Enoncés : Michel Emsalem,
Corrections : Pierre Dèbes

Action de groupe

Exercice 1

Soit $\sigma \in S_5$ défini par

$$\sigma = \begin{matrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{matrix}$$

(a) Ecrire la décomposition de σ en produit de cycles de supports disjoints. Quelle est la signature de σ ?

(b) Donner la liste des éléments de $<\sigma>$. Déterminer $<\sigma> \cap A_5$.

Indication ▼ [002166]

Exercice 2

(a) Montrer que le produit de deux transpositions distinctes est un 3-cycle ou un produit de deux 3-cycles. En déduire que A_n est engendré par les 3-cycles.

(b) Montrer que $A_n =< (123), (124), \dots, (12n) >$.

Correction ▼ [002167]

Exercice 3

On appelle cycle une permutation σ vérifiant la propriété suivante : il existe une partition de $\{1, \dots, n\}$ en deux sous-ensembles I et J tels que la restriction de σ à I est l'identité de I et il existe $a \in J$ tel que $J = \{a, \sigma(a), \dots, \sigma^{r-1}(a)\}$ où r est le cardinal de J. Le sous-ensemble J est appelé le support du cycle σ.
Un tel cycle sera noté $(a, \sigma(a), \dots, \sigma^{r-1}(a))$

(a) Soit $\sigma \in S_n$ une permutation. On considère le sous-groupe C engendré par σ dans S_n. Montrer que la restriction de σ à chacune des orbites de $\{1, \dots, n\}$ sous l'action de C est un cycle, que ces différents cycles commutent entre eux, et que σ est le produit de ces cycles.

(b) Décomposer en cycles les permutations suivantes de $\{1, \dots, 7\}$:

$$\begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 7 & 2 & 1 & 4 & 5 \end{matrix} \qquad \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 4 & 2 & 3 & 5 & 6 & 1 \end{matrix} \qquad \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 7 & 2 & 4 & 5 & 6 \end{matrix}$$

(c) Montrer que si σ est un cycle, $\sigma = (a, \sigma(a), \dots, \sigma^{r-1}(a))$, la conjuguée $\tau\sigma\tau^{-1}$ est un cycle et que $\tau\sigma\tau^{-1} = (\tau(a), \tau(\sigma(a)), \dots, \tau(\sigma^{r-1}(a)))$.

(d) Déterminer toutes les classes de conjugaison des permutations dans S_5 (on considérera leur décomposition en cycles). Déterminer tous les sous-groupes distingués de S_5.

Indication ▼ [002168]

Exercice 4

Montrer que les permutations circulaires engendrent S_n si n est pair, et A_n si n est impair.

Correction ▼ [002169]

Exercice 5

Soit I un sous-ensemble de $\{1, \dots, n\}$ et σ un cycle de support I. Soit τ une autre permutation. Montrer que τ commute avec σ si et seulement si τ laisse invariant I et la restriction de τ à I est égale à une puissance de la restriction de σ à I.

Correction ▼ [002170]

Exercice 6

Soit H un sous-groupe distingué de S_n contenant une transposition. Montrer que $H = S_n$.

Correction ▼ [002171]

Exercice 7

Dans le groupe symétrique S_4 on considère les sous-ensembles suivants :

$$H = \{\sigma \in S_4 \mid \sigma(\{1,2\}) = \{1,2\}\}$$

$$K = \{\sigma \in S_4 \mid \forall a,b \quad a \equiv b \ [\mathrm{mod}\ 2] \Rightarrow \sigma(a) \equiv \sigma(b) \ [\mathrm{mod}\ 2]\}$$

Montrer que H et K sont des sous-groupes de S_4. Les décrire.

Correction ▼ [002172]

Exercice 8

Montrer que l'ordre d'une permutation impaire est un nombre pair.

Indication ▼ [002173]

Exercice 9

Montrer que toute permutation d'ordre 10 dans S_8 est impaire.

Correction ▼ [002174]

Exercice 10

(a) Montrer que tout 3-cycle est un carré. En déduire que le groupe alterné A_n est engendré par les carrés de permutations.

(b) Montrer que A_n est le seul sous-groupe de S_n d'indice 2.

Correction ▼ [002175]

Exercice 11

Trouver toutes les classes de conjugaison de S_4. Donner la liste des sous-groupes distingués de S_4.

Correction ▼ [002176]

Exercice 12

Etant donnés un groupe G et un sous-groupe H, on définit le normalisateur $\mathrm{Nor}_G(H)$ de H dans G comme l'ensemble des éléments $g \in G$ tels que $gHg^{-1} = H$.

(a) Montrer que $\mathrm{Nor}_G(H)$ est le plus grand sous-groupe de G contenant H comme sous-groupe distingué.

(b) Montrer que le nombre de sous-groupes distincts conjugués de H dans G est égal à l'indice $[G : \mathrm{Nor}_G(H)]$ et qu'en particulier c'est un diviseur de l'ordre de G.

Indication ▼ [002177]

Exercice 13

Montrer que pour $m \geq 3$, un groupe simple d'ordre $\geq m!$ ne peut avoir de sous-groupe d'indice m.

Indication ▼ Correction ▼ [002178]

Exercice 14

Soit G un groupe et H un sous-groupe d'indice fini n. Montrer que l'intersection H' des conjugués de H par les éléments de G est un sous-groupe distingué de G et d'indice fini dans G. Montrer que c'est le plus grand sous-groupe distingué de G contenu dans H.

Indication ▼ [002179]

Exercice 15

a) Montrer qu'un groupe G vérifiant

$$\forall a,b \in G \quad a^2b^2 = (ab)^2$$

est commutatif.

(b) Le but de cette question est de donner un exemple de groupe G vérifiant la propriété

$$\forall a,b \in G \quad a^3b^3 = (ab)^3$$

et qui n'est pas commutatif.

(i) montrer qu'il existe un automorphisme σ de $\mathbb{F}_3^2$ d'ordre 3.

(ii) montrer que le groupe G défini comme le produit semi-direct de $\mathbb{F}_3^2$ par $\mathbb{Z}_3$, $\mathbb{Z}_3$ agissant sur $\mathbb{F}_3^2$ via σ répond à la question.

Correction ▼ [002180]

Exercice 16

Soient G un groupe et H un sous-groupe d'indice fini dans G. On définit sur G la relation xRy si et seulement si $x \in HyH$.

(a) Montrer que R est une relation d'équivalence et que toute classe d'équivalence pour la relation R est une union finie disjointe de classes à gauche modulo H.

Soit $HxH = \bigcup_{1 \leq i \leq d(x)} x_iH$ la partition de la classe HxH en classes à gauche distinctes.

(b) Soit $h \in H$ et i un entier compris entre 1 et $d(x)$; posons $h * x_iH = hx_iH$. Montrer que cette formule définit une action transitive de H sur l'ensemble des classes $x_1H, \dots, x_{d(x)}H$ et que le fixateur de x_iH dans cette action est $H \cap x_iHx_i^{-1}$. En déduire que

$$d(x) = [H : H \cap xHx^{-1}]$$

et qu'en particulier $d(x)$ divise l'ordre de G.

(c) Montrer que H est distingué dans G si et seulement si $d(x) = 1$ pour tout $x \in G$.

(d) On suppose que G est fini et que $[G : H] = p$, où p est le plus petit nombre premier divisant l'ordre de G. Le but de cette question est de montrer que H est distingué dans G.

(i) Montrer que pour tout $x \in G$, $d(x) \leq p$. En déduire que $d(x) = 1$ ou $d(x) = p$.

(ii) Montrer que si H n'est pas distingué dans G, il existe une unique classe d'équivalence pour la relation R et que $G = H$, ce qui contredit l'hypothèse $[G : H] = p$.

Correction ▼ [002181]

Exercice 17

Soit G un groupe fini agissant sur un ensemble fini X.

(a) On suppose que toute orbite contient au moins deux éléments, que $|G| = 15$ et que $\mathrm{card}(X) = 17$. Déterminer le nombre d'orbites et le cardinal de chacune.

(b) On suppose que $|G| = 33$ et $\mathrm{card}(X) = 19$. Montrer qu'il existe au moins une orbite réduite à un élément.

Correction ▼ [002182]

Exercice 18

(a) Soit G un groupe et H un sous-groupe. Montrer que la formule

$$g.g'H = gg'H$$

définit une action de G sur l'ensemble quotient G/H. Déterminer le fixateur d'une classe gH.

(b) Soit G un groupe et X et Y deux ensembles sur lesquels G agit (on parlera de G-ensembles). Soit f une application de X dans Y. On dira que f est compatible à l'action de G (ou que f est un morphisme de G-ensembles) si pour tout élément x de X et tout g dans G, $f(g.x) = g.f(x)$. Montrer que si f est bijective et compatible à l'action de G il en est de même de f^{-1}. On dira dans ce cas que f est un isomorphisme de G-ensembles.

(c) Soit G un groupe agissant transitivement sur un ensemble X (i.e. pour tout couple d'éléments x et y de X il existe au moins un élément g du groupe tel que $g.x = y$). Montrer qu'il existe un sous-groupe H de G tel que X soit isomorphe en tant que G-ensemble à G/H (on prendra pour H le fixateur d'un point quelconque de X).

(d) i) Soit H et K deux sous-groupes de G. Montrer qu'il existe une application f de G/H vers G/K compatible avec l'action de G si et seulement si H est contenu dans un conjugué de K. Montrer que dans ce cas f est surjective. Montrer que G/H et G/K sont isomorphes en tant que G-ensembles si et seulement si H et K sont conjugués dans G.

ii) Soit X et Y deux G-ensembles transitifs. Montrer qu'il existe une application de X vers Y compatible avec l'action de G si et seulement si il existe deux éléments x et y de X et Y tels que le fixateur de x soit contenu dans un conjugué du fixateur de y. Montrer que X et Y sont isomorphes si et seulement si les fixateurs de x et de y sont conjugués dans G.

Correction ▼ [002183]

Exercice 19

Soit G un groupe fini et X un G-ensemble transitif. On dira que X est *imprimitif* si X admet une partition $X = \bigcup_{1\leq i\leq r} X_i$ telle que tout élément g de G respecte cette partition, i.e. envoie un sous-ensemble X_i sur un sous-ensemble X_k (éventuellement $k = i$) et telle que $2 \leq r$ et les parties X_i ne sont pas réduites à un élément. Dans le cas contraire on dit que X est *primitif*.

(a) Montrer que dans la décomposition précédente, si elle existe, tous les sous-ensembles X_i ont même nombre m d'éléments.

(b) Soit H un sous-groupe de G. Montrer que G/H est imprimitif si et seulement s'il existe un sous-groupe propre K de G différent de H tel que $H \subset K \subset G$ (on regardera la partition de G/H en classes modulo K).

(c) Déduire de ce qui précède que X est primitif si et seulement si le fixateur d'un élément x de X est maximal parmi les sous-groupes propres de G.

(d) On suppose ici que X est primitif et que H est un sous-groupe distingué de G dont l'action n'est pas triviale sur X. Montrer qu'alors H agit transitivement sur X.

Indication ▼ Correction ▼ [002184]

Exercice 20

Montrer qu'un sous-groupe primitif de S_n qui contient une transposition est S_n tout entier.

Indication ▼ Correction ▼ [002185]

Exercice 21

Soit G un groupe fini et X un G-ensemble. Si k est un entier $(1 \leq k)$, on dit que X est k-transitif, si pour tout couple de k-uplets $(x_1,\dots,x_k)$ et $(y_1,\dots,y_k)$ d'éléments de X distincts deux à deux, il existe au moins un élément g de G tel que pour tout i, $1 \leq i \leq k$, $g.x_i = y_i$. Un G-ensemble 1-transitif est donc simplement un G-ensemble transitif.

(a) Montrer que si X est k-transitif, il est aussi l-transitif pour tout l, $1 \leq l \leq k$.

(b) Montrer que X est 2-transitif si et seulement si le fixateur d'un élément x de X agit transitivement sur $X \setminus \{x\}$.
(c) Montrer que si X est imprimitif, il n'est pas 2-transitif.

(d) Montrer qu'un groupe cyclique C d'ordre premier considéré comme C-ensemble par l'action de translation de C sur lui-même, est primitif mais n'est pas 2-transitif.

(e) Montrer que l'ensemble $\{1,\dots,n\}$ muni de l'action du groupe S_n est k-transitif pour tout k, $1 \leq k \leq n$. En déduire que l'ensemble $\{1,\dots,n\}$ muni de l'action du groupe S_n est primitif.

(f) Montrer que le fixateur de 1 dans S_n est isomorphe à S_{n-1}. Dans la suite on identifie S_{n-1} à ce fixateur. Déduire de l'exercice 19 que S_{n-1} est un sous-groupe propre maximal de S_n.

Indication ▼ [002186]

Exercice 22

Décrire le groupe D_n des isométries du plan affine euclidien qui laissent invariant un polygone régulier à n côtés. Montrer que D_n est engendré par deux éléments σ et τ qui vérifient les relations : $\sigma^n = 1$, $\tau^2 = 1$ et $\tau\sigma\tau^{-1} = \sigma^{-1}$. Quel est l'ordre de D_n ? Déterminer le centre de D_n. Montrer que $D_3 \simeq S_3$.

Indication ▼ [002187]

Exercice 23

Montrer que le groupe des isométries de l'espace affine euclidien de dimension 3 qui laissent invariant un tétraèdre régulier de sommets a_1, a_2, a_3, a_4 est isomorphe à S_4 et que le sous-groupe des isométries directes qui laissent invariant le tétraèdre est isomorphe à A_4.

Correction ▼ [002188]

Exercice 24

Déterminer le groupe des isométries de l'espace affine euclidien de dimension 3 qui laissent invariant un cube.
[002189]

Indication pour l'exercice 1 ▲

Aucune difficulté.

Indication pour l'exercice 3 ▲

(a) est une simple vérification.

(b) Les trois permutations s'écrivent respectivement $(1\,3\,7\,5)\,(2\,6\,4)$, $(1\,7)\,(2\,4\,3)$ et $(2\,3\,7\,6\,5\,4)$.

(c) est une simple vérification.

(d) **Rappel :** De façon générale, on dit qu'une permutation $\omega \in S_n$ est de type $1^{r_1}\text{-}2^{r_2}\text{-}\cdots\text{-}d^{r_d}$ où $d, r_1, \ldots, r_d$ sont des entiers ≥ 0 tels que $r_1 + \cdots + r_d = n$, si dans la décomposition de ω en cycles à support disjoints, figurent r_1 1-cycles (ou points fixes), r_2 2-cycles, ... et r_d d-cycles. En utilisant la question (c), il n'est pas difficile de montrer que deux permutations sont conjuguées dans S_n si et seulement si elles sont de même type. Les classes de conjugaison de S_n correspondent donc exactement à tous les types possibles.

On obtient ainsi facilement les classes de conjugaison de S_5. Soit maintenant H un sous-groupe distingué non trivial de S_5. Dès que H contient un élément de S_5, il contient sa classe de conjugaison ; H est donc une réunion de classes de conjugaison. En considérant toutes les classes possibles que peut contenir H, on montre que $H = A_5$ ou $H = S_5$. Par exemple, si H contient la classe 1-2-2, alors H contient $(1\,2)\,(3\,4) \times (1\,3)\,(2\,5) = (1\,4\,3\,2\,5)$ et donc la classe des 5-cycles. D'après l'exercice 2, H contient alors A_5. Le groupe H est donc A_5 ou S_5. Les autres cas sont similaires.

Indication pour l'exercice 8 ▲

Une puissance impaire d'une permutation impaire ne peut pas être égale à 1.

Indication pour l'exercice 12 ▲

(a) Aucune difficulté.
(b) Le nombre cherché est l'orbite de H sous l'action de G par conjugaison sur ses sous-groupes et $\mathrm{Nor}_G(H)$ est le fixateur de H pour cette action.

Indication pour l'exercice 13 ▲

Etudier l'action du groupe par translation sur l'ensemble quotient des classes modulo le sous-groupe.

Indication pour l'exercice 14 ▲

Le seul point non immédiat est que H' est d'indice fini dans G. Pour cela considérer le morphisme de G à valeurs dans le groupe des permutations des classes à gauche de G modulo H, qui à $g \in G$ associe la permutation $aH \to gaH$ et montrer que le noyau de ce morphisme est le groupe H'.

Indication pour l'exercice 19 ▲

Question (d) : Si K le fixateur d'un élément $x \in X$, alors K est un sous-groupe propre maximal de G et X est isomorphe à $G/\cdot K$ en tant que G-ensemble. Déduire du fait que H n'est pas contenu dans K que $HK = G$ et que $H/\cdot H \cap K \simeq G/\cdot K$.

Indication pour l'exercice 20 ▲

Soit H un tel sous-groupe. On peut supposer sans perte de généralité que H contient la transposition (12). On pourra ensuite procéder comme suit.
- montrer que H est engendré par le fixateur H_1 de 1 et par (12).
- montrer que l'orbite de 2 sous H est l'union de l'orbite de 2 sous H_1 et de 1.
- en déduire que H_1 agit transitivement sur l'ensemble $\{2, \ldots, n\}$ et que H agit 2-transitivement sur $\{1, \ldots, n\}$.
- déduire du point précédent que H contient toutes les transpositions.

Indication pour **l'exercice 21 ▲**

(a) est trivial.

(b) : Noter d'abord que la condition sur le fixateur de x est indépendante de $x \in X$: en effet si g est un élément de G envoyant x sur un autre élément $x' \in X$ (qui existe par transitivité de G), alors $G(x') = gG(x)g^{-1}$ et la correspondance $h \to ghg^{-1}$ permet d'identifier les actions de $G(x')$ sur $X \setminus \{x'\}$ et celle de $G(x)$ sur $X \setminus \{x\}$. Supposons maintenant vérifiée la condition sur le fixateur de x. Si (x,y) et (x',y') sont deux couples d'éléments distincts de X, il existe $\sigma \in G$ tel que $\sigma(x) = x'$ (transitivité de G) et il existe $\tau \in G$ tel que $\tau(x') = x'$ et $\tau(\sigma(y)) = y'$ (transitivité de $G(x')$ sur $X \setminus \{x'\}$ (noter que $\sigma(y) \neq x'$ car $\sigma(x) = x'$)). La permutation $\tau\sigma$ vérifie $\tau\sigma(x) = x'$ et $\tau\sigma(y) = y'$. Cela montre que X est 2-transitif. La réciproque est triviale.

(c) Si l'action de G sur X est imprimitive et $X = \bigcup_{i=1}^{r} X_i$ est une partition de X comme dans la définition, alors il n'existe pas d'élément $g \in G$ envoyant un premier élément $x_1 \in X_1$ dans X_1 et un second élément $x_1' \in X_1$ dans X_2.

(d) L'action par translation d'un groupe cyclique C sur lui-même est transitive, elle est primitive si $|C|$ est premier (toute partition de C en sous-ensembles de même cardinal est forcément triviale) mais elle n'est pas 2-transitive (le fixateur de tout élément est trivial, ce qui contredit le (c) de l'exercice 19).

(e) et (f) ne présentent aucune difficulté.

Indication pour **l'exercice 22 ▲**

On se ramène à la situation où le polygone est inscrit dans le plan complexe et a pour sommets les racines de l'unité $e^{2ik\pi/n}, k = 0, 1, \ldots, n-1$. Une isométrie laissant invariant le polygone fixe nécessairement l'origine. Elle est donc de la forme $z \to az$ ou $z \to a\bar{z}$ avec $|a| = 1$. On voit ensuite que a est nécessairement une racine n-ième de 1. Notons σ l'isométrie $z \to e^{2i\pi/n}z$ et τ la conjugaison complexe. On a $D_n = \{\sigma^k\tau^\varepsilon \mid k = 0, \ldots, n-1, \varepsilon = \pm 1\}$. On vérifie que σ et τ engendrent le groupe D_n et satisfont les relations $\sigma^n = 1$, $\tau^2 = 1$ et $\tau\sigma\tau^{-1} = \sigma^{-1}$. Autrement dit, D_n est isomorphe au groupe diédral d'ordre $2n$. Si n est impair, son centre est trivial et si $n = 2m$ est pair, son centre est $\{1, \sigma^m\}$. Le groupe D_n se plonge naturellement dans S_n ; comme $|D_3| = |S_3| = 6$, ce plongement est un isomorphisme pour $n = 3$.

Correction de l'exercice 2 ▲

(a) On vérifie les deux formules : $(a\,b)(b\,c) = (a\,b\,c)$ pour a,b,c distincts, et $(a\,b)(c\,d) = (a\,b)(b\,c)(b\,c)(c\,d) = (a\,b\,c)(b\,c\,d)$, pour a,b,c,d distincts. On déduit que toute permutation paire, produit d'un nombre pair de transpositions, peut s'écrire comme produit de 3-cycles. Le groupe alterné A_n est donc engendré par les 3-cycles si $n \geq 3$.

(b) On a $(1\,2\,j)\,(1\,2\,i)\,(1\,2\,j)^{-1} = (2\,j\,i)$ pour i,j distincts et différents de 1 et 2, et si en plus k est différent de $1,2,i,j$, on a $(1\,2\,k)\,(2\,j\,i)\,(1\,2\,k)^{-1} = (k\,j\,i)$. Le groupe engendré par les 3-cycles $(1\,2\,i)$ où $i \geq 3$ contient donc tous les 3-cycles ; d'après (a), c'est le groupe alterné A_n.

Correction de l'exercice 4 ▲

Les cas $n = 1$ et $n = 2$ sont immédiats. On peut supposer $n \geq 3$. On vérifie aisément la formule $(a_1\,a_2\,\ldots\,a_{n-1}\,a_n)\,(a_{n-1}\,a_n\,a_{n-}$ $(a_1\,a_n\,a_{n-1})$ où $a_1,\ldots,a_n$ sont les éléments d'un ensemble de cardinal n. On en déduit que le groupe PC_n engendré par les permutations circulaires contient les 3-cycles et donc le groupe alterné A_n (voir exercice 2). Les permutations circulaires sont de signature $(-1)^{n-1}$. Si n est impair, elles sont donc paires d'où $PC_n \subset A_n$ et donc finalement $PC_n = A_n$ dans ce cas. Si n pair, les permutations circulaires sont impaires, donc $PC_n \neq A_n$. L'indice de PC_n dans S_n devant diviser 2 (puisque $PC_n \supset A_n$), il vaut 1, c'est-à-dire $PC_n = S_n$.

Correction de l'exercice 5 ▲

Supposons $\sigma\tau = \tau\sigma$. Pour tout $x \notin I$, on a $\sigma(\tau(x)) = \tau(\sigma(x)) = \tau(x)$; $\tau(x)$, fixé par σ, n'appartient pas à I. Cela montre que le complémentaire de I est invariant par τ. Comme τ est injective, I l'est aussi. Montrons que, sur I, τ est égal à une puissance de σ. Quitte à renuméroter $\{1,\ldots,n\}$, on peut supposer que $I = \{1,\ldots,m\}$ (où $m \leq n$) et $\sigma|_I = (1\,2\,\ldots\,m)$. L'entier $\tau(1)$ est dans I ; soit k l'unique entier entre 1 et m tel que $\tau(1) = \sigma^k(1)$. Pour tout $i \in I$, on a alors $\tau(i) = \tau\sigma^{i-1}(1) = \sigma^{i-1}\tau(1) = \sigma^{i-1}\sigma^k(1) = \sigma^k\sigma^{i-1}(1) = \sigma^k(i)$ (l'identité $\tau\sigma^{i-1} = \sigma^{i-1}\tau$ utilisée dans le calcul découle facilement de l'hypothèse $\sigma\tau = \tau\sigma$). On obtient donc $\tau|_I = (\sigma|_I)^k$. L'implication réciproque est facile.

Correction de l'exercice 6 ▲

Un sous-groupe distingué de S_n qui contient une transposition contient toute sa classe de conjugaison, c'est-à-dire, toutes les transpositions (cf les indications de l'exercice 3, "Rappel") et donc le groupe qu'elles engendrent, c'est-à-dire S_n.

Correction de l'exercice 7 ▲

L'ensemble H est le sous-groupe de S_4 fixant la paire $\{1,2\}$. Tout élément de H fixe aussi la paire $\{3,4\}$. Cela fournit un morphisme $H \to S_2 \times S_2$ qui est clairement bijectif. D'où $H \simeq S_2 \times S_2 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

On a $\sigma \in K$ si et seulement si $\sigma(1) \equiv \sigma(3)$ [mod 2] et $\sigma(2) \equiv \sigma(4)$ [mod 2], c'est-à-dire si et seulement si $\sigma(\{1,3\})$ est soit la paire $\{1,3\}$ soit la paire $\{2,4\}$ (auquel cas $\sigma(\{2,4\})$ est la paire $\{2,4\}$ ou la paire $\{1,3\}$ respectivement). Grâce à l'identité $\sigma\,(1\,3)\,(2\,4)\,\sigma^{-1} = (\sigma(1)\,\sigma(3))\,(\sigma(2)\,\sigma(4))$, on voit que la condition est également équivalente au fait que la conjugaison par σ stabilise la permutation $(1\,3)\,(2\,4)$. Autrement dit K est le sous-groupe des éléments de S_4 commutant avec $(1\,3)\,(2\,4)$. La classe de conjugaison 2-2 ayant 3 éléments, le groupe H est d'ordre $4!/3 = 8$. On peut dresser la liste de ses éléments : si $\omega = (1\,2\,3\,4)$ et $\tau = (1\,2)\,(3\,4)$, alors $K = \{1,\omega,\omega^2,\omega^3,\tau,\omega\tau,\omega^2\tau,\omega^3\tau\}$. On vérifie les relations $\sigma^4 = 1$, $\tau^2 = 1$ et $\tau\sigma\tau^{-1} = \sigma^{-1}$. Le groupe K est égal au produit semi-direct de son sous-groupe distingué $< \omega >$ par son sous-groupe $< \tau >$ et est donc isomorphe au groupe diédral d'ordre 8.

Correction de l'exercice 9 ▲

L'ordre d'une permutation $\omega \in S_n$ est le ppcm des longueurs des cycles de la décomposition de ω en cycles à supports disjoints. De plus, la somme des longueurs de ces cycles (ceux de longueur 1 y compris) vaut n. Pour une permutation d'ordre 10 dans S_8, il n'y a qu'un type possible : 5-2-1. La signature vaut alors $(-1)^{5-1}(-1)^{2-1} = -1$.

Correction de l'exercice 10 ▲

(a) Un 3-cycle ω est d'ordre 3 et vérifie donc $\omega^3 = 1$ soit encore $\omega = (\omega^2)^2$. Le groupe engendré par tous les carrés de permutations dans S_n contient donc tous les 3-cycles, et donc aussi le groupe qu'ils engendrent, c'est-à-dire A_n. L'autre inclusion est facile puisque le carré d'une permutation est toujours une permutation paire.

(b) Si H est un sous-groupe d'indice 2 de S_n, il est distingué. On a alors $\sigma^2 \in H$ pour tout $\sigma \in S_n$ (cf exercice **??**). D'après la question (a), $H = A_n$.

Correction de l'exercice 11 ▲

Les classes de conjugaison de S_n correspondent aux types possibles d'une permutation de n éléments (cf indication exercice 3 Rappel). Pour $n = 4$, on a 5 classes : 1-1-1-1, 2-1-1, 2-2, 3-1 et 4.

Soit H un sous-groupe distingué non trivial de S_4. Si H contient la classe 2-1-1 (transpositions), alors $H = S_4$. Si H contient la classe 3-1, alors $H \supset A_4$ (cf exercice 2) et donc $H = A_4$ ou $H = S_4$. Si H contient la classe 4, alors $H = S_4$ (cf exercice 4). Si H contient la classe 2-2, alors $H \supset V_4$ (voir la correction de l'exercice **??** définition de V_4), ce qui donne $H = V_4$ ou bien, au vu des cas précédents, $H = A_4$ ou $H = S_4$. Les sous-groupes distingués de S_4 sont donc $\{1\}$, V_4, A_4 et S_4.

Correction de l'exercice 13 ▲

Soit H un sous-groupe d'indice m d'un groupe G. L'action de G par translation à gauche sur l'ensemble quotient G/H des classes à gauche modulo H induit un morphisme $G \to \mathrm{Per}(G/H)$ qui est non-trivial et donc est injectif puisque le noyau, distingué dans G, ne peut être trivial si G est simple. L'ordre de G doit donc diviser l'ordre du groupe $\mathrm{Per}(G/H)$ qui vaut $m!$. Il faut nécessairement que $|G| = m!$. Mais alors le morphisme précédent est un isomorphisme et G est isomorphe au groupe symétrique S_m, ce qui contredit la simplicité de G.

Correction de l'exercice 15 ▲

(a) L'identité $a^2b^2 = (ab)^2$, par simplification à gauche par a et à droite par b, se réécrit $ab = ba$.

(b) La correspondance $(x,y) \to (x+y,y)$ définit un automorphisme σ de $\mathbb{F}_3^2$ d'ordre 3. Identifions le groupe $<\sigma>$ au groupe $\mathbb{Z}/3\mathbb{Z}$ et considérons le produit semi-direct $\mathbb{F}_3^2 \rtimes \mathbb{Z}/3\mathbb{Z}$. Pour tout élément $((x,y),i)$, on a $((x,y),i)^2 = ((x,y)+\sigma^i(x,y),2i)$ et $((x,y),i)^3 = ((x,y)+\sigma^i(x,y)+\sigma^{2i}(x,y),3i) = ((0,0),0)$ puisque $(\mathrm{Id}+\sigma^i+\sigma^{2i})(x,y) = (3x+iy+2iy,3y) = (0,0)$. La formule $a^3b^3 = (ab)^3$ est donc satisfaite pour tous a,b dans $\mathbb{F}_3^2 \rtimes \mathbb{Z}/3\mathbb{Z}$. Mais ce produit semi-direct n'est pas commutatif car l'action de $\mathbb{Z}/3\mathbb{Z}$ n'est pas l'action triviale.

Correction de l'exercice 16 ▲

(a) Que R soit une relation d'équivalence est immédiat. La classe d'un élément $x \in G$ est l'ensemble HxH, lequel est égal à la réunion des ensembles hxH où h décrit H. Ces derniers ensembles sont des classes à gauche modulo H et sont donc égaux ou disjoints.

(b) Pour tout $i = 1,\ldots,d(x)$, hx_iH est une classe à gauche, contenue dans $h(HxH)H \subset HxH$, donc est de la forme x_jH. La formule $h * x_iH = hx_iH$ définit ainsi une permutation de l'ensemble des classes $x_1H,\ldots,x_{d(x)}H$ (la permutation réciproque est celle induite par h^{-1}) et donc une action de H sur cet ensemble. Cette action est transitive : pour $i,j \in \{1,\ldots,d(x)\}$, $h = x_i^{-1}x_j$ vérifie $h * x_iH = x_jH$.

Un élément $h \in H$ est dans le fixateur $H(x_iH)$ d'une classe x_iH si et seulement si $hx_iH = x_iH$ c'est-à-dire si $h \in x_iHx_i^{-1}$. D'où $H(x_iH) = H \cap x_iHx_i^{-1}$. On obtient alors $d(x) = [H : (H \cap x_iHx_i^{-1})]$ ce qui prouve que $d(x)$ divise $|H|$ et donc aussi $|G|$.

(c) Si H est distingué dans G, alors classes à droite et classes à gauche modulo H coincident d'où $HxH = xHH = xH$ et donc $d(x) = 1$ pour tout $x \in G$. Inversement, pour tout $x \in G$, si $d(x) = 1$, alors $HxH = xH$ ce qui entraine $Hx \subset xH$ et donc $x^{-1}Hx \subset H$.

(d) (i) De façon générale, on a $d(x) \leq [G : H]$. On a ainsi $d(x) \leq p$ si $[G : H] = p$. Comme $d(x)$ divise $|G|$ et que p est le plus petit premier divisant $|G|$, nécessairement $d(x) = 1$ ou $d(x) = p$.

(ii) Si H n'est pas distingué alors il existe $x \in G$ avec $d(x) \neq 1$ et donc $d(x) = p$. Mais alors $\mathrm{card}(HxH) = d(x)\,|H| = p\,|H| = [G : H]\,|H| = |G|$. C'est-à-dire, il n'existe qu'une seule classe $HxH = G$, laquelle est aussi la classe de l'élément neutre $H1H = H$, ce qui contredit l'hypothèse $[G:H] = p > 1$. Conclusion : le sous-groupe H est distingué dans G.

Correction de l'exercice 17 ▲

Toute orbite $\mathscr{O} = \mathscr{O}_x$ d'un élément $x \in X$ est en bijection avec l'ensemble $G/\cdot G(x)$ des classes à gauche de G modulo le fixateur $G(x)$ de G. En particulier, le cardinal de $\mathscr{O}$ divise l'ordre de G. De plus la somme des longueurs des orbites est égale au cardinal de l'ensemble X.

(a) Si $|G| = 15$, $\mathrm{card}(X) = 17$ et s'il n'y a pas d'orbite à un seul élément, il n'y a qu'une seule possibilité : 4 orbites de longueur 3 et une de longueur 5.

(b) Supposons $|G| = 33$ et $\mathrm{card}(X) = 19$. Aucune somme de diviseurs $\neq 1$ de 33 n'est égale à 19 donc nécessairement il existe au moins une orbite réduite à un élément.

Correction de l'exercice 18 ▲

(a) Si g'_1, g'_2 sont dans la même classe à gauche de G modulo H, c'est-à-dire, si $g'_1H = g'_2H$ ou encore si $(g'_2)^{-1}g'_1 \in H$ alors $(gg'_2)^{-1}(gg'_1) = (g'_2)^{-1}g'_1 \in H$: les classes gg'_1H et gg'_2H sont égales. Pour tous $g, g' \in H$, la classe $gg'H$ ne dépend donc pas du représentant choisi g' de la classe $g'H$; on peut la noter $g \cdot g'H$. On vérifie sans difficulté que la correspondance $(g, g'H) \to g \cdot g'H$ satisfait les autres conditions de la définition d'une action de G sur l'ensemble quotient $G/\cdot H$.

Pour $g, \gamma \in G$, on a $\gamma \cdot gH = gH$ si et seulement si $g^{-1}\gamma g \in H$ ce qui équivaut à $\gamma \in gHg^{-1}$. Le fixateur de la classe gH est le sous-groupe conjugué gHg^{-1} de H par g.

(b) Pour tout $y \in Y$ et tout $g \in G$, on a $f(g \cdot f^{-1}(y)) = g \cdot f(f^{-1}(y)) = g \cdot y$. En appliquant f^{-1}, on obtient $g \cdot f^{-1}(y) = f^{-1}(g \cdot y)$, ce qui montre que f^{-1} est compatible à l'action de G.

(c) Soit $x \in X$ fixé. Pour $g \in G$, l'élément $g \cdot x$ ne dépend que de la classe à gauche de g modulo le fixateur $G(x)$ de x. Cela permet de définir une application $G/\cdot G(x) \to X$: à chaque classe $gG(x)$ on associe $g \cdot x$. On montre sans difficulté que cette application est compatible avec l'action de G (vérification formelle), injective (par construction) et surjective (par l'hypothèse de transitivité) ; c'est donc un isomorphisme de G-ensembles.

(d) i) Supposons donnée une application $f : G/\cdot H \to G/\cdot K$ compatible avec l'action de G. Pour tout $h \in H$, on a $f(hH) = f(H) = h \cdot f(H)$. Ce qui, d'après la question (a), donne $h \in gKg^{-1}$, où g est un représentant de la classe $f(H)$ dans $G/\cdot K$.

Réciproquement, supposons $H \subset gKg^{-1}$ avec $g \in G$. Considérons l'application $\varphi : G/\cdot H \to G/\cdot K$ qui à toute classe γH associe la classe γgK. Cette application est bien définie : en effet, si $\gamma_2^{-1}\gamma_1 \in H$, alors $(\gamma_2 g)^{-1}\gamma_1 g = g^{-1}(\gamma_2^{-1}\gamma_1)g \in g^{-1}Hg \subset K$; la classe γgK ne dépend donc pas du représentant γ de la classe γH. De plus φ est compatible à l'action de G : pour tous $\gamma, \gamma' \in G$, on a $\varphi(\gamma' \cdot \gamma H) = \varphi(\gamma'\gamma H) = \gamma'\gamma gK = \gamma' \cdot \varphi(\gamma H)$.

Si $f : G/\cdot H \to G/\cdot K$ est compatible avec l'action de G, alors son image contient toute orbite dès qu'elle en contient un élément. Comme l'action de G sur sur $G/\cdot K$ ne possède qu'une orbite, l'image de f contient tout $G/\cdot K$: f est surjective.

D'après ce qui précède, les ensembles $G/\cdot H$ et $G/\cdot K$ sont isomorphes comme G-ensembles si et seulement si $H \subset gKg^{-1}$ avec $g \in G$ et $\mathrm{card}(G/\cdot H) = \mathrm{card}(G/\cdot K)$ ce qui équivaut à $H \subset gKg^{-1}$ et $|H| = |K|$ ou encore à $H = gKg^{-1}$.

ii) Il suffit de réécrire les résultats de la question précédente en remplaçant $G/\cdot H$ et $G/\cdot K$ par $G/\cdot G(x)$ et $G/\cdot G(y)$ qui, d'après la question (c) sont G-isomorphes à X et Y respectivement (où x et y sont des points fixés de X et Y respectivement).

Correction de l'exercice 19 ▲

(a) Pour $1 \leq i, j \leq r$ quelconques et $x_i, x_j \in X_i \times X_j$, il existe $g \in G$ tel que $g \cdot x_i = x_j$ (par transitivité de G). On a alors $g \cdot X_i = X_j$. En particulier $\mathrm{card}(X_i) = \mathrm{card}(g \cdot X_i) = \mathrm{card}(X_j)$.

(b) Si l'action de G sur $G/\cdot H$ est imprimitive, le sous-ensemble $K = \{g \in G \,|\, g \cdot X_1 = X_1\}$, où X_1 est par exemple celui des sous-ensembles $X_i \subset X$ qui contient la classe neutre H de $G/\cdot H$, est un sous-groupe propre de G ($K \neq G$ car G agissant transitivement, il existe $g \in G$ tel que $(g \cdot X_1) \cap X_2 \neq \emptyset$) et contenant strictement H (car encore par transitivité, il existe $g \in G$ tel que $g \cdot H$ soit un élément de X_1 (ce qui assure que $g \in K$) mais différent de H (ce qui assure que $g \notin H$)).

Inversement, si un tel sous-groupe K de G existe, la relation "$gH \sim g'H$ si $(g')^{-1}g \in K$" est bien définie sur $G/\cdot H$ (la définition ne dépend pas des représentants dans G des classes gH et $g'H$) et est une relation d'équivalence (immédiat). La partition associée de $G/\cdot H$ en classes d'équivalence vérifie les conditions de la définition d'imprimitivité (pour l'action de G sur $G/\cdot H$) : la partition est non triviale car K est strictement contenu entre H et K ; et si $(\gamma H)K$ est une de ces classes d'équivalence et $g \in G$, alors $g \cdot (\gamma H)K$ est la classe $(g\gamma H)K$: l'action de G permute bien les classes constituant la partition de X.

(c) D'après l'exercice 18, les ensembles X et $G/\cdot G(x)$ sont isomorphes comme G-ensembles. L'action de G sur X est primitive si et seulement si celle de G sur $G/\cdot G(x)$ l'est, ce qui, d'après la question précédente, équivaut à dire que le fixateur $G(x)$ est maximal parmi les sous-groupes de G.

(d) Soient $x \in X$ et $G(x)$ son fixateur. Le sous-groupe H étant distingué dans G, l'ensemble $HG(x)$ est un sous-groupe ; c'est le sous-groupe engendré par H et $G(x)$. De plus, l'action de H sur G n'étant pas triviale, H n'est pas contenu dans $G(x)$ et par conséquent $HG(x)$ contient strictement $G(x)$. D'après la question (c), il en résulte que $HG(x) = G$. On vérifie sans peine que l'application $H/\cdot(H \cap G(x)) \to (HG(x))/\cdot G(x)$ qui à toute classe $h(H \cap G(x))$ associe la classe $hG(x)$ est une bijection (ce qui généralise le théorème d'isomorphisme $HK/K \simeq H/(H \cap K)$ qui est vrai sous l'hypothèse supplémentaire "K distingué" (qui assure que les ensembles HK/K et $H/(H \cap K)$ sont des groupes et non de simples ensembles comme ici)). On obtient donc que les ensembles $H/\cdot(H \cap G(x))$ et $G/\cdot G(x)$ sont isomorphes comme G-ensembles (la compatibilité des actions est immédiate). Or ces deux ensembles sont en bijection avec les orbites de x sous H et sous G respectivement. Conclusion : l'action de H est, comme celle de G, transitive sur l'ensemble X.

Correction de l'exercice 20 ▲

Soit H un sous-groupe primitif de S_n contenant une transposition. On peut supposer que H contient la transposition $(1\,2)$. Le sous-groupe engendré par le fixateur $H(1)$ et $(1\,2)$ contient strictement $H(1)$. D'après l'exercice 19 (question (c)), ce groupe est H.

Considérons l'ensemble $\mathcal{O}$ réunion de l'orbite $H(1) \cdot 2$ de 2 sous $H(1)$ et du singleton $\{1\}$. Pour montrer que $\mathcal{O}$ est l'orbite de 2 sous H, il suffit de montrer que $2 \in \mathcal{O}$ (ce qui est clair) et que $\mathcal{O}$ est stable sous l'action de H, ou, ce qui est équivalent, stable sous l'action de $H(1)$ et de $(1\,2)$. L'élément 1 est envoyé sur $1 \in \mathcal{O}$ par les éléments de $H(1)$ et sur $2 \in \mathcal{O}$ par $(1\,2)$. L'ensemble $H(1) \cdot 2$ est invariant sous l'action de $H(1)$. Enfin, si $h \cdot 2$ désigne un élément quelconque de $H(1) \cdot 2$, alors son image par la permutation $(1\,2)$ est 2 si $h \cdot 2 = 1$, 1 si $h \cdot 2 = 2$ et $h \cdot 2$ si $h \cdot 2 \neq 1,2$; dans tous les cas, l'image est dans $\mathcal{O}$.

On a donc $\mathcal{O} = H \cdot 2 = H(1) \cdot 2 \cup \{1\}$. L'action de H étant transitive, cet ensemble est égal à $\{1,\dots,n\}$ et donc $H(1) \cdot 2 = \{2,\dots,n\}$ (puisque $1 \notin H(1) \cdot 2$). Cela montre que l'action de $H(1)$ sur $\{2,\dots,n\}$ est transitive, et donc que H agit transitivement sur $\{1,\dots,n\}$ (exercice 21).

Pour i, j entiers distincts entre 1 et n, choisissons alors $g \in G$ tel que $g(1) = i$ et $g(2) = j$. On a $g(1\,2)g^{-1} = (g(1)\,g(2)) = (i\,j)$. Cela montre que H contient toutes les transpositions. Conclusion : $H = S_n$.

Correction de l'exercice 23 ▲

Notons G le groupe des isométries de l'espace euclidien de dimension 3 laissant invariant l'ensemble $\{a_1,\dots,a_4\}$ des 4 sommets d'un tétraèdre régulier. Le fixateur $G(a_4)$ agit transitivement sur $\{a_1,a_2,a_3\}$: en effet ce sous-groupe contient la rotation d'axe la droite joignant a_4 au centre de gravité du triangle de sommets a_1,a_2,a_3, laquelle agit sur ces points comme un 3-cycle. D'après l'exercice 21, le groupe G agit 2-transitivement sur $\{a_1,\dots,a_4\}$. De plus $G(a_4)$ contient une isométrie agissant sur $\{a_1,\dots,a_4\}$ comme une transposition, par exemple la symétrie par rapport au plan médiateur P du segment $[a_1,a_2]$, laquelle échange a_1 et a_2 et fixe a_3 et a_4 qui sont dans P. D'après l'exercice 20, on a $G \simeq S_4$.

Notons G_+ le sous-groupe de G constitué de ses isométries directes. Le groupe G_+ est le noyau du morphisme $\det : G_+ \to \{1,-1\}$ qui à tout $g \in G$ vu comme matrice associe son déterminant. Comme ce morphisme est surjectif (la rotation et la symétrie considérées ci-dessus sont respectivement directe et indirecte), G_+ est d'indice 2. D'où $G \simeq A_4$ puisque A_4 est le seul sous-groupe de S_4 d'indice 2 (cf exercice 10).