-groupe de G, alors on considère l'ensemble $\{m \in \mathbb{Z}, x_0^m \in H\}$ qui est un idéal non nul (car H est un groupe, et un groupe fini !) de $\mathbb{Z}$ donc monogène engendré par un certain d non nul. On vérifie facilement que $H = \langle x_0^d \rangle$. Allons-y dans le cas des endomorphismes ! Soit donc F un sous-espace stable de u. On considère l'ensemble $I = \{P \in \mathbb{K}[X], P(u).x_0 \in F\}$ qui est un idéal de $\mathbb{K}[X]$ car F est u-stable, non nul car $\chi_u \in I$. Ainsi I est monogène engendré par un certain polynôme D. On en déduit que l'endomorphisme $u_{|F}$ est cyclique, engendré par $D(u).x_0$.
Supposons (ii) ou (iii), c'est-à-dire que u est un endomorphisme cyclique. Notons $\mathcal{D}_u$ l'ensemble des diviseurs unitaires du polynôme minimal π_u de u qui est d'ailleurs ici égal à son polynôme caractéristique puisque u est cyclique. Notons aussi $\mathcal{S}_u$ l'ensemble des sous-espaces stables de u. On va montrer qu'il existe une bijection φ entre $\mathcal{D}_u$ et $\mathcal{S}_u$ en associant à un polynôme P le sous-espace u-stable : $\ker P(u)$.
Commençons par montrer que φ est injective. Soient P_1, $P_2 \in \mathcal{D}_u$ tels que $\ker P_1(u) = \ker P_2(u)$. Alors il existe $Q \in \mathbb{K}[X]$ tel que $\pi_u = P_1 Q$. Alors $\mathrm{Im}\, Q(u) \subset \ker P_1(u) = \ker P_2(u)$. Donc $(P_2Q)(u) = P_2(u) \circ Q(u) = 0$. Ainsi $\pi_u \mid P_2Q$ i.e. $P_1Q \mid P_2Q$, et $P_2 \mid P_1$. De même, on montrerait que $P_1 \mid P_2$.
Montrons maintenant la surjectivité : soit F un sous-espace u-stable. On va montrer que $F = \ker \pi_{u|F}(u)$. Notons K le sous-espace $\ker \pi_{u|F}(u)$. Il est clair que $F \subset K$ par définition même de K. Comme $\pi_{u|F}$ annule u

sur K, on a $\pi_{u|K} \mid \pi_{u|F}$. Ainsi $\deg(\pi_{u|K}) \leqslant \deg(\pi_{u|F})$. Comme K est u-stable, $u_{|K}$ est cyclique et donc $\dim(K) = \deg(\pi_{u|K})$. D'autre part, on a toujours (que u soit cyclique ou non) $\deg(\pi_{u|F}) \leqslant \dim(F)$. D'où $\dim(K) \leqslant \dim(F)$. Cette inégalité jointe à l'inclusion $F \subset K$ donne l'égalité souhaitée. Ainsi le nombre de sous-espaces u-stables est fini puisque l'ensemble des diviseurs unitaires de π_u est lui-même fini !
Réciproquement, supposons qu'il y a qu'un nombre fini de sous-espaces stables. On note $F_1, \ldots, F_r$ les sous-espaces u-stables stricts (i.e. $\neq E$), alors il existe un élément non nul $x_0 \in E \setminus F_1 \cup \ldots \cup F_r$. En effet, puisque $\mathbb{K}$ est infini, E n'est pas réunion de sous-espaces vectoriels propres (cf par exemple, Tauvel - Exercices de mathématiques pour l'agrégation). On considère alors l'espace vectoriel "engendré" par x_0 i.e. l'ensemble $\{P(u).x_0 \mid P \in \mathbb{K}[X]\}$. C'est un sev u-stable distinct des F_i puisque x_0 n'est dans aucun des F_i, il est donc forcément égal à E. Ainsi, $\{P(u).x_0 \mid P \in \mathbb{K}[X]\} = E$ et donc u est cyclique.

(4.29) Une réflexion est toujours diagonalisable. Deux réflexions commutent ssi elles sont diagonalisables dans une même base ou encore ssi tout espace propre de l'une est stable par l'autre. Réponse de Foys.

(4.30) Dans le cas des formes quadratiques non dégénérées, l'ensemble des formes quadratiques de signature donnée est ouvert. Voir [FGN3], page 214 ou [Gou], page 267.

(4.31) On sait qu'il existe $P \in \mathbb{C}[X]$ tel que $e^{P(A)} = A$ (cf (4.33)). D'autre part, d'après (4.32), il existe $Q \in \mathbb{C}[X]$ tel que $e^{P(A)/n} = Q(A)$. Alors $Q(A)^n = A$.

(4.32) L'ensemble $\Gamma = \{P(A), A \in \mathbb{C}[X]\}$ est un sev de $\mathcal{M}_n(\mathbb{C})$, donc est fermé. Or $e^A \in \overline{\Gamma}$, donc il existe $P \in \mathbb{C}[X]$ tel que $e^A = P(A)$. Voir [Gou], page 187.

(4.33) On commence par écrire la décomposition de Dunford de M, i.e. $M = D + N$ avec D diagonalisable, et N nilpotente et $DN = ND$. Il est important de rappeler pour la suite que D et N sont aussi des polynômes en M. Comme D et N sont trigonalisables et commutent, elles sont cotrigonalisables. On voit alors que les valeurs propres de M sont celles de D (puisque celles de N sont nulles). Ainsi si M est inversible, D l'est aussi et on peut écrire : $M = D(I + D^{-1}N)$.
L'objectif est maintenant de montrer que $D = e^{U(M)}$ et que $I + D^{-1}N = e^{V(M)}$. On aura alors $M = e^{U(M)}e^{V(M)} = e^{(U+V)(M)}$.
• Comme D est diagonalisable, il existe $\Omega \in \mathrm{GL}_n(\mathbb{C})$ telle que $D = \Omega\Delta\Omega^{-1}$ avec $\Delta = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$. Les λ_i sont non nuls puisque D est inversible. Par surjectivité de l'exponentielle de $\mathbb{C}$ sur $\mathbb{C}^*$, il existe $\mu_i \in \mathbb{C}$ tel que $e^{\mu_i} = \lambda_i$, $\forall i$. Grâce à l'interpolation de Lagrange, on construit un polynôme $Q \in \mathbb{C}[X]$ tel que $Q(\lambda_i) = \mu_i$.
On a alors :
$$\begin{aligned} D &= \Omega\,\mathrm{diag}(e^{\mu_1}, \ldots, e^{\mu_n})\,\Omega^{-1} \\ &= \Omega \exp(\mathrm{diag}(\mu_1, \ldots, \mu_n))\,\Omega^{-1} \\ &= \Omega \exp\left(\mathrm{diag}(Q(\lambda_1), \ldots, Q(\lambda_n))\right)\Omega^{-1} \\ &= \Omega \exp\left(Q(\mathrm{diag}(\lambda_1, \ldots, \lambda_n))\right)\Omega^{-1} \\ &= \exp\left(\Omega Q(\Delta)\Omega^{-1}\right) \\ &= \exp\left(Q(\Omega\Delta\Omega^{-1})\right) \\ &= \exp\left(Q(D)\right) \end{aligned}$$
Comme D est un polynôme en M, il existe $U \in \mathbb{C}[X]$ tel que $D = e^{U(M)}$.
• On a $I + D^{-1}N = \exp\left(\sum_{k=1}^{n-1}(-1)^{k-1}\frac{(D^{-1}N)^k}{k}\right)$. Comme D^{-1} est un polynôme en D (en effet, il suffit d'appliquer Cayley-Hamilton à D), et que D est un polynôme en M, on a $D^{-1} \in \mathbb{C}[M]$. On a aussi $N \in \mathbb{C}[M]$. Ainsi il existe $V \in \mathbb{C}[X]$ tel que $I + D^{-1}N = e^{V(M)}$.

Le résultat ne subsiste plus sur $\mathbb{R}$, puisque $\exp(\mathcal{M}_n(\mathbb{R})) \subset \mathrm{GL}_n^+(\mathbb{R})$ (car $\det(\exp) = \exp(\mathrm{trace})$).

(4.34) a) On a $\exp(\mathcal{M}_n(\mathbb{R})) = \{A \in \mathrm{GL}_n(\mathbb{R}), \exists B \in \mathcal{M}_n(\mathbb{R}), A = B^2\}$. L'inclusion "$\subset$" est évidente, il suffit d'écrire $A = e^M = \left(e^{M/2}\right)^2$. Pour l'autre inclusion, on écrit $A = B^2 = B\overline{B}$. Comme A est inversible, B l'est aussi et donc, d'après (4.33), il existe $Q \in \mathbb{C}[X]$ tel que $B = e^{Q(B)}$. Alors $\overline{B} = \overline{e^{Q(B)}} = e^{\overline{Q(B)}} = e^{\overline{Q}(B)}$. On a donc, puisque $Q(B)$ et $\overline{Q}(B)$ commutent, $A = e^{(Q+\overline{Q})(B)}$, et comme $Q + \overline{Q}$ est un polynôme à coefficients réels, on a $(Q + \overline{Q})(B) \in \mathcal{M}_n(\mathbb{R})$ et l'inclusion "$\supset$" est vérifiée.
b) Supposons qu'il existe $B \in \mathcal{M}_n(\mathbb{R})$ telle que $A = B^2$. Alors il existe d'après a), une matrice réelle M telle que $A = e^M$. Il suffit alors d'écrire que $A = \left(e^{M/k}\right)^k$.

(4.35) Sans perte de généralité, on peut supposer que les sommets de l'hexagone H_1 ont pour affixe $z_{1,k} = e^{i(2k-1)\pi/6}$, $1 \leqslant k \leqslant 6$. Soit H_2, l'hexagone de sommets les milieux des côtés de H_1. Notons $z_{2,k}$ les affixes des sommets de H_2, $Z_i = {}^t(z_{i,1}, \ldots, z_{i,6})$ et

$$M = \begin{pmatrix} 1/2 & 1/2 & 0 & 0 & 0 & 0 \\ 0 & 1/2 & 1/2 & 0 & 0 & 0 \\ 0 & 0 & 1/2 & 1/2 & 0 & 0 \\ 0 & 0 & 0 & 1/2 & 1/2 & 0 \\ 0 & 0 & 0 & 0 & 1/2 & 1/2 \\ 1/2 & 0 & 0 & 0 & 0 & 1/2 \end{pmatrix}$$

On a $Z_{i+1} = MZ_i$. On vérifie que $z_{2,k} = \cos\left(\frac{\pi}{6}\right) e^{ik\pi/3}$, $1 \leqslant k \leqslant 6$. De même $z_{3,k} = \cos^2\left(\frac{\pi}{6}\right) e^{i(2k+1)\pi/6}$, $1 \leqslant k \leqslant 6$. On montre par récurrence ainsi que $z_{2p+1,k} = \cos^{2p}\left(\frac{\pi}{6}\right) e^{i(2k+p)\pi/6}$, $1 \leqslant k \leqslant 6$, et $z_{2p,k} = \cos^{2p-1}\left(\frac{\pi}{6}\right) e^{i(k+p-1)\pi/3}$, $1 \leqslant k \leqslant 6$. (Réponse de Portland)

(4.36) En fait, il suffit de connaître les sous-groupes finis de $\mathrm{O}_2(\mathbb{R})$, puisqu'un sous-groupe fini de $\mathrm{GL}_2(\mathbb{R})$ est conjugué à un sous-groupe de $\mathrm{O}_2(\mathbb{R})$ (en prenant un produit scalaire moyenné). Les sous-groupes finis de $\mathrm{O}_2(\mathbb{R})$ sont cycliques ou diédraux. Voir Tisseron, Géométries affine, projective et euclidienne et [FGN3], page 309.

(4.37) Soit G un sous-groupe fini de $\mathrm{GL}_n(\mathbb{R})$. Les valeurs propres de $g \in G$ sont n racines de l'unité. Ainsi $\mathrm{tr}(g) \leqslant n$ et il y a égalité si et seulement si $g = 1$.
Remarquer que $\frac{1}{|G|}\sum_{g\in G} g$ est un projecteur. Voir [Tau-ex], page 42.

(4.38) Voir [Tau-ex], page 99, et cette discussion sur le forum.

(4.39) Notons $A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ et $B = A - I_2$. On montre par récurrence que $B^n = 2^{n-1}B$.

D'où $A^n = \sum_{k=1}^{n} \mathrm{C}_n^k 2^{k-1} B + I_2$. Donc $A^n = \begin{pmatrix} \frac{3^n}{2} + 1 & \frac{3^n}{2} - 1 \\ \frac{3^n}{2} - 1 & \frac{3^n}{2} + 1 \end{pmatrix}$.

(4.40) Deux endomorphismes semblables sont toujours équivalents. Lorsqu'il s'agit des projections, la réciproque est vraie. En effet, dans une bonne base, la matrice d'une projection de rang r est $\begin{pmatrix} I_r & \\ & 0 \end{pmatrix}$. Ainsi, si deux projections sont équivalentes (i.e. de même rang), alors elles sont semblables.

(4.41) L'application $\exp : \mathcal{M}_n(\mathbb{C}) \longrightarrow \mathrm{GL}_n(\mathbb{C})$ n'est pas injective, mais surjective d'après la question (4.33).
Par exemple, lorsque $n = 2$, on a $\exp \begin{pmatrix} 0 & -2\pi \\ 2\pi & 0 \end{pmatrix} = \exp \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.
Voir par exemple : [Gou], page 201 ; [OA], page 213 ; [FGN2], page 113 et Mneimné-Testard, Introduction à la théorie des groupes de Lie classiques.

(4.42) Indication de Meu : utiliser le polynôme annulateur $(X-1)^2(X-2)$. Si on note (e_1, e_2, e_3, e_4) la base canonique de $\mathbb{K}^4$, les sous-espaces stables sont exactement ceux qui s'écrivent $F \oplus G$ avec F égal à $\{0\}$, $\mathbb{K}e_1$ ou $\mathbb{K}e_1 \oplus \mathbb{K}e_2$ et G n'importe quel sous-espace de $\mathbb{K}e_3 \oplus \mathbb{K}e_4$.

(4.43) Comme $\pi_u(u) = 0$, en écrivant la décomposition de π_u en produit de facteurs irréductibles $P_1^{\alpha_1} \dots P_r^{\alpha_r}$, il existe $P_i(u) \notin \mathrm{GL}_n(\mathbb{R})$. Ainsi, il existe $x \neq 0$ tel que $P_i(u).x = 0$. Alors l'ev engendré par x et $u(x)$ est stable par u (car $\deg(P_i) \leqslant 2$). Voir [Tau], page 169.

(4.44) Voir [FGN2], page 135.

(4.45) L'exercice est corrigé dans [Ort], page 177. On trouve l'exemple : $\mathrm{GL}_3(\mathbb{R}) \simeq \mathrm{SL}_3(\mathbb{R}) \times \mathbb{R}^\star$.

(4.46) Soit $b \in B$ inversible dans A. Puisque A est de dim. finie sur k, alors la sous-algèbre k de B aussi. Ainsi il existe $P \in k[X], P \neq 0$ un polynôme annulateur de b de degré minimal . Si $P(0) = 0$, on peut écrire $P = XQ(X)$. Par minimalité de P, $Q(b) \neq 0$. Alors b est soit nul, soit un diviseur de zéro, donc b n'est ni inversible dans B, ni dans A, d'où une contradiction. On a donc $P(0) \neq 0$, et on peut toujours supposer que $P(0) = 1$, quitte à diviser par $P(0)$. Ainsi, $P(X) = XR(X) + 1$. Par hypothèse, il existe $a \in A$ tel que $ab = ba = 1$. Mézalor $a = P(b) - abR(b) = -R(b) \in k \subset B$, et a est un inverse de b dans B. Réponse de GreginGre.

(4.47) La matrice $A = \begin{pmatrix} 0 & i \\ i & 2 \end{pmatrix}$ est symétrique complexe non diagonalisable. Elle a pour polynôme caractéristique $\chi_A(X) = X^2 - 2X + 1 = (X-1)^2$. Si elle était diagonalisable, elle serait semblable à I_2 et donc égale à I_2. On peut étendre ce contre exemple dans $\mathcal{M}_n(\mathbb{C})$ par $\begin{pmatrix} A & 0 \\ 0 & I_{n-2} \end{pmatrix}$. Cf [Hau], page 75.

(4.48) Voir [FGN3], page 108.

(4.49) D'abord, P_σ est diagonalisable sur $\mathbb{C}$, car annulée par un polynôme scindé à racines simples : $T^{n!}-1$. Ensuite, si $\sigma = (\sigma_1 \dots \sigma_s)$ est la décomposition de σ en cycles disjoints, on réordonne les vecteurs de la base canonique en $B = (B_1, \dots, B_s)$ où B_ℓ contient les vecteurs de la base canonique numérotés par le cycle σ_ℓ. Dans cette base, la matrice "devient" $\mathrm{Diag}(P_{\sigma_1}, \dots, P_{\sigma_s})$, où chaque bloc P_{σ_ℓ} est la matrice compagnon du polynôme $T^{n_\ell}-1$. Celle-ci est diagonalisable dans la base de Vandermonde associée aux racines $n_\ell-$ièmes de l'unité $(\zeta_1, \dots, \zeta_{n_\ell})$, qui sont les valeurs propres. Réponse donnée par Ritchie.

(4.50) Soit V le sous-espace de E^* engendré par les ϕ_x avec $x \in \mathbb{R}$. Si $f \in E$ appartient à l'orthogonal de V notée V°, alors $\forall x \in \mathbb{R}, \phi_x(f) = 0$ i.e. $\forall x \in \mathbb{R}, f(x) = 0$, donc $f = 0$ et ainsi, puisque la dimension de E est finie, on a $V^{\circ\perp} = V$ donc $E^* = V$. Cela signifie que les formes linéaires ϕ_x engendrent E^*. Voir [Gou], page 152.

(4.51) La famille est libre (cf [Tau-ex], page 3), donc la dimension est n.

(4.52) Voir [FGN1], page 261.

(4.53) La relation $z_j = (a_j + a_{j+1})/2$ s'écrit matriciellement $MA = Z$ avec

$$M = \begin{pmatrix} 1/2 & 1/2 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \ddots & \ddots & 1/2 & 1/2 \\ 1/2 & 0 & \cdots & 0 & 1/2 \end{pmatrix}, \quad Z = {}^t(z_1, \dots, z_n), \quad A = {}^t(a_1, \dots, a_n)$$

En développant par rapport à la première colonne, on obtient $\det(2M) = 1 + (-1)^{n+1}$. Donc si n est impair, $\mathrm{Im}(M) = \mathbb{C}^n$, et pour tout $Z \in \mathbb{C}^n$, il existe $A \in \mathbb{C}^n$ tel que $MA = Z$. Si n est pair, $\mathrm{rg}(M) = n-1$. $\{{}^t(1,1,0,\dots,0), {}^t(0,1,1,\dots,0), \dots, {}^t(0,\dots,0,1,1)\}$ est une base de $\mathrm{Im}(M)$. Ce qui implique que $Z \in \mathrm{Im}(M)$ si et seulement si $z_1 - z_2 + z_3 + \cdots - z_n = 0$.
Voir [FGN3], page 299.

(4.54) Voir [FGN1], page 299.

(4.55) D'après (4.50), il existe $x_1, \dots, x_n \in X$ tels que $(\phi_{x_1}, \dots, \phi_{x_n})$ soit une base de E^*. Soit $\Theta : E \longrightarrow \mathbb{R}^n$, l'application $f \longmapsto (f(x_1), \dots, f(x_n))$. D'après le choix des x_i, Θ est injective et comme $\dim E = \dim E^* = n = \dim \mathbb{R}^n$, on en déduit que Θ est une bijection. Voir [Gou], page 152.

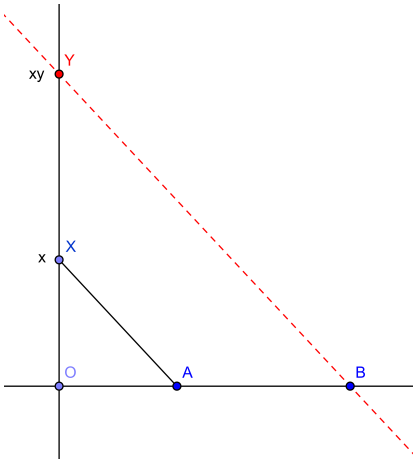
5. Géométrie

(5.1) L'ensemble $\mathcal{C}$ des réels constructibles est un sous-corps de $\mathbb{R}$. En effet, 0 et 1 sont constructibles. Supposons que x et y sont constructibles, alors :

• $x - y$ est clairement constructible.

• Dans la figure ci-dessous, d'après le théorème de Thalès on a $\dfrac{\overline{OB}}{\overline{OA}} = \dfrac{\overline{OY}}{\overline{OX}}$, en prenant $x = \overline{OX}$, $y = \overline{OB}$, et $\overline{OA} = 1$ on a $\overline{OY} = xy$ donc xy est constructible.

• Si $y \neq 0$, en prenant $\overline{OB} = \overline{OX} = 1$ et $\overline{OA} = y$ on a $\overline{OY} = \dfrac{1}{y}$. Donc $\dfrac{1}{y}$ est constructible.

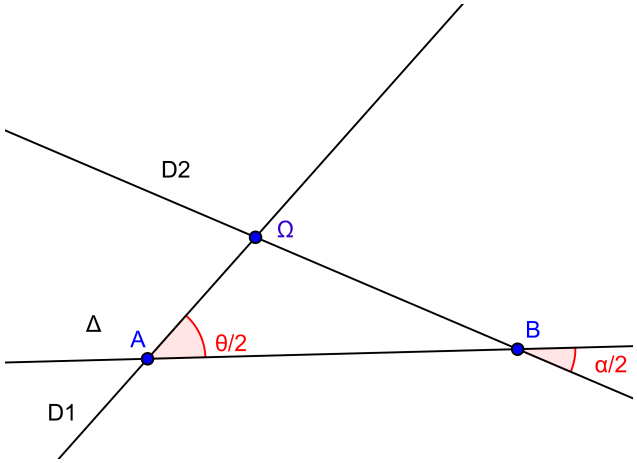


Ainsi $\mathcal{C}$ est un sous-corps de $\mathbb{R}$ qui contient $\mathbb{Q}$.
Donc l'ensemble des points constructibles du plan est un sous-corps de $\mathbb{C}$.
En fait $\mathcal{C}$ est le plus petit sous-corps de $\mathbb{R}$ stable par $\sqrt{\ }$. Pour prouver cette assertion, soit $x > 1$, on considère le cercle de centre $((x-1)/2, 0)$ de rayon $(x+1)/2$, qui coupe l'axe des abscisses en $B(-1,0)$ et $A(x,0)$. Soit $M(0,y)$ l'intersection du cercle avec l'axe des ordonnées (et $y > 0$). On a $BM^2 = 1 + y^2$ et $AM^2 = x^2 + y^2$ ainsi que $BM^2 + AM^2 = (x+1)^2$ ce qui implique que $2y^2 = 2x$, d'où $y = \sqrt{x}$.
Remarque : on peut aussi voir que AOM et BOM sont des triangles semblables.
Finalement la relation $(x+iy)^{-1} = \dfrac{x - iy}{x^2 + y^2}$ prouve que l'inverse d'un nombre constructible est constructible.
Ainsi l'ensemble des points constructibles du plan est-il un sous-corps de $\mathbb{C}$.

(5.2) Considérons les points correspondant aux $n+1$ vecteurs de la base canonique de $\mathbb{R}^{n+1}$, et voyons les comme dans un hyperplan affine correspondant à $\mathbb{R}^n$. Il est alors clair que cela forme $n+1$ points de $\mathbb{R}^n$ à même distance mutuelle. Merci à Skilveg pour nous avoir fait partager cette réponse. On pourra également regarder l'exercice "Groupe des isométries du simplexe régulier" de [FGN3], page 313, où on trouvera la démonstration de l'existence d'un tel simplexe.

(5.3)

Soient $r' = r(A, \theta)$ et $r = r(B, \alpha)$, deux rotations. On décompose chaque rotation en un produit de 2 symétries axiales dont les axes passent par le centre de ladite rotation, un des axes pouvant être choisie arbitrairement (noté Δ). Alors $r' \circ r = s_{D1} \circ s_\Delta \circ s_\Delta \circ s_{D2} = s_{D1} \circ s_{D2}$ qui est une rotation si $\alpha + \theta \neq 0$ à 2π près.
Alors le point Ω, construit sur la figure, est le centre de la composée des deux rotations planes.



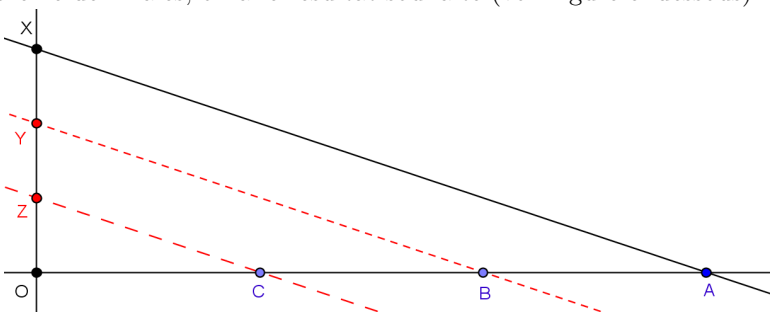
(5.4) Se trouve partout. Par exemple : Monier - Algèbre - page 362, ou [Per], page 145.

(5.5) On peut décrire les classes de conjugaison par une liste de formes réduites (toute transformation circulaire étant conjuguée à une et une seule des transformations de la liste).
Homographies :
- L'identité.
- $z \mapsto k\,z$, avec k de module $\leqslant 1$, de partie imaginaire $\geqslant 0$, différent de 0 et 1 (homographies à deux points fixes).
- $z \mapsto z + 1$ (homographies à un point fixe).

Antihomographies :
- $z \mapsto k\,\overline{z}$ avec $0 < k \leqslant 1$ (antihomographies avec au moins deux points fixes).
- $z \mapsto e^{i\theta}/\overline{z}$ avec $0 < \theta \leqslant \pi$ (antihomographies sans point fixe).
- $z \mapsto \overline{z} + 1$ (antihomographies avec 1 point fixe).

On constate que chacune des classes de conjugaison comprend une infinité d'éléments, sauf celle de l'identité bien sûr. Par conséquent le centre du groupe circulaire est réduit à l'identité.
Réponse de Meu.

(5.6) Si OX est le segment à partager en 3. On prend $OA = 3\,OX$, $OC = OX$ et $OB = 2\,OX$. En appliquant le théorème de Thalès, on a le résultat souhaité (voir figure ci-dessous).



(5.7) a) Considérons un point A du plan affine et son orbite $\{g(A);\ g \in G\}$ sous l'action de G groupe fini. Cette orbite étant conservée par tout élément g de G, son isobarycentre est donc un point fixe O pour tout élément g de G.
b) Soient r et r' deux rotations d'un même sous-groupe G des isométries, r et r' ayant un centre différent. Considérons $f = r \circ r' \circ r^{-1} \circ r'^{-1}$ qui est dans G. La partie linéaire de f est $Id_{\vec{E}}$; f est donc une translation de vecteur non nul car r et r' ne commutent pas, ayant un centre différent. On a $\forall\ n \in \mathbb{Z},\ f^n \in G$, et donc le sous-groupe de G engendré par f est dans G et est infini. Réponse donnée par Jean-Eric.

(5.8) D'après (5.7), chaque élément g de G admet au moins un point fixe commun O, et donc chaque élément de g ne peut être qu'une rotation de centre O ou bien un symétrie orthogonale d'axe contenant le point O. (G étant un groupe fini, il ne peut contenir de translation de vecteur non nul, ni de symétrie glissée : pour les translations, G serait infini et une symétrie glissée composée avec elle-même est une translation de vecteur non

nul). Supposons que G ne contient que des rotations, alors G est engendré par la rotation r ayant la mesure d'angle la plus petite dans l'intervalle $]0, 2\pi[$ parmi toutes les rotations de G. Cette rotation r a pour ordre n, ordre de G. C'est donc un groupe cyclique d'ordre n. Supposons maintenant que G contienne une symétrie orthogonale d'axe s passant par O. On écrit $G = G^+ \cup sG^+$ où G^+ est le sous groupe des rotations engendré par une rotation r_1 d'ordre n. l'élément $r_1 \circ s$ est un antidéplacement donc aussi une symétrie axiale qui vérifie : $(r_1 \circ s)^2 = I_d$ donc d'ordre 2. De plus $s^2 = I_d$. Alors G est isomorphe au groupe diédral d'ordre $2n$, produit semi-direct du groupe cyclique d'ordre n engendré par r et du groupe $\{I_d,\ s\}$. Réponse donnée par Jean-Eric.

(5.9) On note le réseau $R = \mathbb{Z}\vec{e}_1 + \mathbb{Z}\vec{e}_2$. Soit f une isométrie vectorielle directe conservant R. Le groupe cherché étant fini, il ne peut contenir de translation. Par suite nous sommes réduits à des rotations. Dans le base $(\vec{e}_1, \vec{e}_2)$, la matrice de f est à coefficients entiers et de la forme $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$. Sa trace étant entière et valant $2\cos\theta$, cette valeur est entière seulement pour les valeurs déterminées, car $-2 \leq 2\cos\theta \leq 2$.
Pour cela on a à résoudre $2\cos\theta = 0$, $\cos\theta = \frac{1}{2}$ et $2\cos\theta = \frac{-1}{2}$, $\cos\theta = 1$, $\cos\theta = -1$, ce qui conduit à $\theta = \frac{\pi}{2}$, $\theta = \frac{\pi}{3}$,$\theta = -\frac{\pi}{3}$, $\theta = \frac{2\pi}{3}$, $\theta = -\frac{2\pi}{3}$, $\theta = 0$ ou $\theta = \pi$.
Alors étant donné les valeurs de θ, tout élément cherché est d'ordre 1 pour $\theta = 0$, d'ordre 2 pour $\theta = \pi$, d'ordre 4 pour $\theta = \frac{\pi}{2}$, et d'ordre 6 dans les autres cas.

(5.10) Notons z_1, z_2, z_3 les affixes des sommets du triangle ABC. Le triangle ABC est équilatéral (E) ssi il est équilatéral direct ou indirect.
Posons $j = e^{i\pi/3}$. On a $1 + j + \bar{j} = 0$. Ainsi,

$$\begin{aligned}(E) &\Leftrightarrow z_1 - z_3 = j(z_1 - z_2) \text{ ou } z_1 - z_3 = \bar{j}(z_1 - z_2)\\ &\Leftrightarrow \big((z_2 - z_1) - j(z_3 - z_1)\big)\big((z_2 - z_1) - \bar{j}(z_3 - z_1)\big) = 0\\ &\Leftrightarrow z_1^2 + z_2^2 + z_3^2 = z_1z_2 + z_2z_3 + z_1z_3\end{aligned}$$

Une autre solution équivalente donnée par Bruno :
On se place dans le plan complexe et on considère le triangle équilatéral $\big((A,1),(B,j),(C,j^2)\big)$, le triangle $\big((M,z),(M',z'),(M'',z'')\big)$ est directement semblable à ABC si, et seulement si, il exite un couple $(a,b) \in \mathbb{C}^* \times \mathbb{C}$ tel que :

$$\left\{\begin{array}{rcl} z & = & a + b \\ z' & = & j\,a + b \\ z'' & = & j^2\,a + b \end{array}\right.$$

Le triangle $MM'M''$ est donc équilatéral *direct* si et seulement si le système de trois équations à deux inconnues (a,b) a une solution, ce qui équivaut à écrire que son déterminant est nul car la matrice du système est de rang deux, les vecteurs de $\mathbb{C}^3$ $(1,1,1)$ et $(1,j,j^2)$ étant linéairement indépendants. Le calcul du déterminant donne : $0 = j\,z + j^2\,z' + z''$ ce que l'on met encore sous la forme :

$$z + j\,z' + j^2\,z'' = 0.$$

Mais le triangle peut également être directement semblable au triangle (A,C,B) et l'on obtient la CNS :

$$z + j^2\,z' + j\,z'' = 0.$$

Ce qui fait que le triangle $MM'M''$ est équilatéral si, et seulement si :

$$(z + j\,z' + j^2\,z'')(z + j^2\,z' + j\,z'') = z^2 + z'^2 + z''^2 - (zz' + z'z'' + z''z) = 0$$

Voir par exemple [FGN3], page 256.

(5.11) Si $p = 0$ les racines complexes de $X^3 + q$ sont $a, ae^{i\pi/3}, ae^{-i\pi/3}$ ou $a^3 = q$, ce sont donc les affixes d'un triangle équilatéral.
Montrons que c'est le seul cas.
Notons z_1, z_2, z_3 les racines de $X^3 + pX + q$. Les points ayant pour affixes les z_i forment un triangle équilatéral ssi (P) : $z_1^2 + z_2^2 + z_3^2 = z_1z_2 + z_2z_3 + z_1z_3$ d'après l'exercice précédent.
Or $(X - z_1)(X - z_3)(X - z_3) = X^3 - \Sigma_1X^2 + \Sigma_2X - \Sigma_3$
Ainsi $(P) \Leftrightarrow \Sigma_1^2 - 3\Sigma_2 = 0 \Leftrightarrow p = 0$.

(5.12) Notons $A(z), B(z^2), C(z^3)$. On peut supposer $z \neq 0$ et $z \neq 1$. Le triangle ABC est iscoèle si et seulement si (1) : $|z^3 - z| = |z^3 - z^2|$ ou (2) : $|z^2 - z| = |z^2 - z^3|$ ou (3) : $|z - z^3| = |z - z^2|$.
(1) $\Leftrightarrow |z+1| = |z|$, (2) $\Leftrightarrow |z| = 1$, (3) $\Leftrightarrow |z+1| = 1$.
Ainsi ABC est isocèle si et seulement si z appartient $\mathcal{C}(O,1) \cup \mathcal{C}(-1,1) \cup \mathcal{D}$, où $\mathcal{D}$ est la droite d'équation $x = -1/2$.

(5.13) Voir par exemple Berger, Géométrie, 11.2.5 et 11.2.7

(5.14) On pourra consulter l'article suivant de Vidiani.

(5.15) Les coordonnées barycentriques du point de concours...
des médianes d'un triangle ABC sont $((A,1),(B,1),(C,1))$,
des bissectrices d'un triangle ABC sont $((A,a),(B,b)(C,c))$,
des hauteurs d'un triangle ABC non rectangle : $((A,\tan A),(B,\tan B),(C,\tan C))$,
des hauteurs d'un triangle rectangle en A, $((A,1),(B,0),(C,0))$,
des médiatrices d'un triangle : $((A,\sin 2A),(B,\sin 2B),(C,\sin 2C))$.
Référence : Transmath 1ère S - exercice 111, page 265. On trouvera ici un récapitulatif de toutes les coordonnées barycentriques des points remarquables d'un triangle.

(5.16) Soit G l'isobarycentre du quadrilatère $ABCD$, i.e. le barycentre du système $\{(A,1),(B,1),(C,1),(D,1)\}$. Par associativité du barycentre le segment joignant les points $I = \{(A,1),(B,1)\}$ et $J = \{(C,1),(D,1)\}$ ainsi que le segment joignant les points $K = \{(A,1),(D,1)\}$ et $L = \{(B,1),(C,1)\}$ se coupent en G leur milieu. Réponse de Jean-éric.

(5.17) Voici une réponse donnée par Pappus.
On vectorialise au point O d'intersection de D et Π. La fonction $M \longmapsto d(M,D)^2 + d(M,\Pi)^2$ est une forme quadratique définie positive. Le lieu demandé est donc un ellipsoïde de centre O dont Π est sans doute un plan diamétral conjugué de D, ce dernier point étant à vérifier.

(5.18) On se place dans un repère orthonormal du plan, la parabole $\mathcal{P}$ ayant pour équation $y^2 = 2px$. On note $\mathcal{C}$ le cercle d'équation $x^2 + y^2 - 2ax - 2by + c = 0$.
Un point $M(x,y)$ appartient à $\mathcal{C} \cap \mathcal{P}$ ssi $\begin{cases} y^2 = 2px \\ \frac{y^4}{4p^2} + (1 - \frac{a}{p})y^2 - 2by + c = 0 \end{cases}$.
On pose alors $P(y) = \frac{y^4}{4p^2} + (1 - \frac{a}{p})y^2 - 2by + c$.
Les points M_1, M_2, M_3 et M_4 appartiennent à $\mathcal{C} \cap \mathcal{P}$ si y_1, y_2, y_3, y_4 sont les racines de P qui est de degré 4.
Les relations entre racines et coefficients d'un polynôme conduisent à $\sigma_1 = \sum_{i=1}^4 y_i = 0$. Donc l'isobarycentre des points M_1, M_2, M_3 et M_4 ayant pour ordonnée $y = \frac{1}{4}\sum_{i=1}^4 y_i = 0$ est donc sur l'axe des abscisses, axe de symétrie de la parabole $y^2 = 2px$. Réponse donnée par Jean-éric. Voir Franchini-Jacquens, page 143.

(5.19) On commence par déterminer le sous-groupe G_D des isométries de l'espace affine euclidien laissant globalement invariant une droite D de cet espace. Maintenant soient L et L' les droites en question, l'ensemble des isométries de l'espace envoyant L sur L' est de la forme $\sigma.G_L = G_{L'}.\sigma$ où σ est une isométrie particulière envoyant L sur L'. Pour σ, je suggère de prendre un (ou le , car il me semble qu'il n'y en a qu'un) retournement échangeant L et L'. Merci Pappus.

(5.20) Lieu du second foyer des coniques de foyer F passant par P et Q, (sous-entendu : l'excentricité e est variable !).
1° La directrice associée à F passe par l'un ou l'autre de deux points fixes situé sur la droite PQ.
2° Le lieu du second foyer quand on fait le choix d'un de ces deux points est la conique (ellipse ou hyperbole à préciser) de foyers P et Q passant par F.
Réponse donnée par Pappus accompagée d'un joli dessin.

(5.21) Une réflexion est une symétrie orthogonale s_Q par rapport à un plan Q. Il faut donc trouver une c.n.s. pour qu'il existe un plan Q tel que $s_{P_1} \circ s_Q = s_{P_2} \circ s_{P_3}$.
Si des plans P et Q se coupent en une droite Δ alors $s_P \circ s_Q$ est une rotation d'axe Δ. Si des plans P et Q sont parallèles et distincts, alors $s_P \circ s_Q$ est une translation de vecteur orthogonal à P et Q.
Réciproquement, pour toute rotation r d'axe Δ contenu dans P, il existe un plan Q tel que $r = s_P \circ s_Q$ et pour toute translation t de vecteur orthogonal à P, il existe un plan Q tel que $t = s_P \circ s_Q$.
On conclut donc, dans le cas où P_2 et P_3 ne sont pas parallèles, que $s_{P_1} \circ s_{P_2} \circ s_{P_3}$ est une réflexion si et seulement si P_1 contient la droite d'intersection de P_2 et P_3, et dans le cas où P_2 et P_3 sont parallèles et distincts, que $s_{P_1} \circ s_{P_2} \circ s_{P_3}$ est une réflexion si et seulement si P_1 est parallèle à P_2 et P_3. Enfin si $P_2 = P_3$ alors $s_{P_1} \circ s_{P_2} \circ s_{P_3} = s_{P_1}$ est toujours une réflexion.
On peut formuler l'ensemble des résultats ainsi : $s_{P_1} \circ s_{P_2} \circ s_{P_3}$ est une réflexion si et seulement si les plans P_1, P_2, P_3 appartiennent à un même faisceau linéaire de plans.

Merci Meu pour cette belle réponse.

(5.22) Voici 2 preuves, une version "Algèbre linéaire" et une autre plus "affine", proposées par Jean-éric.
• Considérons deux rotations affines r et r du plan d'angle θ pour r et θ' pour r'. Les matrices des applications linéaires $\vec{f}$ et $\vec{f'}$ associées à r et r' sont respectivement de la forme :

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} \cos\theta' & -\sin\theta' \\ \sin\theta' & \cos\theta' \end{pmatrix}.$$

L'application affine $r \circ r'$ a pour partie linéaire $\vec{f} \circ \vec{f'}$ de matrice

$$\begin{pmatrix} \cos(\theta+\theta') & -\sin(\theta+\theta') \\ \sin(\theta+\theta') & \cos(\theta+\theta') \end{pmatrix}.$$

Ainsi la composée de deux rotations affines est une rotation affine si, et seulement si $\theta + \theta' \not\equiv 0 \pmod{2}\pi$, et c'est une translation sinon.
• $r = s_D \circ s_\delta$ et $r' = s_\delta \circ s_{D'}$, où δ est la droite (OO') centres respectifs des deux rotations (prendre une droite passant par O si $O = O'$). On a aussi $(D, \delta) \equiv \frac{\theta}{2} \pmod{\pi}$ et $(\delta, D') \equiv \frac{\theta'}{2} \pmod{\pi}$. Alors $r \circ r' = s_D \circ s_{D'}$ est une rotation d'angle $\theta + \theta'$, sauf si $\frac{\theta}{2} + \frac{\theta'}{2} \equiv 0 \pmod{\pi}$, dans ce cas c'est une translation.
Voir également la preuve de pappus ici.

(5.23) Une belle question qui vaut bien un fil pour elle toute seule que voilà. Et voici un beau résumé de Meu à propos du théorème de Motzkin.

(5.24) Voir la question (4.53).

(5.25) La parole est à Pappus :
L'application $\tau : z \longmapsto \dfrac{z+1}{z-1}$ est une transposition circulaire et à ce titre conserve les cercles "généralisés" de $\mathbb{C}$.
Quant aux coniques, je ne vois pas très bien ce qu'on peut en dire, à part le fait que leurs images par τ sont des courbes algébriques de degré plus élevé, sans doute 4. L'application τ est le produit commutatif de la symétrie $z \longmapsto \overline{z}$ avec l'inversion par rapport au cercle d'équation $z\overline{z} - z - \overline{z} - 1 = 0$. Il suffit de regarder comment une conique se transforme par cette inversion, passionnant ! Voir le beau dessin ici.

(5.26) On reconnaît l'écriture complexe d'une similitude indirecte : $z \mapsto a\overline{z} + b$, avec $a = e^{\frac{i\pi}{n}}$. Comme $|a| = 1$ c'est donc une isométrie, et mieux un antidéplacement : soit une symétrie axiale, soit une symétrie glissée.
Notons f l'application affine associée. Comme $f \circ f$ a pour écriture complexe $z \mapsto e^{\frac{i\pi}{n}}(e^{\frac{i\pi}{n}}\overline{z} + 1) + 1 = z + e^{\frac{i\pi}{n}} + 1$, $f \circ f$ est une translation de vecteur d'affixe $e^{\frac{i\pi}{n}} + 1$. Par suite f est une symétrie glissée.
Ainsi f est la symétrie glissée de vecteur $\vec{u}$ d'affixe : $\frac{1}{2}(e^{\frac{i\pi}{n}} + 1)$ et d'axe dirigé par $\vec{u}$ passant par le point d'affixe $\frac{1}{2}$, car le milieu $[Of(O)]$ est sur l'axe. Réponse donnée par Jean-éric.

6. Formes quadratiques et hermitiennes

(6.1) Une petite histoire de Meu :
Un bien chiant celui-ci. Et super facile à poser pour l'examinateur : pendant que la candidate faisait son développement sur la classification affine des quadriques réelles, il a effectué vite fait (en se cachant) le produit de $x + 2y - z + 1$ par $x - y + 3z - 2$ et viré le terme constant.
Mais la candidate, sans se démonter, a écrit la matrice de la forme quadratique homogénéisée (multipliée par 2 pour ne pas trainer de fractions)

$$\begin{pmatrix} 2 & 1 & 2 & -1 \\ 1 & -4 & 7 & -5 \\ 2 & 7 & -6 & 5 \\ -1 & -5 & 5 & 0 \end{pmatrix}$$

et calculé les mineurs principaux : 2 (à l'aise), -9 (pas dur), 0 (bon, là il vaut mieux écrire Sarrus). Arrivé là, elle se dit : tiens tiens, la conique à l'infini est dégénérée, la signature est $(1, 1)$ vu l'alternance de signes, c'est donc deux droites réelles sécantes. Puis elle s'arme de courage et calcule le déterminant 4×4 en échelonnant, ce qui lui permet de voir que la matrice est en fait de rang 3 (et donc de signature $(2, 1)$ ou $(1, 2)$). Elle jette alors un coup d'oeil à sa liste de quadriques et voit que la quadrique proposée est un cylindre hyperbolique (équation réduite $XY = 1$).

(6.2) Voici une réponse donnée par Meu :
Je suppose qu'il faut interpréter $\int$ comme $\int_a^b$ avec $a < b$. On pose $\ell = b - a$. On constate :
1) Que la forme quadratique est définie positive sur l'hyperplan des P tels que $\int P = 0$.
2) Que Cauchy-Schwarz nous dit que $(\int_a^b P)^2 \leq (\int_a^b P^2) \times (\int_a^b 1^2) = \ell \int_a^b P^2$, avec égalité si et seulement si P

est constant.
3) Que la valeur de la forme quadratique pour $P = c$ constant est $c^2\,(\ell - \ell^2)$.
Par conséquent, la signature de la forme quadratique est $(n+1, 0)$ si $0 < \ell < 1$, $(n, 0)$ si $\ell = 1$ et $(n, 1)$ si $\ell > 1$.

(6.3) C'est la question (5.17).

(6.4) Voir (4.47).

(6.5) Voir (4.48).

(6.6) Pour la simplicité de $\mathrm{SO}_3(\mathbb{R})$, voir par exemple, [Per], page 148, et pour la non-simplicité de $\mathrm{SO}_4(\mathbb{R})$, page 166. Voici une preuve (rapide ?) de la simplicité de $\mathrm{SO}_3(\mathbb{R})$. Soit $G \lhd \mathrm{SO}_3(\mathbb{R})$ et $G \neq \{id\}$. On va montrer que G contient un retournement et comme les retournements sont conjugués dans $\mathrm{SO}_3(\mathbb{R})$ et engendrent $\mathrm{SO}_3(\mathbb{R})$, on aura $G = \mathrm{SO}_3(\mathbb{R})$, car G est normal. Soit $g \in \mathrm{SO}_3(\mathbb{R})\backslash\{id\}$. On considère l'application continue $f : \mathrm{SO}_3(\mathbb{R}) \longrightarrow \mathbb{R}$ définie par $f(h) = \mathrm{tr}(hgh^{-1}g^{-1})$. Comme $\mathrm{SO}_3(\mathbb{R})$ est connexe et compact, $\mathrm{Im}(f)$ est un segment du type $[a, 3]$ et $a \neq 3$ (car le centre de $\mathrm{SO}_3(\mathbb{R})$ est trivial). Ainsi, on peut trouver n tel que $a < 1 + \cos(\frac{\pi}{n}) < 3$. Donc il existe $h \in \mathrm{SO}_3(\mathbb{R})$ tel que $\mathrm{tr}(hgh^{-1}g^{-1}) = 1 + \cos(\frac{\pi}{n})$. Or $g_0 = hgh^{-1}g^{-1} \in G$ car G est normal. Ainsi, $g_0^n \in G$ et est un retournement.

(6.7) La parole est à Meu : l'interprétation qui me semble la plus naturelle est de se poser la question de la dimension maximale d'un sous-espace linéaire (ou sous-espace projectif) contenu dans une quadrique projective (ou alors la dimension maximale d'un sous-espace affine contenu dans une quadrique affine). Une telle question pourrait avoir été posée, par exemple, à quelqu'un ayant parlé de sous-espace totalement isotropes maximaux (SETIM). En effet un sous-espace linéaire maximal contenu dans une quadrique projective est exactement le projectifié d'un SETIM de la forme quadratique équation de la quadrique.
Pour une forme quadratique non dégénérée, la dimension des SETIM (quelquefois appelée indice de Witt) est :
- sur $\mathbb{C}$, la partie entière de la moitié de la dimension.
- sur $\mathbb{R}$ où l'invariant est la signature (p, q), $\min(p, q)$.
Pour une forme quadratique non dégénérée sur un corps fini (de caractéristique $\neq 2$) de discriminant δ (modulo les carrés), l'indice de Witt est :
- k, si la dimension est $2k + 1$,
- si la dimension est $2k$, c'est k quand $(-1)^k\delta$ est un carré et $k - 1$ dans le cas contraire.
Pour une forme quadratique dégénérée, il faut ajouter la dimension du noyau à l'indice de Witt de la partie non dégénérée. Enfin, quand on projectifie pour passer aux quadriques, il faut bien sûr soustraire 1 aux dimensions. Par exemple, une surface quadrique affine réelle non dégénérée contient des droites si et seulement si son équation homogénéisée est de signature $(2, 2)$ (hyperboloide à une nappe ou paraboloide hyperbolique).
Petit ajout : les quadriques projectives réelles non dégénérées sont classifiées par leur indice de Witt, donc en fait par la dimension maximale des sous-espaces linéaires qu'elles contiennent (c'est vrai aussi en complexe, mais c'est moins drôle puisqu'il y a une seule classe). Ainsi pour les surfaces quadriques, il y a
- celle qui a des droites (indice de Witt 2),
- celle qui a des points, mais pas de droites (indice de Witt 1),
- et celle qui n'a même pas de points (indice de Witt 0).
Tout ceci tourne autour du théorème de Witt. Comme référence on peut prendre [Per] ou Berger.

(6.8) Voir [FGN3], page 21 et [Gou], page 266.

(6.9) Voir (3.7).

(6.10) On pourra lire les pages 163 et 167 du [Per] et consulter le Lelong Ferrand Arnaudies, tome 1, problème 5, page 510.

On utilise les quaternions réels. A chaque $q = (t, x, y, z) \in \mathbb{H}$ on associe la matrice $\phi(q) = \begin{pmatrix} u & -\overline{v} \\ v & \overline{u} \end{pmatrix}$ avec $u = t + iz$ et $v = ix + y$. Il reste à montrer que la restriction de ϕ à $\mathbb{S}^3$ est un isomorphisme de $\mathbb{S}^3$ sur $\mathrm{SU}_2(\mathbb{C})$, où $\mathbb{S}^3 = \{q \in \mathbb{H} \mid N(q) = 1\}$.

(6.11) L'espace vectoriel engendré par les matrices orthogoanles est $\mathcal{M}_n(\mathbb{R})$ tout entier. En effet, les matrices élémentaires E_{ij} sont combinaisons linéaires de matrices orthogonales.
Soient $A = I_n$, $B_i = I_n - 2E_{ii}$, $C_{ij} = I_n - E_{ii} - E_{jj} + E_{ij} + E_{ji}$ et $D_{ij} = I_n - E_{ii} - E_{jj} - E_{ij} + E_{ji}$. Il est facile de voir que ces matrices sont dans $\mathrm{O}_n(\mathbb{R})$. Et on a $A - B_i = 2E_{ii}$, $C_{ij} - D_{ij} = 2E_{ij}$. Par exemple pour $n = 6$

$$D_{35} = \begin{pmatrix} 1 & & & & & \\ & 1 & & & & \\ & & 0 & & -1 & \\ & & & 1 & & \\ & & 1 & & 0 & \\ & & & & & 1 \end{pmatrix}.$$

(6.12) Soit G un sous-groupe ccompact de $\mathrm{GL}_n(\mathbb{R})$ contenant $\mathrm{O}_n(\mathbb{R})$. Soit $A \in G$. La décomposition polaire permet d'écrire $A = OS$ avec $O \in \mathrm{O}_n(\mathbb{R})$ et $S \in \mathrm{S}_n^{++}(\mathbb{R})$. Comme $\mathrm{O}_n(\mathbb{R}) \subset G$ et que $A \in G$, la matrice S appartient à G, donc $(S^k)_{k\in\mathbb{Z}}$ est une suite d'éléments de G. Puisque G est compact, cette suite est bornée ; de plus, $S \in \mathrm{S}_n^{++}(\mathbb{R})$ est diagonalisable donc $\forall \lambda \in \mathrm{Sp}(S)$, on a $|\lambda| = 1$. Comme $S \in \mathrm{S}_n^{++}(\mathbb{R})$ ses valeurs propres sont positives, donc on a $\lambda = 1$, $\forall \lambda \in \mathrm{Sp}(S)$. Donc $S = I_n$, car S est diagonalisable. Donc $A = O \in \mathrm{O}_n(\mathbb{R})$, i.e. $G \subset \mathrm{O}_n(\mathbb{R})$.

(6.13) On procède par récurrence sur n. Pour $n = 1$, on a $\mathrm{O}(1, \mathbb{Q}) = \mathrm{O}(1, \mathbb{R})$. Supposons $n > 1$ et que le résultat est établi pour $n-1$. Soit $(u_1 \ldots, u_n)$ une b.o.n. de $\mathbb{R}^n$ (avec la structure euclidienne standard). Tout d'abord, les points rationnels sont dense dans la sphère unité de $\mathbb{R}^n$: on se ramène par projection stéréographique à la densité de $\mathbb{Q}^{n-1}$ dans $\mathbb{R}^{n-1}$. On peut donc trouver un vecteur unitaire rationnel v_1 aussi proche que l'on veut de u_1. On en déduit qu'on peut trouver une b.o.n. $(v_1, u'_2, \ldots, u'_n)$ aussi proche que l'on veut de $(u_1 \ldots, u_n)$ et dont le premier vecteur est rationnel. On peut compléter v_1 en une b.o.n. rationnelle $(v_1, w_2, \ldots, w_n)$. Si $v_1 \neq e_1$, il suffit par exemple de prendre l'image de la base canonique $(e_1, \ldots, e_n)$ par la symétrie orthogonale par rapport à $(v_1 - e_1)^\perp$. On peut alors appliquer l'hypothèse de récurrence dans l'hyperplan $v_1^\perp$ pour en déduire qu'il existe une b.o.n rationnelle $(v_2, \ldots, v_n)$ de cet hyperplan aussi proche que l'on veut de $(u'_2, \ldots, u'_n)$. On peut donc bien trouver une b.o.n. rationnelle $(v_1, \ldots, v_n)$ aussi proche que l'on veut de $(u_1, \ldots, u_n)$. Réponse de Meu.

(6.14) On fait le calcul de l'intégrale dans une base orthonormée de $\mathbb{R}^n$ diagonalisant Q qui s'écrit donc dans cette base : $Q(x_1, \ldots, x_n) = a_1 x_1^2 + \cdots + a_n x_n^2$. Puis on fait le changement de variables : $y_1 = (\sqrt{a}_1)x_1, \ldots, y_n = (\sqrt{a}_n)x_n$ dont le jacobien est $\frac{1}{\sqrt{a_1 \ldots a_n}} = \frac{1}{\sqrt{\mathrm{Discr}(Q)}}$. En utilisant que $\int_{\mathbb{R}} e^{-x^2} dx = \pi^{\frac{1}{2}}$, on obtient :

$$\int_{\mathbb{R}^n} e^{-Q(x)} dx = \frac{\pi^{\frac{n}{2}}}{\sqrt{\mathrm{Discr}(Q)}}.$$

Le volume V de $\{s \in \mathbb{R}^n \mid Q(x) \leqslant 1\}$ vaut

$$\int_{a_1 x_1^2 + \cdots + a_n x_n^2 \leqslant 1} dx_1 \ldots dx_n$$

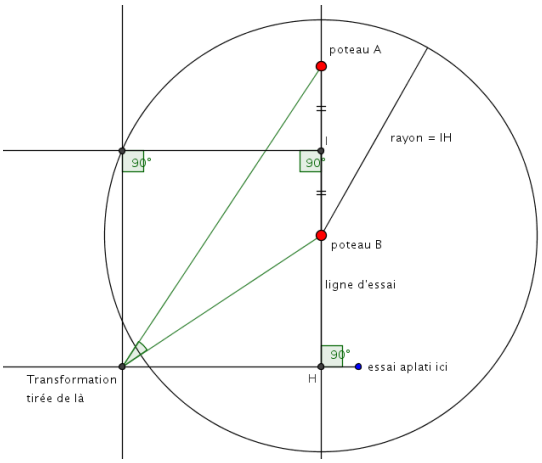
et après le même changement de variables que précédemment, on trouve que

$$V = \int_{x_1^2 + \cdots + x_n^2 \leqslant 1} \frac{dx_1 \ldots dx_n}{\sqrt{\mathrm{Discr(Q)}}} = \frac{\text{Volume de la boule unité de } \mathbb{R}^n}{\sqrt{\mathrm{Discr(Q)}}}$$

(6.15) On sait qu'un endomorphisme normal d'un ev euclidien est diagonalisable en base orthornormée (cf [Gou], page 254). Soit A la matrice de u dans une base orthonormée formée de vecteurs propres pour u, i.e. $A = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$. Alors la matrice de u^* dans cette base est $\mathrm{diag}(\overline{\lambda}_1, \ldots, \overline{\lambda}_n)$ (puisque la base est orthonormée). Or on sait qu'il existe $P \in \mathbb{C}[X]$ tel que $P(\lambda_i) = \overline{\lambda}_i$ (polynôme d'interpolation de Lagrange), et on a alors $u^* = P(u)$. La réciproque est triviale ! Voir [Tau], page 191.

(6.16)

Comme l'a fait remarquer Meu, on ne choisit pas le point d'où tirer une pénalité. Il s'agit en fait de la transformation d'un essai : on choisit alors le point d'où est tiré la transformation sur la perpendiculaire à la ligne d'essai passant par le point où l'essai a été aplati.
Soit T = point où le buteur mathématicien tirera sa tranformation, et $HT = x$. Alors $\tan(ATB) = \tan(HTA) - \tan(HTB) = \dfrac{xAB}{x^2 + HA.HB} = f(x)$ et f est max pour $x = \sqrt{HA.HB}$.
Référence : Midi Olympique - Numéro spécial mathématiques. D'après bs !



(6.17) Soient x, y deux vecteurs d'un espace préhilbertien complexe.
Soit $t \in \mathbb{R}$, et soit $u \in \mathbb{C}$ tel que $u < x, y >= | < x, y > |$. On a $< tx + uy, tx + uy > \geqslant 0$, $\forall t \in \mathbb{R}$.
En développant, on trouve $t^2 < x, x > + tu < x, y > + t\bar{u} < y, x > + u\bar{u} < y, y > \geqslant 0$,
c'est-à-dire $t^2 < x, x > + 2t\overline{< x, y >} + < y, y > \geqslant 0$, $\forall t \in \mathbb{R}$. Le discriminant est négatif...

(6.18) Merci à Meu pour cette réponse :

Un élément d'ordre 2 du groupe orthogonal est une symétrie orthogonale. Une symétrie orthogonale commute avec tout élément du groupe orthogonal si et seulement si son espace fixe est stable par tout élément du groupe orthogonal ; il n'y a que l'espace nul pour qui ça arrive, auquel cas la symétrie est la symétrie par rapport à l'origine. Le seul sous-groupe distingué à deux éléments du groupe orthogonal est donc $\{\pm 1\}$.
Si n est pair, $\{\pm 1\} \subset \mathrm{SO}(n,\mathbb{R})$ et donc $\mathrm{O}(n,\mathbb{R})$ ne peut être isomorphe à $\mathrm{SO}(n,\mathbb{R}) \times \mathbb{Z}/2\mathbb{Z}$ car ce dernier a au moins deux sous-groupes distingués d'ordre 2.
Si n est impair, on a bien la structure de produit direct donné par l'isomorphisme

$$\begin{array}{rcl} \mathrm{O}(n,\mathbb{R}) & \longrightarrow & \mathrm{SO}(n,\mathbb{R}) \times \{\pm 1\} \\ u & \longmapsto & (\det(u)\, u, \det(u)) \end{array}$$

En relation avec ceci, on peut remarquer que le groupe des isométries d'un polyèdre régulier de dimension 3 est isomorphe au produit direct de son groupe de rotations par $\mathbb{Z}/2\mathbb{Z}$ si et seulement s'il présente une symétrie centrale, ce qui est le cas de quatre sur cinq.

Références

[Del] Delcourt. Théorie des groupes, *Dunod*.

[FGN1] Francinou, Gianella, Nicolas. Exercices de Mathématiques Oraux X-ENS, Algèbre 1, *Cassini, 2007* .

[FGN2] Francinou, Gianella, Nicolas. Exercices de Mathématiques Oraux X-ENS, Algèbre 2, *Cassini, 2006*.

[FGN3] Francinou, Gianella, Nicolas. Exercices de Mathématiques Oraux X-ENS, Algèbre 3, *Cassini, 2008*.

[FG] Francinou, Gianella. Exercices de Mathématiques pour l'Agrégation, *Masson*.

[Gou] Gourdon. Les Maths en tête, Mathématiques pour M', *Ellipses* (1994).

[Goz] Gozard. Théorie de Galois, *Ellipses*.

[Hau] Hauchecorne. Les contre-exemples en Mathématiques, *Ellipses*.

[OA] Beck, Mallick, Peyré. Objectif Agrégation, *Ellipses*.

[Ort] Ortiz. Exerices d'Algèbre, *Ellipses*.

[Per] Perrin. Cours d'Algèbre, *Ellipses*.

[Tau] Tauvel. Cours d'Algèbre, *Dunod*.

[Tau-ex] Tauvel. Exercices de Mathématiques pour l'Agrégation, *Masson*.