Feuille 4

Exercice 1. [Actions de groupes, Dummit-Foot, page 117 exercice 6]
Soit R l'anneau des polynômes à quatre variables et coefficients dans $\mathbb{Z}$. Considérons l'action

$$\begin{array}{rcl} \mathcal{S}_4 \times R & \longrightarrow & R \\ (\sigma, p(x_1,x_2,x_3,x_4)) & \longmapsto & p(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_{\sigma(4)}). \end{array}$$

a) Déterminer l'orbite contenant $x_1 + x_2$.

b) Déterminer l'orbite contenant $x_1x_2 + x_3x_4$.

Éléments de solution 1.

Exercice 2. [Actions de groupes, Dummit-Foot, page 125 corollaire 9]

a) Soient G un groupe et $Z(\mathrm{G})$ son centre. Supposons que $\mathrm{G}/Z(\mathrm{G})$ soit cyclique. Montrer que G est abélien.

b) Soit p un nombre premier, soit G un groupe d'ordre p^2. Montrer que G est abélien.

Éléments de solution 2.

a) Soient G un groupe et $Z(\mathrm{G})$ son centre. Supposons que $\mathrm{G}/Z(\mathrm{G})$ soit cyclique. Montrons que G est abélien.
Rappelons que le centre $Z(\mathrm{G})$ de G est distingué. Considérons le morphisme quotient $\pi\colon G \to \mathrm{G}/Z(\mathrm{G})$. Par hypothèse $\mathrm{G}/Z(\mathrm{G})$ est engendré par un élément $\overline{g_0}$. Puisque π est surjective il existe $g_0 \in G$ tel que $\pi(g_0) = \overline{g_0}$. Soient g, h dans G. Il existe n, $m \in \mathbb{Z}$ tels que $\pi(g) = \overline{g_0}^n$ et $\pi(h) = \overline{g_0}^m$. Par suite $\pi(gg_0^{-n}) = \pi(hg_0^{-m}) = e$ et $y = gg_0^{-n}$, $z = gg_0^{-m}$ appartiennent à $Z(\mathrm{G})$. Alors

$$gh = yg_0^n z g_0^m = yzg_0^{n+m} = zg_0^m y g_0^n = hg$$

c'est-à-dire G est abélien.

b) L'équation aux classes pour l'action de G sur lui-même par conjugaison assure que le centre $Z(\mathrm{G})$ de G n'est pas réduit à l'élément neutre. En faisons agir G sur lui-même par conjugaison

$$\mathrm{G} \times \mathrm{G} \to \mathrm{G}, \qquad (g,h) \mapsto hgh^{-1}.$$

Notons que g appartient à $Z(\mathrm{G})$ si et seulement si l'orbite $\mathcal{O}_g$ de g sous cette action est réduite à $\{g\}$. L'équation aux classes assure que

$$|\mathrm{G}| = |Z(\mathrm{G})| + \sum_{i=1}^{r} |\mathcal{O}_{g_i}|.$$

D'après le théorème de Lagrange $|\mathcal{O}_{g_i}|$ divise p donc

$$|\mathrm{G}| = |Z(\mathrm{G})| + \sum_{i=1}^{r} |\mathcal{O}_{g_i}|$$

conduit à

$$|\mathrm{G}| \equiv |Z(\mathrm{G})| \bmod p$$

soit

$$0 \equiv |Z(\mathrm{G})| \bmod p$$

Mais e_{G} appartient à $Z(\mathrm{G})$ donc $|Z(\mathrm{G})| \geq p$. Par suite $Z(\mathrm{G})$ est de cardinal p ou p^2.
Si $|Z(\mathrm{G})| = p^2$, alors $\mathrm{G} = Z(\mathrm{G})$ est abélien.
Si $|Z(\mathrm{G})| = p$, alors $\mathrm{G}/Z(\mathrm{G})$ est de cardinal p premier, $\mathrm{G}/Z(\mathrm{G})$ est cyclique et G est, d'après a), abélien.

Exercice 3. Soit G un groupe.

a) Supposons que G est fini. Notons p le plus petit nombre premier divisant le cardinal de G. Montrer que tout sous-groupe de G d'indice p est distingué (indication : commencer par montrer que tout sous-groupe H de G d'indice p agit trivialement sur G/H, en déduire que H est distingué dans G).

b) Supposons que G est infini. Supposons que G admet un sous-groupe strict H d'indice fini. Montrer que G n'est pas un groupe simple.

Éléments de solution 3.

a) Supposons que G est fini. Notons p le plus petit nombre premier divisant le cardinal de G. Soit H un sous-groupe de G d'indice p. Posons $X = \mathrm{G}/\mathrm{H}$. C'est un ensemble de cardinal p, muni de l'action naturelle transitive de G. Cette action induit un morphisme de groupes finis $\varphi\colon G \to \mathcal{S}_X$. Intéressons-nous à la restriction de cette action au sous-groupe H, autrement dit au morphisme $\varphi\colon \mathrm{H} \to \mathcal{S}_X$. Puisque H agit trivialement sur la classe x_0 de H dans $X = \mathrm{G}/\mathrm{H}$ l'action de H sur X induit une action de H sur $X' = X \smallsetminus \{x_0\}$ c'est-à-dire un morphisme de groupes $\psi\colon H \to \mathcal{S}_{X'}$. Or $|X'| = p - 1$ donc tous les facteurs premiers de $|\mathcal{S}_{X'}|$ sont strictement inférieurs à p. Or les facteurs premiers de |H| sont par hypothèse tous supérieurs ou égaux à p. Par suite |H| et $|\mathcal{S}_{X'}|$ sont premiers entre eux. Le morphisme ψ est donc trivial. Il en résulte que H agit trivialement sur X' et donc aussi sur X.

Montrons que cela implique que G est distingué dans G. Soit $h \in \mathrm{H}$ et soit $g \in \mathrm{G}$. Puisque H agit trivialement sur X on a $h \cdot (g\mathrm{H}) = g\mathrm{H}$ donc $(g^{-1}hg)\mathrm{H} = \mathrm{H}$, par suite $g^{-1}hg$ appartient à H, *i.e.* H est distingué dans G.

b) Supposons que G est infini. Supposons que G admet un sous-groupe strict H d'indice fini. Considérons l'action de G sur l'ensemble fini $X = \mathrm{G}/\mathrm{H}$, *i.e.* le morphisme de groupes induit

$$\varphi\colon \mathrm{G} \to \mathcal{S}_X.$$

Comme l'action de G sur X est transitive et comme $H \neq G$ le morphisme φ est non trivial. Son noyau est donc un sous-groupe distingué de G distinct de G. De plus G est infini et $\mathcal{S}_X$ est fini, par conséquent φ n'est pas injectif, *i.e.* $\ker\varphi \neq \{\mathrm{id}\}$. Ainsi $\ker\varphi$ est un sous-groupe distingué de G distinct de $\{\mathrm{id}\}$ et de G ; le groupe G n'est donc pas trivial.

Exercice 4. [Actions de groupes, Combes, page 43 ou Perrin, page 17 Lemme 4.16]
Soit G un p-groupe fini agissant sur un ensemble fini E. Montrer que le nombre de points fixes pour l'action est congru à $|E|$ modulo p.

Éléments de solution 4.

Exercice 5. [Actions de groupes, Combes, pages 42-43 exercice 1]
Soient X un ensemble fini de cardinal $n > 0$ et p un nombre premier. Soit σ la permutation circulaire $(12\cdots p) \in \mathcal{S}_p$. Considérons l'action

$$\begin{array}{rcl} \mathbb{Z}/p\mathbb{Z} \times X^p & \longrightarrow & X^p \\ (\overline{k}, (x_1, x_2, \cdots, x_p)) & \longmapsto & (x_{\sigma^k(1)}, x_{\sigma^k(2)}, \cdots, x_{\sigma^k(p)}). \end{array}$$

a) Montrer que cette application est bien définie.

b) En utilisant l'équation aux classes, montrer que $n^p \equiv n \bmod p$.

c) En appliquant la formule de Burnside, retrouver ce théorème dû à Fermat.

Éléments de solution 5.

Exercice 6.

a) Soit G un groupe fini agissant sur un ensemble fini X. En considérant l'ensemble

$$E = \{(g, x) \in \mathrm{G} \times X \,|\, g \cdot x = x\}$$

calculer le nombre moyen de points fixes d'un élément de G.

b) Combien y a-t-il de colliers différents formés de 9 perles dont 4 bleues, 3 blanches et 2 rouges ?

Éléments de solution 6.

a) Désignons par $\mathrm{Fix}(g) = \{x \in X \,|\, g \cdot x = x\}$ l'ensemble des points fixes de g dans X.
On calcule le cardinal de E de deux façons différentes. D'une part

$$|E| = \sum_{g \in \mathrm{G}} |\mathrm{Fix}(g)|$$

et d'autre part

$$\begin{aligned} |E| &= \sum_{x \in X} |\mathrm{Stab}_{\mathrm{G}}(x)| \\ &= \sum_{\overline{x} \in X/\mathrm{G}} \sum_{y \in \overline{x}} |\mathrm{Stab}_{\mathrm{G}}(y)| \\ &= \sum_{\overline{x} \in X/\mathrm{G}} |\overline{x}| \cdot |\mathrm{Stab}_{\mathrm{G}}(\overline{x})| \\ &= |\mathrm{G}| \cdot \left| X/\mathrm{G} \right| \end{aligned}$$

On en déduit l'égalité

$$\sum_{g \in \mathrm{G}} |\mathrm{Fix}(g)| = |\mathrm{G}| \cdot \left| X/\mathrm{G} \right|$$

i.e.

$$\frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} |\mathrm{Fix}(g)| = \left| X/\mathrm{G} \right|$$

Le nombre moyen de points fixes d'un élément de G est donc $\left| X/\mathrm{G} \right|$, c'est-à-dire le nombre d'orbites de l'action.

b) On représente un collier par cercle du plan euclidien orienté $\mathbb{R}^2$ de centre O et de rayon 1 muni de neuf points p_1, p_2, …, p_9 disposés à intervalles réguliers.
Deux colliers sont équivalents si et seulement si on peut obtenir l'un à partir de l'autre en effectuant une rotation plane du collier ou en le retournant comme une crêpe dans l'espace de dimension 3.
Autrement dit l'ensemble X de tous les colliers possibles à 9 perles dont 4 bleues, 3 blanches et 2 rouges est muni d'une action du groupe diédral $\mathrm{G} = \mathrm{D}_9$ des isométries d'un polygône régulier à neuf côtés. Ce groupe G est un sous-groupe de $\mathrm{SO}_2(\mathbb{R})$, de cardinal 18. Plus précisément

$$\mathrm{G} = \{\mathrm{id},\, r,\, r^2,\, r^3,\, r^4,\, r^5,\, r^6,\, r^7,\, r^8,\, s,\, r \circ s,\, r^2 \circ s,\, r^3 \circ s,\, r^4 \circ s,\, r^5 \circ s,\, r^6 \circ s,\, r^7 \circ s,\, r^8 \circ s\}$$

où r est la rotation de centre 0 et d'angle $\frac{2\pi}{9}$ et s est la symétrie orthogonale d'axe $\Delta = (Op_1)$.
En particulier le groupe G contient 9 rotations et 9 symétries orthogonales. Le nombre de colliers distincts est le nombre d'orbites de l'action de G sur X, *i.e.* $\left| X/\mathrm{G} \right|$. Or

$$\left| X/\mathrm{G} \right| = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} |\mathrm{Fix}(g)|.$$

Déterminons $\mathrm{Fix}(g)$ pour tout $g \in \mathrm{G}$. Soit g dans G.

- Si $g = \mathrm{id}$, alors $\mathrm{Fix}(g) = X$ et

$$|\mathrm{Fix}(g)| = |X| = \binom{9}{4}\binom{5}{3} = 126 \times 10 = 1260.$$

- Si g appartient à $\{r, r^2, r^4, r^5, r^7, r^8\}$, alors $\langle g\rangle \subset \mathrm{G}$ est constitué des 9 rotations. Ainsi un collier fixe par g est fixe par r ce qui implique que toutes les perles sont de la même couleur : contradiction. Par conséquent $\mathrm{Fix}(g) = \emptyset$.
- Si $g \in \{r^3, r^6\}$, alors dans un collier fixe par g le nombre de perles d'une couleur donnée doit être un multiple de 3 ce qui n'est pas le cas dans l'ensemble X. Il s'en suit que $\mathrm{Fix}(g) = \emptyset$.
- Si g est une symétrie, on peut supposer que $g = s$, les autres cas étant identiques. Puisque l'axe Δ ne contient qu'une perle (p_1), dans un collier fixe par g les perles p_i, $i \neq 1$, vont par paire de même couleur. Cela assure que p_1 est nécessairement blanche. Se donner un collier fixe par g revient donc à se donner les couleurs des perles p_2, p_3, p_4, p_5 de sorte que 2 soient bleues, 1 blanche et 1 rouge. Le nombre de tels colliers vaut

$$|\mathrm{Fix}(g)| = \binom{4}{2} \cdot \binom{2}{1} = 6 \times 2 = 12.$$

Par suite

$$\left|X/\mathrm{G}\right| = \frac{1}{18}(1260 + 9 \times 12) = 76.$$

Il y a donc exactement 76 colliers formés de 9 perles dont 4 bleues, 3 blanches et 2 rouges.

Exercice 7. [Groupe symétrique, signature]
Montrer que la signature ε est le seul morphisme de groupes de $\mathcal{S}_n$ vers le groupe multiplicatif $\{1, -1\}, \cdot$.

Éléments de solution 7.

Exercice 8. [Sous-groupes finis de O(2), Nourdin, page 221]
Nous allons montrer que tout sous-groupe fini de O(2) non contenu dans SO(2) est un groupe diédral.

a) Soient G un groupe et H_0 et H des sous-groupes de G tel que H_0 est d'indice fini dans G. Montrer que

$$|\mathrm{H} : \mathrm{H} \cap \mathrm{H}_0| \leq |\mathrm{G} : \mathrm{H}_0|\,.$$

b) Soient $\mathrm{H} \subset \mathrm{O}(2)$ fini et $\mathrm{H}^+ := \mathrm{H} \cap \mathrm{SO}(2)$. On suppose que $\mathrm{H}^+ \neq \mathrm{H}$. Utiliser le résultat précédent pour montrer que $|\mathrm{H} : \mathrm{H}^+| = 2$.

c) Soit $s \in \mathrm{H} \setminus \mathrm{H}^+$ et soit r un générateur du groupe cyclique H^+ d'ordre n. Montrer que $srs = r^{-1}$.

d) Montrer que $\mathrm{H} = \langle r, s\rangle$ et que $\mathrm{H} = \mathrm{D}_{2n}$.

Éléments de solution 8.

Exercice 9. [Sous-groupes finis de O(3), Delcourt, page 163]
Nous allons déterminer, à isomorphisme près, tous les sous-groupes finis de O(3).
Soient $\mathrm{H} \subset \mathrm{O}(3)$ fini et $\mathrm{H}^+ := \mathrm{H} \cap \mathrm{SO}(3)$. Supposons que $\mathrm{H} \neq \mathrm{H}^+$.

a) Si $-\mathrm{id} \in \mathrm{H}$, alors montrer que

$$\begin{array}{rcl} \phi\colon \mathrm{H} & \longrightarrow & \mathrm{H}^+ \times \mathbb{Z}/2\mathbb{Z} \\ g & \longmapsto & (\det(g)\mathrm{Id} \circ g, \det(g)) \end{array}$$

est un isomorphisme. Conclure que H est isomorphe à l'un des groupes suivants : $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathrm{D}_{2n} \times \mathbb{Z}/2\mathbb{Z}$, $\mathcal{A}_4 \times \mathbb{Z}/2\mathbb{Z}$, $\mathcal{A}_5 \times \mathbb{Z}/2\mathbb{Z}$, $\mathcal{S}_4 \times \mathbb{Z}/2\mathbb{Z}$.

b) Si $-\mathrm{id} \notin \mathrm{H}$, alors montrer que

$$\begin{array}{rcl} \phi\colon \mathrm{H} & \longrightarrow & \mathrm{SO}(3) \\ g & \longmapsto & \det(g)\mathrm{id} \circ g \end{array}$$

est un morphisme injectif. Conclure que H est isomorphe à l'un des groupes suivants : $\mathbb{Z}/n\mathbb{Z}, \mathrm{D}_{2n}, \mathcal{S}_4$.

Éléments de solution 9.

Exercice 10. [Perrin, page 35 exercice 6]
Soient G un groupe fini et p le plus petit facteur premier de $|\mathrm{G}|$. Soit H un sous-groupe d'ordre p, distingué dans G. Montrer que H est central, *i.e.* $\mathrm{H} \subset Z(\mathrm{G})$.

Indication : faire opérer G sur H par conjugaison et étudier Aut(H).

Éléments de solution 10.

Considérons

$$\mathrm{G} \times \mathrm{H} \to \mathrm{H}, \qquad (g,h) \mapsto ghg^{-1}$$

C'est une action bien définie car $\mathrm{H} \lhd \mathrm{G}$. Soit $\varphi\colon \mathrm{G} \to \mathcal{S}_{\mathrm{H}}$ le morphisme associé

$$\begin{array}{rcl} \varphi\colon \mathrm{G} & \to & \mathcal{S}_{\mathrm{H}} \\ g & \mapsto & \varphi_g\colon \mathrm{H} \to \mathrm{H} \\ & & \quad h \mapsto ghg^{-1} \end{array}$$

Notons que φ_g est un automorphisme de H donc $\varphi(G)$ est un sous-groupe de Aut(H). Puisque H est cyclique, $\mathrm{Aut}(\mathrm{H}) \simeq \mathrm{Aut}\left(\mathbb{Z}/p\mathbb{Z}\right) \simeq \left(\mathbb{Z}/p\mathbb{Z}\right)^{\times}$. Par suite $|\mathrm{Aut}(\mathrm{H})| = |\left(\mathbb{Z}/p\mathbb{Z}\right)^{\times}| = p-1$. Le théorème d'isomorphisme assure que $|\varphi(\mathrm{G})|$ divise $|\mathrm{G}|$. Par hypothèse p est le plus petit facteur premier de $|\mathrm{G}|$, il s'en suit que $|\varphi(\mathrm{G})| = 1$. Par conséquent pour tout g dans G nous avons $\varphi_g = \mathrm{id}$ et $\mathrm{H} \subset Z(\mathrm{G})$.

Exercice 11. [Perrin, p. 18 exercice 5.3]
Soient $\mathbb{F}_p$ le corps fini à p éléments (p un nombre premier) et $\mathrm{G} = \mathrm{GL}(n, \mathbb{F}_p)$, $n \in \mathbb{N}^*$.

a) Montrer que le cardinal de G est égal à

$$(p^n-1)(p^n-p)\cdots(p^n-p^{n-1}) = mp^{n(n-1)/2},$$

avec $p \nmid m$.

b) Considérons l'ensemble des matrices triangulaires supérieures strictes :

$$\mathrm{P} = \{A = (a_{ij}) \mid a_{ij} = 0 \text{ si } i > j \text{ et } a_{ii} = 1\}.$$

Montrer que P est un p-Sylow de G.

Éléments de solution 11.

a) Soit M un élément de $\mathrm{GL}(n, \mathbb{F}_p)$. Notons c_i ses colonnes. Il y a $p^n - 1$ choix possibles pour c_1 (les vecteurs non nuls de $\mathbb{F}_p^n$), $p^n - p$ choix possibles pour c_2 (les vecteurs de $\mathbb{F}_p^n$ non multiples de c_1), $p^n - p^2$ choix possibles pour c_3 (c_3 est un vecteurs de $\mathbb{F}_p^n$ qui n'est pas combinaison linéaire de c_1 et c_2). Il en résulte que

$$|\mathrm{G}| = (p^n-1)(p^n-p)\cdots(p^n-p^{n-1}).$$

Mais

$$\begin{array}{rcl} (p^n-1)(p^n-p)\cdots(p^n-p^{n-1}) & = & (p^n-1)(p^{n-1}-1)\ldots(p-1)pp^2\ldots p^{n-1} \\ & = & (p^n-1)(p^{n-1}-1)\ldots(p-1)p^{1+2+\ldots+(n-1)} \\ & = & (p^n-1)(p^{n-1}-1)\ldots(p-1)p^{n(n-1)/2} \end{array}$$

De plus p ne divise pas $(p^n-1)(p^{n-1}-1)\ldots(p-1)$ d'où le résultat.

b) Soit M un élément de P ; M a $\frac{n(n-1)}{2}$ coefficients libres donc $|\mathrm{P}| = p^{n(n-1)/2}$ et P est un p-Sylow de G.

Exercice 12.

Supposons qu'il existe un groupe simple G d'ordre 180.

a) Montrer que G contient trente six 5-Sylow.

b) Montrer que G contient dix 3-Sylow. Montrer que deux 3-Sylow distincts ne peuvent pas contenir un même élément $g \neq e_{\mathrm{G}}$ (Indication : considérer les ordres possibles pour le centralisateur de g, observer qu'un groupe d'ordre 18 admet un unique 3-Sylow).

c) Conclure.

Éléments de solution 12.

a) Montrons que G contient trente six 5-Sylow. Pour tout premier p qui divise $|\mathrm{G}|$ notons n_p le nombre de p-Sylow de G. Les théorèmes de Sylow assurent que n_5 divise 36 et $n_5 \equiv 1 \pmod 5$. Ceci implique que n_5 appartient à $\{1, 6, 36\}$. Puisque par hypothèse G est simple on ne peut avoir $n_5 = 1$ (sinon l'unique 5-Sylow serait distingué dans G). Il en résulte que n_5 appartient à $\{6, 36\}$. Supposons que $n_5 = 6$. Alors l'action transitive de G par conjugaison sur l'ensemble de ses 5-Sylow induit un morphisme non trivial $f\colon \mathrm{G} \to \mathcal{S}_6$. Le groupe G étant par hypothèse simple, le noyau de ce morphisme est trivial, *i.e.* ce morphisme est injectif. Considérons le morphisme $g\colon \mathrm{G} \to {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$ donné par $g = f \circ \mathrm{sgn}$. Comme G est simple et comme $\ker g \lhd \mathrm{G}$ nous avons l'alternative : $\ker g = \{\mathrm{id}\}$ ou $\ker g = \mathrm{G}$. Puisque $|\mathrm{G}| > |{}^{\mathbb{Z}}\!/_{2\mathbb{Z}}|$ le morphisme g n'est pas injectif, *i.e.* $\ker g \neq \{\mathrm{id}\}$. Ainsi $\ker g = \mathrm{G}$ et G est un sous-groupe de $\mathcal{A}_6$. D'une part $|\mathcal{A}_6| = \frac{|\mathcal{S}_6|}{2} = \frac{6!}{2} = 360$, d'autre part $|\mathrm{G}| = 180$, autrement dit G est d'indice 2 dans $\mathcal{A}_6$. Le groupe G est donc un sous-groupe distingué non trivial et propre de $\mathcal{A}_6$: contradiction avec le fait que $\mathcal{A}_6$ est simple. Par conséquent $n_5 = 36$.

b) Montrons que G contient dix 3-Sylow. Pour tout premier p qui divise $|\mathrm{G}|$ notons n_p le nombre de p-Sylow de G. Les théorèmes de Sylow assurent que n_3 divise 20 et $n_3 \equiv 1 \pmod 3$. Ceci implique que n_3 appartient à $\{1, 4, 10\}$. Puisque par hypothèse G est simple on ne peut avoir $n_3 = 1$ (sinon l'unique 3-Sylow serait distingué dans G). Si n_3 était égal à 4, on en déduirait comme au a) un morphisme injectif de G dans $\mathcal{S}_4$ ce qui est impossible car $180 = |\mathrm{G}| > |\mathcal{S}_4| = 4! = 24$. Ainsi $n_3 = 10$.

Montrons que deux 3-Sylow distincts ne peuvent pas contenir un même élément $g \neq e_{\mathrm{G}}$.
Soient S et T deux 3-Sylow de G distincts. Soit $g \in \mathrm{S} \cap \mathrm{T}$. Notons $\mathrm{Z} = \{x \in \mathrm{G} \,|\, xg = gx\}$ le centralisateur de g dans G. Supposons que $g \neq e_{\mathrm{G}}$. Un groupe d'ordre 9 étant abélien, Z contient S et T. Par conséquent $|\mathrm{Z}| \in \{18, 36, 45, 90\}$. L'action transitive de G sur ${}^{\mathrm{G}}\!/_{\mathrm{Z}}$ induit un morphisme injectif de G vers $\mathcal{S}_{{}^{\mathrm{G}}/_{\mathrm{Z}}}$. Or $|\mathrm{G}| = 180$ et $|\mathcal{S}_{{}^{\mathrm{G}}/_{\mathrm{Z}}}| \in \{2, 4! = 24, 5! = 120, 10!\}$ donc $|\mathcal{S}_{{}^{\mathrm{G}}/_{\mathrm{Z}}}| = 10!$ et $|\mathrm{Z}| = 18$. Ainsi S et T sont des 3-Sylow de Z et un groupe d'ordre 18 admet un unique 3-Sylow d'où $\mathrm{S} = \mathrm{T}$: contradiction. Finalement $\mathrm{S} \cap \mathrm{T} = \{e_{\mathrm{G}}\}$.

c) D'après a) le groupe G contient exactement $36 \times 4 = 144$ éléments d'ordre 5.
D'après b) le groupe G contient dix 3-Sylow dont les intersections deux à deux sont triviales. Par suite il y a dans G exactement $10 \times 8 = 80$ éléments distincts de e_{G} d'ordre divisant 9.
Ainsi G possède au moins $144 + 80 = 224 > 180$ éléments distincts : contradiction.
Il n'existe donc pas de groupe simple d'ordre 180.

Exercice 13. Soit E un $\mathbf{F}_q$-espace vectoriel de dimension finie n. Pour $0 \leq d \leq n$, combien E possède-t-il de sous-espaces vectoriels de dimension d ?

Indication : considérer l'action de $\mathrm{GL}(E)$ sur l'ensemble des sous-espaces vectoriels de dimension d de E.

Éléments de solution 13.

Exercice 14. [Sous-groupes de Sylow]
Expliciter les sous-groupes de Sylow des groupes suivants :

a) les groupes symétriques $\mathcal{S}_3$ et $\mathcal{S}_4$,

b) les groupes alternés $\mathcal{A}_4$ et $\mathcal{A}_5$ ([exercice 6 p. 98 Szpirglas]),

c) les groupes diédraux D_{2n} ([Dummit-Foot, p. 146, exercice 5, 12]),

d) le groupe hamiltonien $\mathbb{H}_8$,

e) Pour $\mathcal{S}_4$, $\mathcal{A}_4$ et $\mathcal{A}_5$ donner une interprétation géométrique de ses 3-sous-groupes de Sylow ([Caldero-Germoni p. 373]).

Éléments de solution 14.

a)

b) Déterminons les sous-groupes de Sylow de $\mathcal{A}_4$. Le groupe $\mathcal{A}_4$ est d'ordre $12 = 2^2 \times 3$.

Les théorèmes de Sylow assurent que
— le nombre n_2 de sous-groupes d'ordre $2^2 = 4$ de $\mathcal{A}_4$ est 1 ou 3 ;
— le nombre n_3 de sous-groupes d'ordre 3 de $\mathcal{A}_4$ est 1 ou 4.
Le groupe $\mathcal{A}_4$ ne contient pas de cycle de longueur 4 donc les seuls éléments d'ordre pair sont les doubles transpositions. Il y en a trois ainsi $\mathcal{A}_4$ contient un seul sous-groupe d'ordre 4, isomorphe au groupe de Klein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
Le groupe $\mathcal{A}_4$ contient les cycles de longueur 3. Il y en a plus de deux donc $n_3 = 4$.

Déterminons les sous-groupes de Sylow de $\mathcal{A}_5$. Le groupe $\mathcal{A}_5$ est d'ordre $60 = 2^2 \times 3 \times 5$.

Les 3-Sylow de $\mathcal{A}_5$ sont d'ordre 3, donc cycliques ; chacun est engendré par un 3-cycle et contient deux 3-cycles. Les 3-Sylow sont deux à deux d'intersection réduite à $\{e\}$. Comme il y a vingt 3-cycles dans $\mathcal{A}_5$, il y a dix 3-Sylow.
On peut aussi utiliser les théorèmes de Sylow : le nombre de 3-Sylow est $\equiv 1 \pmod 3$ et divise 20 ; c'est donc 1, 4 ou 10. Puisque $\mathcal{A}_5$ est simple il ne peut y avoir qu'un seul 5-Sylow. Si c'est 4 l'action par conjugaison de $\mathcal{A}_5$ sur l'ensemble de ses 3-Sylow induit un morphisme de $\mathcal{A}_5$ dans $\mathcal{S}_4$ qui est non trivial (car l'action par conjugaison est transitive) et donc injectif (car le noyau distingué est forcément trivial puisque $\mathcal{A}_5$ est simple) : contradiction avec le fait que l'ordre de $\mathcal{A}_5$ ne divise par celui de $\mathcal{S}_4$.

Les 5-Sylow de $\mathcal{A}_5$ sont d'ordre 5, donc cycliques ; chacun est engendré par un 5-cycle et contient quatre 5-cycles. Les 5-Sylow sont deux à deux d'intersection réduite à $\{1\}$. Comme il y a vingt-quatre 5-cycles dans $\mathcal{A}_5$, il y a six 5-Sylow.
On peut aussi utiliser les théorèmes de Sylow : le nombre de 5-Sylow est $\equiv 1 \pmod 5$ et divise 12 ; c'est donc 1 ou 6. Puisque $\mathcal{A}_5$ est simple il ne peut y avoir qu'un seul 3-Sylow. Par conséquent le nombre de 5-Sylow est 6.

On a donc déterminé $6 \times 4 = 24$ éléments d'ordre 5 et $2 \times 10 = 20$ éléments d'ordre 3 ce qui fait, en ajoutant l'identité, 45 éléments de $\mathcal{A}_5$.

Soit n_2 le nombre de 2-Sylow, *i.e.* le nombre de sous-groupes d'ordre 4 de $\mathcal{A}_5$. Rappelons qu'un groupe d'ordre 4 est soit cyclique, soit isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
Le groupe $\mathcal{A}_5$ ne contient par d'élément d'ordre 4. En effet les éléments d'ordre 4 du groupe symétrique $\mathcal{S}_5$ sont les 4-cycles qui sont des permutations impaires. Par suite chaque 2-Sylow est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; il est engendré par deux produits de deux transpositions qui commutent et contient trois éléments d'ordre 2. Les trois éléments d'ordre 2 sont les trois produits de deux transpositions qui commutent qu'on peut former avec quatre éléments de $\{1, 2, 3, 4, 5\}$. On en déduit que les 2-Sylow sont deux à deux d'intersection réduite à {e}. Il y a 15 éléments d'ordre 2 dans $\mathcal{A}_5$ et cinq 2-Sylow.
les sous-groupes d'ordre 4 de $\mathcal{A}_5$ sont engendrés par les paires de transpositions disjointes : on a 5 paires de transpositions distinctes (elles sont déterminées par le seul élément de $\{1, 2, 3, 4, 5\}$ qui reste fixe par la double transposition) qui engendrent des sous-groupes distincts. Cela fait donc déjà cinq 2-Sylow isomorphes à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
Par ailleurs $n_2 \equiv 1 \pmod 2$ et n_2 divise 15 donc n_2 appartient à $\{1, 3, 5, 15\}$. En utilisant ce qui précède on se ramène à $n_2 \in \{5, 15\}$. De plus il y a au plus $60 - 45 - 1 = 14$ éléments d'ordre 2. Finalement $n_2 = 5$.

c) i) Déterminons les sous-groupes de Sylow du groupe D_8. Le groupe D_8 est d'ordre $2^3 = 8$. Les 2-Sylow sont d'ordre 2^3, il n'y en a donc qu'un, c'est D_8.

ii) Déterminons les sous-groupes de Sylow du groupe D_{10}. Le groupe D_{10} est le groupe des isométries du plan qui conservent un pentagone régulier, il est d'ordre $2 \times 5 = 10$.

Soit n_2 le nombre de ses 2-Sylow, *i.e.* le nombre de ses sous-groupes d'ordre 2. D'après les théorèmes de Sylow $n_2 \equiv 1 \pmod 2$ et n_2 divise 5. Ainsi $n_2 \in \{1, 5\}$. Par ailleurs les sous-groupes de D_{10} engendrés par les cinq symétries par rapport aux médiatrices de chacun des côtés du pentagone sont cinq groupes d'ordre 2. Il s'en suit que $n_2 = 5$.

Soit n_5 le nombre de 5-Sylow de D_{10}, *i.e.* le nombre de sous-groupes d'ordre 5 de D_{10}. Les théorèmes de Sylow assurent que $n_5 \equiv 1 \pmod 2$ et n_5 divise 2. Il n'y a donc qu'un unique 5-Sylow, le sous-groupe engendré par la rotation d'angle $2\pi/5$ dont le centre est le centre du pentagone.

d)

e)

Exercice 15. [p-Sylow de $\mathrm{GL}(2, \mathbb{F}_p)$]
Soient $\mathbb{F}_p$ le corps fini à p éléments (p un nombre premier) et $\mathrm{G} = \mathrm{GL}(2, \mathbb{F}_p)$.

a) Soit P l'ensemble des matrices triangulaires supérieures strictes de G. Montrer que $n_p = [\mathrm{G} : N_{\mathrm{G}}(\mathrm{P})]$.

b) Montrer que $N_{\mathrm{G}}(\mathrm{P})$ contient les matrices triangulaires supérieures de G.

c) En déduire que $n_p \mid p + 1$.

d) Utiliser les théorèmes de Sylow pour conclure que $n_p = 1 + p$.

Éléments de solution 15.

Exercice 16. [p-Sylow de $\mathcal{S}_p$, Szpirglas, p. 101 exercice 20]

a) Quel est l'ordre d'un p-Sylow de $\mathcal{S}_p$?

b) Combien y a-t-il de p-Sylow dans $\mathcal{S}_p$?

c) En déduire le théorème de Wilson, c'est à dire

$$(p-1)! \equiv -1 \bmod p.$$

Éléments de solution 16.

a) L'ordre de $\mathcal{S}_p$ est $p! = p(p-1)!$. De plus p et $(p-1)!$ sont premiers entre eux. Par suite un p-Sylow de $\mathcal{S}_p$ est d'ordre p.

b) Pour déterminer le nombre de p-Sylow de $\mathcal{S}_p$ on cherche combien il y a d'éléments d'ordre p de $\mathcal{S}_p$. Ce sont les p-cycles qui sont conjugués entre eux. Pour calculer leur nombre il suffit de calculer l'ordre du centralisateur C de l'un d'eux, par exemple du p-cycle $\sigma = (1\ 2\ \ldots\ p)$. Si s est une permutation, alors

$$s\sigma s^{-1} = (s(1)\ s(2)\ \ldots\ s(p))$$

Donc $s \in C$ si

$$(\sigma(1)\ \sigma(2)\ \ldots\ \sigma(p)) = (s(1)\ s(2)\ \ldots\ s(p))$$

c'est-à-dire si s est une puissance de la permutation circulaire d'ordre p. L'ordre de C est donc égal à p et il y a $\frac{p!}{p} = (p-1)!$ éléments d'ordre p dans $\mathcal{S}_p$ car $\mathcal{S}_p/C$ est en bijection avec les conjugués de σ.

Ces éléments d'ordre p se répartissent entre $\frac{(p-1)!}{p-1} = (p-2)!$ p-Sylow de $\mathcal{S}_p$ qui contiennent chacun $(p-1)$ éléments d'ordre p.

Autre rédaction possible : un p-Sylow est d'ordre p, p étant premier, un p-Sylow est donc un sous-groupe cyclique d'ordre p. Il y a $(p-1)!$ p-cycles dans $\mathcal{S}_p$ donc $\frac{(p-1)!}{p-1} = (p-2)!$ p-Sylow.

c) Notons n_p le nombre de p-Sylow. D'après b) on a $n_p = (p-2)!$. D'après les théorèmes de Sylow $n_p \equiv 1 \bmod p$. Donc $(p-2)! \equiv 1 \bmod p$ et $(p-1)! \equiv p - 1 \bmod p$. Mais $p - 1 \equiv -1 \bmod p$. Il en résulte que $(p-1)! \equiv -1 \bmod p$.

Exercice 17. [p-groupes, Calais, page 296 remarque 8.40]
Un p-groupe est par définition un groupe dont chaque élément est d'ordre une puissance de p. Montrer qu'un p-groupe fini est un groupe d'ordre p^k pour un certain $k \in \mathbb{N}^*$.

Éléments de solution 17.

Exercice 18. [Groupes simples, Perrin, page 18 proposition 4.17]
Soient G un groupe infini et H un sous-groupe propre de G tel que [G : H] est fini. Montrer que G n'est pas simple.

Éléments de solution 18.
Considérons l'action de G sur ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ donnée par

$$\mathrm{G} \times {}^{\mathrm{G}}\!/_{\mathrm{H}} \to {}^{\mathrm{G}}\!/_{\mathrm{H}}, \qquad (g, g_1\mathrm{H}) \mapsto gg_1\mathrm{H}$$

Le morphisme associé est

$$\begin{array}{rcl} \varphi\colon \mathrm{G} & \to & \mathcal{S}_{{}^{\mathrm{G}}\!/_{\mathrm{H}}} = \mathcal{S}_n \\ g & \mapsto & \varphi_g\colon {}^{\mathrm{G}}\!/_{\mathrm{H}} \to {}^{\mathrm{G}}\!/_{\mathrm{H}} \\ & & \qquad g_1 \mapsto gg_1\mathrm{H} \end{array}$$

où $n = [\mathrm{G} : \mathrm{H}]$.

Raisonnons par l'absurde : supposons que G soit simple. Alors puisque $\ker\varphi$ est un sous-groupe distingué de G nous avons l'alternative
— ou bien $\ker\varphi = \{e_{\mathrm{G}}\}$,
— ou bien $\ker\varphi = \mathrm{G}$.

Comme G est infini, φ n'est pas injective, *i.e.* $\ker\varphi \neq \{e_{\mathrm{G}}\}$. Par conséquent $\ker\varphi = \mathrm{G}$. Or $\ker\varphi = \mathrm{G}$ si et seulement si pour tout $g \in \mathrm{G}$, pour tout $g_1 \in \mathrm{G}$ nous avons $gg_1\mathrm{H} = \mathrm{H}$. En particulier pour $g_1 = e_{\mathrm{G}}$ nous obtenons $\mathrm{H} = g\mathrm{H}$ soit $g \in \mathrm{H}$; ainsi $\mathrm{G} \subset \mathrm{H}$ et $\mathrm{G} = \mathrm{H}$: contradiction avec l'hypothèse "H est un sous-groupe propre de G".

Exercice 19. [Groupes simples]
Soient G un groupe fini et H un sous-groupe propre de G tel que |G| ne divise pas [G : H]!. Montrer que G n'est pas simple.

Éléments de solution 19.
Considérons l'action de G sur ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ donnée par

$$\mathrm{G} \times {}^{\mathrm{G}}\!/_{\mathrm{H}} \to {}^{\mathrm{G}}\!/_{\mathrm{H}}, \qquad (g, g_1\mathrm{H}) \mapsto gg_1\mathrm{H}$$

Le morphisme associé est

$$\begin{array}{rcl} \varphi\colon \mathrm{G} & \to & \mathcal{S}_{{}^{\mathrm{G}}\!/_{\mathrm{H}}} \\ g & \mapsto & \varphi_g\colon {}^{\mathrm{G}}\!/_{\mathrm{H}} \to {}^{\mathrm{G}}\!/_{\mathrm{H}} \\ & & \qquad g_1 \mapsto gg_1\mathrm{H} \end{array}$$

Raisonnons par l'absurde : supposons que G soit simple. Alors $\ker\varphi$ étant un sous-groupe distingué de G, nous avons l'alternative suivante
— ou bien $\ker\varphi = \mathrm{G}$,
— ou bien $\ker\varphi = \{e_{\mathrm{G}}\}$.

Nous allons considérer ces deux éventualités :
— Supposons que $\ker\varphi = \mathrm{G}$. Alors pour tout $g \in \mathrm{G}$, pour tout $g_1 \in \mathrm{G}$ nous avons $gg_1\mathrm{H} = \mathrm{H}$. Pour $g_1 = e_{\mathrm{G}}$ nous obtenons $g\mathrm{H} = \mathrm{H}$ d'où $g \in \mathrm{H}$. Ainsi $\mathrm{G} \subset \mathrm{H}$. Mais par ailleurs $\mathrm{H} \subset \mathrm{G}$ donc $\mathrm{H} = \mathrm{G}$: contradiction avec l'hypothèse "H est un sous-groupe propre de G".
— Supposons que $\ker\varphi = \{e_{\mathrm{G}}\}$. Alors φ est injective et |G| divise [G : H]! : contradiction avec l'hypothèse "|G| ne divise pas [G : H]!".

Il en résulte que G n'est pas simple.

Exercice 20. [p-groupes, Perrin, page 35 exercice 5]
Soit G un p-groupe de cardinal p^α. Montrer que G a des sous-groupes distingués d'ordre p^β, pour tout entier $\beta \leq \alpha$.

Éléments de solution 20.

Exercice 21. [Groupes simples, Calais, page 214 proposition 6.15]
Soient $p \neq q$ deux nombres premiers. Montrer que tout groupe d'ordre pq n'est pas simple.

Éléments de solution 21.

Soient p et q deux nombres premiers. Supposons quitte à renommer p et q que $p > q$. Soitn_p le nombre de p-sous-groupes de Sylow de G. Le second théorème de Sylow assure que $n_p \equiv 1 \bmod p$ et n_p divise q, *i.e.* $n_p \in \{1, q\}$. Comme $p > q$, $q \not\equiv 1 \bmod p$; par suite $n_p = 1$. Le groupe G contient donc un unique p-sous-groupe de Sylow qui est distingué dans G (théorème de Sylow).

Exercice 22. [Groupes simples, Perrin, page 37 exercice (2)b]
Soient p, q, r trois nombres premiers distincts. Montrer que tout groupe d'ordre pqr n'est pas simple.

Éléments de solution 22.

Soient p, q et r trois nombres premiers distincts. Soit G un groupe d'ordre pqr. Quitte à renommer p, q et r nous supposons que $p < q < r$. D'après les théorèmes de Sylow nous avons

$$n_p \,|\, qr \qquad\qquad n_p \equiv 1 \bmod p$$

$$n_q \,|\, pr \qquad\qquad n_q \equiv 1 \bmod q$$

$$n_r \,|\, pq \qquad\qquad n_r \equiv 1 \bmod r$$

Si $n_p = 1$ ou $n_q = 1$ ou $n_r = 1$, alors d'après les théorèmes de Sylow G possède un sous-groupe distingué ; le groupe G n'est donc pas simple.

Supposons désormais que $n_p \neq 1$, $n_q \neq 1$ et $n_r \neq 1$. Alors

$$n_p \in \{q, r, qr\} \qquad\qquad n_p \equiv 1 \bmod p$$

$$n_q \in \{p, r, pr\} \qquad\qquad n_q \equiv 1 \bmod q$$

$$n_r \in \{p, q, pq\} \qquad\qquad n_r \equiv 1 \bmod r$$

Mais $p < q < r$ donc

— $n_r = pq$ et G contient $pq(r-1)$ éléments d'ordre r ;

— et $n_q \in \{r, pr\}$ et G contient au moins $r(q-1)$ éléments d'rodre q.

Par ailleurs $n_p \in \{q, r, qr\}$ et G contient au moins $q(p-1)$ éléments d'ordre p. Finalement G contient au moins

$$pq(r-1) + r(q-1) + q(p-1) + \underbrace{1}_{\text{élément neutre}}$$

éléments. Remarquons que

$$pq(r-1) + r(q-1) + q(p-1) + 1 = pqr + rq - r - q + 1.$$

Comme $q > 2$ et $r > q$ nous obtenons $2r > q + r$ et $rq > 2r$ d'où $rq > q + r$ et $rq + 1 > q + r$ soit $rq - r - q + 1 > 0$. Finalement $pqr + rq - r - q + 1 > pqr$, autrement dit G contient strictement plus de pqr éléments : contradiction avec $|\mathrm{G}| = pqr$.

Exercice 23. [Groupes simples, Calais, page 216 exercice 8]
Soient p, q des nombres premiers distincts. Montrer que tout groupe d'ordre p^2q n'est pas simple.

Éléments de solution 23.

Exercice 24.
Montrer qu'un groupe d'ordre 56 n'est pas simple.

Éléments de solution 24. Soit G un groupe d'ordre $56 = 2^3 \times 7$. Soit n_2 le nombre de 2-Sylow et n_7 le nombre de 7-Sylow.

D'après les théorèmes de Sylow

$$n_2 \equiv 1 \pmod 2 \qquad\qquad n_2|7$$

$$n_7 \equiv 1 \pmod 7 \qquad\qquad n_7|8$$

Par conséquent $n_2 \in \{1, 7\}$ et $n_7 \in \{1, 8\}$.

Si $n_7 = 1$, alors d'après les théorèmes de Sylow G possède un sous-groupe distingué propre donc G n'est pas simple.

Supposons que $n_7 \neq 1$, alors $n_7 = 8$ et G compte huit sous-groupes d'ordre 7, c'est-à-dire déjà $8(7-1) = 48$ éléments d'ordre 7 (remarque : $7-1$ = nombre d'éléments non triviaux d'un sous-groupe d'ordre 7). En ajoutant l'élément neutre nous avons donc "listé" 49 éléments du groupe G. Si $n_2 \neq 1$, alors $n_2 = 7$, on a donc au moins deux sous-groupes de G distincts d'ordre $2^3 = 8$ qui sont isomorphes ce qui ajoute plus de sept éléments. Le groupe G compte donc plus de 56 éléments : contradiction. Par suite $n_2 = 1$; d'après les théorèmes de Sylow G possède un sous-groupe distingué propre donc G n'est pas simple.

Exercice 25. [Groupes simples, Perrin, page 37 exercice 3]
Soit G un groupe d'ordre $2k$, avec k un entier impair, $k \neq 1$. Montrer que G n'est pas simple. (Considérer l'action de G sur G par translation et étudier le morphisme $\varepsilon \circ \phi$ ou ε est la signature sur le groupe symétrique $\mathcal{S}_\mathrm{G}$ et ϕ est le morphisme $\mathrm{G} \to \mathcal{S}_\mathrm{G}$ associé à cette action.)

Éléments de solution 25.

Exercice 26. [Groupes simples]
Montrer qu'aucun groupe (non banal, *i.e.* non isomorphe à $\mathbb{Z}/p\mathbb{Z}$) d'ordre < 60 est simple.

Éléments de solution 26.

Exercice 27.

On cherche à montrer que $\mathcal{A}_5$ est le seul groupe simple d'ordre 60.

a) Faire la liste des éléments de $\mathcal{A}_5$ avec leur ordre respectif. Décrire les classes de conjugaison dans $\mathcal{A}_5$.

b) Montrer que $\mathcal{A}_5$ est simple.

c) Soit G un groupe simple d'ordre $p^\alpha m$ avec $\alpha \geq 1$ et m non divisible par p. Notons n_p le nombre de p-Sylow de G. Montrer que $|\mathrm{G}|$ divise $n_p!$.

d) Soit G un groupe simple d'ordre 60. Montrer que le nombre de 2-Sylow de G est égal à 5 ou à 15.

e) En déduire que G contient un sous-groupe d'ordre 12.

f) Conclure.

Éléments de solution 27.

a) Faisons la liste des éléments de $\mathcal{A}_5$ avec leur ordre respectif.

Les 60 éléments de $\mathcal{A}_5$ sont les suivants :

- l'identité d'ordre 1 qui forme une classe de conjugaison ;
- les double transpositions $(a\ b)(c\ d)$ où $\{a, b, c, d\}$ est de cardinal 4. Elles sont au nombre de 15, elles sont d'ordre 2 et elles forment une classe de conjugaison ;
- les 3-cycles $(a\ b\ c)$ où $\{a, b, c\}$ est de cardinal 3. Ils sont au nombre de 20, ils sont d'ordre 3 et forment une classe de conjugaison ;

- les 5-cycles $(a\ b\ c\ d\ e)$ où $\{a, b, c, d, e\}$ est de cardinal 5. Ils sont au nombre de 24, ils sont d'ordre 5 et forment deux classes de conjugaison : celle de (1 2 3 4 5) et (2 1 3 4 5).

Nous avons bien énuméré tous les éléments de $\mathcal{A}_5$: $1 + 15 + 20 + 24 = 60$.

b) Montrons que $\mathcal{A}_5$ est simple. Soit $H \neq \{e\}$ un sous-groupe distingué de $G = \mathcal{A}_5$. Puisque H est distingué, H est réunion de classes de conjugaison dans G. Comme aucun des entiers $1+15 = 16$, $1 + 12 = 13$, $1 + 24 = 25$, $1 + 15 + 12 = 28$, $1 + 15 + 24 = 40$, $1 + 20 = 21$, $1 + 20 + 15 = 36$, $1 + 20 + 12 = 33$, $1 + 20 + 24 = 45$ ne divise $60 = |\mathcal{A}_5|$, le théorème de Lagrange assure que H contient nécessairement toutes les classes de conjugaison de G, donc $H = G$.

c) Regardons l'action transitive de G par conjugaison sur l'ensemble Syl_p de ses p-Sylow. Comme G est simple $n_p > 1$. On obtient donc un morphisme non trivial $G \to \mathcal{S}_{\mathrm{Syl}_p} \simeq \mathcal{S}_{n_p}$. Puisque G est simple ce morphisme est injectif. Il en résulte que $|G|$ divise $|\mathcal{S}_{n_p}| = n_p!$.

d) Soit G un groupe simple d'ordre 60. Montrons que le nombre de 2-Sylow de G est égal à 5 ou à 15.

Soit n_2 le nombre de 2-Sylow. Les théorèmes de Sylow assurent que n_2 est impair et divise 15 ; par suite n_2 appartient à $\{1, 3, 5, 15\}$. Le groupe G étant simple, $n_2 \neq 1$, *i.e.* n_2 appartient à $\{3, 5, 15\}$. Le groupe G est d'ordre $2^2 \cdot 15$; d'après le c) $|G|$ divise $n_2!$ donc $n_2 \neq 3$. Ainsi n_2 vaut 5 ou 15.

e) Montrons que G contient un sous-groupe d'ordre 12.

Supposons dans un premier temps que $n_2 = 5$; alors le normalisateur d'un 2-Sylow de G est de cardinal $60/5 = 12$ d'où le résultat.

Supposons désormais que $n_2 = 15$. Montrons qu'il existe deux 2-Sylow distincts S et S tels que $|S \cap T| = 2$. Sinon on aurait exactement $15 \cdot 3 + 1 = 46$ éléments d'ordre divisant 4. De plus les théorèmes de Sylow assurent que $n_5 = 6$ donc que G contient $6 \cdot 4 = 24$ éléments d'ordre 5. Ainsi d'une part G contient au moins $46+24 = 70$ éléments et d'autre par $|G| = 60$: contradiction. On dispose donc de deux 2-Sylow distincts S et S tels que $S \cap T = \{e, g\}$ avec g d'ordre 2. Désignons par H le centralisateur de g dans G. Alors H contient S et S donc son cardinal est multiple de 4 et > 6. Ainsi $|H|$ appartient à $\{12, 20, 60\}$. Si $|H| = 20$, alors l'action transitive de G sur G/H induit un morphisme injectif $G \to \mathcal{S}_{G/H} \simeq \mathcal{S}_3$: contradiction. Si $|H| = 60$, alors g est dans le centre de G ce qui assure que le centre $Z(G)$ de G est non trivial : contradiction avec le fait que G est simple. Il s'en suit que $|H| = 12$.

f) Soit H le sous-groupe de G d'ordre 12 construit au e). L'action transitive de G sur G/H induit un morphisme injectif $\varphi\colon G \to \mathcal{S}_{G/H} \simeq \mathcal{S}_5$. Alors $\varphi(G) \cap \mathcal{A}_5$ est un sous-groupe distingué de $\varphi(G)$ qui est simple donc $\varphi(G) \cap \mathcal{A}_5 \in \{\mathrm{id}, \mathcal{A}_5\}$. Dans le premier cas on en déduit que $|\varphi(G)| \leq 2$ (en composant avec la signature) : contradiction. Par suite $\varphi(G)$ contient $\mathcal{A}_5$. Par cardinalité on obtient que φ induit bien un isomorphisme $G \simeq \mathcal{A}_5$.

Exercice 28. Trouver l'ordre du groupe G qui satisfait les conditions suivantes :

a) G est un sous-groupe d'un groupe d'ordre 100,

b) G ne contient pas d'élément d'ordre 2,

c) G n'est pas cyclique.

Éléments de solution 28.

Soit G un groupe tel que

a) G est un sous-groupe d'un groupe d'ordre 100,

b) G ne contient pas d'élément d'ordre 2,

c) G n'est pas cyclique.

D'après a) $|G|$ divise 100, *i.e.* $|G| \in \{1, 2, 4, 5, 10, 20, 25, 50, 100\}$.
D'après b) $|G|$ n'est pas un multiple de 2 d'où $|G| \in \{1, 5, 25\}$.
D'après c $|G| = 25$.

Exercice 29. [Groupe symétrique, Dummit-Foot, page 127 et page 132 exercice 33]

a) Déterminer le nombre de permutations conjuguées à un m-cycle dans $\mathcal{S}_n$.

b) Trouver toutes les classes de conjugaison de $\mathcal{S}_4$ et leurs cardinaux.

c) Donner la liste des sous-groupes distingués de $\mathcal{S}_4$.

d) Donner la liste des sous-groupes de $\mathcal{S}_4$.

Éléments de solution 29.

Exercice 30. [Groupe alterné, classes de conjugaison, Perrin, page 16 lemme 4.11]
Montrer que pour $n \geq 5$, les 3-cycles sont conjugués dans $\mathcal{A}_n$.

Éléments de solution 30.

Exercice 31. [Groupe symétrique, Perrin, page 13 exemple 3.2.2]
Déterminer le centre du groupe $\mathcal{S}_n$.

Éléments de solution 31.

Si $n = 2$, on a $Z(\mathcal{S}_2) = \mathcal{S}_2$.

Supposons $n \geq 3$. Soient a, b dans $\{1, 2, \ldots, n\}$ et σ dans $\mathcal{S}_n$. Montrer que

$$\sigma \circ (a\ b) \circ \sigma^{-1} = (\sigma(a)\ \sigma(b))$$

Soit σ un élément du centre de $\mathcal{S}_n$. En particulier $\sigma \circ (1\ 2) = (1\ 2) \circ \sigma$, *i.e.* $\sigma \circ (1\ 2) \circ \sigma^{-1} = (1\ 2)$. Par suite (a))

$$(\sigma(1)\ \sigma(2)) = (1\ 2).$$

Ainsi nécessairement $\sigma(1) = 1$ ou $\sigma(1) = 2$. De même $\sigma \circ (1\ 3) = (1\ 3) \circ \sigma$ et donc

$$(\sigma(1)\ \sigma(3)) = (1\ 3).$$

Il en résulte que $\sigma(1) = 1$. Ce qu'on a fait avec 1 peut être fait avec n'importe quel entier compris entre 2 et n. Il en résulte que $\sigma = \mathrm{id}$.

Réciproquement id commute avec toutes les permutations.

Exercice 32.

a) Soient G un groupe fini et N un sous-groupe distingué de G.
Soit $g \in \mathrm{G}$ tel que $\mathrm{pgcd}(o(g), [\mathrm{G} : \mathrm{N}]) = 1$. Montrer que $g \in \mathrm{N}$.

b) Montrer que $\mathcal{A}_4$ n'a pas de sous-groupe d'ordre 6.

c) Montrer que $\mathcal{A}_5$ est un groupe simple.

Éléments de solution 32.

Exercice 33. [Variation aux colliers de Pólya, Armstrong, pages 98-100]
On souhaite dénombrer le nombre de cubes distincts que l'on peut fabriquer en coloriant chacune de ses faces ou bien avec de la peinture rouge, ou bien avec de la peinture verte. Deux cubes sont identiques s'ils le sont à une rotation près.

a) Soit G un groupe opérant sur un ensemble X. Soient g et h conjugués dans G. Montrer que

$$\big|\,\mathrm{fix}(g)\,\big| = \big|\,\mathrm{fix}(h)\,\big|$$

en construisant une bijection entre ces ensembles.

b) En appliquant la formule de Burnside à l'action du groupe des symétries rotationelles sur l'ensemble de tous les cubes possibles (sans identification), montrer qu'il y a 10 types de cubes distincts.

Éléments de solution 33.

Exercice 34. [Szpirglas, p. 98 exercice 5]
Montrer que $\mathcal{S}_4$ possède trois 2-sous-groupes de Sylow isomorphes à D_8.

Éléments de solution 34. Le groupe $\mathcal{S}_4$ est d'ordre $24 = 2^3 \times 3$. Par ailleurs D_8 est le groupe des isométries du plan qui conservent un carré donc $\mathrm{D}_8 \subset \mathcal{S}_4$.

Soit n_2 le nombre de 2-Sylow de $\mathcal{S}_4$. Le groupe D_8 est l'un de ces 2-Sylow. Les théorèmes de Sylow assurent que n_2 divise 3 et $n_2 \equiv 1 \bmod 2$. Il s'en suit que $n_2 \in \{1, 3\}$. Si $n_2 = 1$, alors D_8 est distingué dans $\mathcal{S}_4$. Désignons les sommets du carré préservé par D_8 par 1, 2, 3 et 4 dans l'ordre où on les rencontre lorsqu'on se déplace dans le sens positif sur ce carré. Soit s la symétrie par rapport à la médiatrice de $[1, 4]$ et $[2, 3]$. C'est la permutation $(1\ 4)(2\ 3)$. Notons que $(1\ 3)s(1\ 3) = (2\ 3)$ n'appartient pas à D_8 (en effet les deux seules transpositions qui appartiennent à D_8 sont les symétries par rapport aux deux diagonales du carré, soit $(1\ 3)$ et $(2\ 4)$). Ainsi D_8 n'est pas distingué dans $\mathcal{S}_4$. Il y a donc 3 sous-groupes d'ordre 8 qui sont conjugués donc isomorphes. Ces trois sous-groupes sont les trois 2-Sylow de $\mathcal{S}_4$.

Exercice 35. Soit G un groupe fini d'ordre $|\mathrm{G}| = p^a m$ avec p premier et $\mathrm{pgcd}(p, m) = 1$. Soient $\mathrm{S} \subset \mathrm{G}$ un p-Sylow et H un sous-groupe de G. Montrer qu'il existe $g \in \mathrm{G}$ tel que $g\mathrm{S}g^{-1} \cap \mathrm{H}$ soit un p-Sylow de H.

Éléments de solution 35. On a $|\mathrm{G}| = p^a m$ et $|\mathrm{H}| = p^b n$. On fait agir G (et donc également H) par translation sur l'ensemble X des classes à gauche de G modulo S. Notons que $g' \in \mathrm{Stab}(g\mathrm{S})$ équivaut à $g' \in g\mathrm{S}g^{-1}$. Par ailleurs l'ensemble X est de cardinal m qui n'est pas un multiple de p. L'une des orbites Ω de X sous l'action de H est donc de cardinal p^c pour un certain $c \leq b$. Mais comme de plus $|\mathrm{Stab}(x)| \cdot |\Omega| = |\mathrm{H}| = p^b n$ et $\mathrm{pgcd}(|\Omega|, p) = 1$ on a finalement $|\Omega| = n$ et $|\mathrm{Stab}(x)| = p^b$ comme attendu.

Exercice 36.

(1) Soient $\Bbbk$ un corps et G un groupe fini. Montrer qu'il existe un entier n tel que G soit isomorphe à un sous-groupe de $\mathrm{GL}_n(\Bbbk)$. [Indication : on pourra commencer par plonger G dans un groupe symétrique.]

(2) Soit $\mathbb{F}_p$ le corps à p éléments où p désigne un nombre premier. Montrer que le groupe des matrices triangulaires supérieures avec des 1 sur la diagonale est un p-Sylow de $\mathrm{GL}_n(\mathbb{F}_p)$.

Éléments de solution 36.

(1) Tout groupe fini se plonge dans un groupe symétrique $\mathcal{S}_n$ en faisant agir G sur lui-même par translation ce qui montre que $n = |\mathrm{G}|$ convient. De plus le groupe symétrique $\mathcal{S}_n$ se plonge dans $\mathrm{GL}(n, \Bbbk)$ pour tout corps $\Bbbk$ en faisant agir $\mathcal{S}_n$ sur les vecteurs d'une base de $\Bbbk^n$.

(2) Le cardinal de $\mathrm{GL}(\mathbb{F}_p)$ est (compter les base de $(\mathbb{F}_p)^n$

$$|\mathrm{GL}(n, \mathbb{F}_p)| = (p^n - 1)(p^n - p)(p^n - p^2) \dots (p^n - p^{n-1}) = p^{1+2+\dots+(n-1)} m$$

avec $\mathrm{pgcd}(m, p) = 1$. Or $p^{1+2+\dots+(n-1)}$ est le cardinal du groupe des matrices triangulaires unipotentes.