# FEUILLE N° 5

LU3MA270 – 2023/24

**Exercice 1.** *On considère l'application $\tau\colon G \to S_G$ donnée par l'action de $G$ sur lui-même par translations : $g \mapsto (\tau_g\colon x \mapsto g * x)$. C'est un morphisme de groupes : $\tau_{g*h} = \tau_g \circ \tau_h$. C'est une injection, d'inverse à gauche $\sigma \mapsto \sigma(e)$. Le groupe $G$ est isomorphe au sous-groupe $\tau(G) \subseteq S_G$. En numérotant arbitrairement les éléments de $G = \{g_1, \dots, g_n\}$, on a aussi un isomorphisme $S_n \simeq S_G$ donné par $\sigma \mapsto (g_i \mapsto g_{\sigma(i)})$. En conclusion, $G$ est isomorphe à un sous-groupe de $S_n$.*

**Exercice 2.** *Une permutation $\sigma$ de $S_n$ est uniquement déterminée par son écriture en cycles disjoints. La preuve de l'existence de cette écriture montre que les cycles disjoints sont les orbites du sous-groupe $\langle\sigma\rangle$. Il est clair que les points fixes de $\sigma$ sont les orbites de taille $1$ de cette action. Pour chaque permutation, on considère la partition de $\{1, \dots, n\}$ en orbite. Si on associe à chaque orbite sa taille, on obtient une partition entière de $n$, et le nombre de $1$ est le nombre de points fixes de $\sigma$.*
*<u>Si $n = 3$</u> : Les partitions entières de $3$ sont*

$$3 = 3 = 2 + 1 = 1 + 1 + 1.$$

- *Il y a $1 = \binom{3}{3}$ partition qui donne $3 = 3$, et il y a $2!$ cycles dont le support donne le même ensemble de cardinal $3$ : on choisit le successeur d'un élement, puis le successeur du successeur, etc. . .*
- *Il y a $3 = \binom{3}{2,1}$ partitions qui donnent $3 = 2 + 1$, et il y a $1!0!$ produit de cycles qui donne chaque partition.*
- *Il y a $1 = \binom{3}{1,1,1} * \frac{1}{3!}$ partitions qui donnent $3 = 1 + 1 + 1$ (on peut permuter les ensembles de même taille et on obtient la même partition), et il y a $0!0!0!$ produit de cycles qui donne cette partition.*

*Le nombre moyen de points fixes est donc :*

$$\frac{1}{3!}(2 * 0 + 3 * 1 + 1 * 3) = 1.$$

*<u>Si $n = 4$</u> : Les partitions entières de $4$ sont*

$$4 = 4 = 3 + 1 = 2 + 2 = 2 + 1 + 1 = 1 + 1 + 1 + 1.$$

- *Il y a $1 = \binom{4}{4}$ partition qui donne $4 = 4$, et il y a $3!$ cycles qui donne cette partition.*
- *Il y a $4 = \binom{4}{3,1}$ partitions qui donnent $4 = 3 + 1$, et il y a $2!0!$ produits de cycles qui donnent chaque partition.*
- *Il y a $3 = \binom{4}{2,2} * \frac{1}{2!}$ partitions qui donnent $4 = 2 + 2$, et il y a $1!1!$ produit de cycles qui donne chaque partition.*
- *Il y a $6 = \binom{4}{2,1,1} * \frac{1}{2!}$ partitions qui donnent $4 = 2 + 1 + 1$, et il y a $1!0!0!$ produit de cycle qui donne chaque partition.*
- *Il y a $1 = \binom{4}{1,1,1,1} * \frac{1}{4!}$ partitions qui donnent $4 = 1 + 1 + 1 + 1$, et il y a $0!0!0!0!$ produit de cycles qui donne cette partition.*

*Le nombre moyen de points fixes est donc :*

$$\frac{1}{4!}(6*0+8*1+3*0+6*2+1*4)=1.$$

*Cas général : on va utiliser la formule de Burnside. Le groupe $S_n$ opère sur l'ensemble $E=\{1,\dots,n\}$. Comme $(i,1)(1)=i$, l'action de $S_n$ est transitive : il n'y a qu'une orbite. Soit $\Omega=\{E\}\subset\mathcal{P}(E)$ le quotient de $E$ par cette action. On a :*

$$1=\#\Omega=\frac{1}{|S_n|}\sum_{\sigma\in S_n}\#(E^\sigma),$$

*où $E^\sigma$ désigne les points de $E$ stabilisés par $\sigma$. On en conclut que le nombre moyen de points fixes d'une permutation de $S_n$ est* 1.

**Exercice 3.**

(a) *Une permutation $\sigma$ envoie des sous-ensembles disjoints sur des sous-ensembles disjoints par injectivité, et conserve le cardinal des sous-ensembles par bijectivité. On a donc une application naturelle $\mathcal{D}(n,i_1,\dots,i_r)\to\mathcal{D}(n,i_1,\dots,i_r)$ donnée par*

$$\sigma\cdot(I_1,\dots,I_r)=(\sigma(I_1),\dots,\sigma(I_r)).$$

*On a bien $\sigma_1\cdot\sigma_2\cdot\mathbb{I}=(\sigma_1\circ\sigma_2)\cdot\mathbb{I}$ et $\mathrm{id}\cdot\mathbb{I}=\mathbb{I}$.*

*L'action est transitive : étant donné $\mathbb{I}=(I_1,\dots,I_r)\in\mathcal{D}(n,i_1,\dots,i_r)$, on numérote les éléments de $I_1$ arbitrairement de 1 à $i_1$, ceux de $I_2$ de $i_1+1$ à $i_1+i_2$, etc...Alors $\mathbb{I}$ est l'image de $(\{1,\dots,i_1\},\{i_1+1,\dots,i_1+i_2\},\dots)$ par la permutation $\sigma$ qui à $j$ associe l'élément numéroté $j$. Tous les éléments de $\mathcal{D}(n,i_1,\dots,i_r)$ sont donc dans la même orbite.*

(b) *Si $\sigma$ fixe $\mathbb{I}=(I_1,\dots,I_r)\in\mathcal{D}(n,i_1,\dots,i_r)$, alors pour tout $j$, la restriction de $\sigma$ à $I_j$ à la source et au but est une permutation. Inversement étant donné des permutations respectives $\sigma_1,\dots,\sigma_r$ de $I_1,\dots,I_r$, on définit une permutation $\sigma$ qui fixe $\mathbb{I}$ en posant $\sigma(k)=\sigma_j(k)$ si $k\in I_j$. On en déduit que le stabilisateur de $\mathbb{I}$ est de cardinal $\prod_{j=1}^r i_j!$.*

*La formule des classes donne maintenant :*

$$\#\mathcal{D}(n,i_1,\dots,i_r)=\#\mathcal{O}_{\mathbb{I}}=\frac{|S_n|}{|\mathrm{Stab}(\mathbb{I})|}=\frac{n!}{i_1!\cdots i_r!}=\binom{n}{i_1,\dots,i_r}.$$

(c) *On note $\mathcal{D}(n;r)$ l'ensemble des partitions indexées par $\{1,\dots,r\}$ de $\{1,\dots,n\}$. On peut voir $\mathcal{D}(n;r)$ comme l'ensemble des applications $\{1,\dots,n\}\to\{1,\dots,r\}$ en considérant la bijection qui à une application associe ses fibres. On a*

$$(x_1+\cdots+x_r)^n=\sum_{1\le k_1,\dots,k_n\le r}x_{k_1}\cdots x_{k_r}=\sum_{\mathbb{I}\in\mathcal{D}(n;r)}x_1^{\#I_1}\cdots x_r^{\#I_r},$$

*où on a noté $I_j=\{i\colon k_j=i\}$. Or $\mathcal{D}(n;r)$ est l'union disjointe pour $i_1+\cdots+i_r=n$ des ensembles $\mathcal{D}(n,i_1,\dots,i_r)$, d'où :*

$$(x_1+\cdots+x_r)^n=\sum_{i_1+\cdots+i_r=n}\sum_{\mathbb{I}\in\mathcal{D}(n,i_1,\dots,i_r)}x_1^{i_1}\cdots x_r^{i_r}.$$

*D'après la question précédente :*

$$(x_1+\cdots+x_r)^n=\sum_{i_1+\cdots+i_r=n}\binom{n}{i_1,\dots,i_r}x_1^{i_1}\cdots x_r^{i_r}.$$

**Exercice 4.**


darondeau@imj-prg.fr

(a) *On a* $\forall x \in H\colon x = x^{-1}$, *donc* $xy = (y^{-1}x^{-1})^{-1} = yx$.

*On raisonne par récurrence sur l'ordre de H fini. Si* $|H| = 1$, *on a bien* $1 = 2^0$. *Supposons maintenant que tout groupe fini d'ordre* $\leq n$ *tel que* $\forall x \in H\colon x^2 = e$ *ait un ordre une puissance de* 2. *Soit H d'ordre* $\leq 2n$. *Le groupe H est abélien donc pour tout* $x \neq e$, *le sous-groupe* $\{e, x\}$ *est un sous-groupe distingué d'indice n. Le groupe quotient* $H' = H/\langle x\rangle$ *est d'ordre n et la projection canonique étant un morphisme surjectif il vérifie* $\forall [y] \in H'\colon [y]^2 = [y^2] = [e]$. *Par hypothèse de récurrence, il existe k tel que* $|H'| = 2^k$. *On en déduit que* $|H| = 2^{k+1}$, *ce qui conclut la récurrence.*

*Autre correction proposée par un élève : montrer que H est un espace vectoriel sur* $\mathbb{Z}/2\mathbb{Z}$, *pour l'opération* $[k] \cdot x = k \cdot x = x + \cdots + x$.

(b) *Par le théorème de Lagrange, l'ordre de tout élément divise l'ordre de G. Les ordres possibles sont donc* $1, 2, 3, 6$.

(c) *Si x et d'ordre* $= 2$, *y est d'ordre* $= 3$ *et* $xy = yx$, *alors :*

$$(xy)^i = x^i y^i = e \implies x^i = y^{-i}.$$

*or par le théorème de Lagrange, l'ordre de* $x^i$ *divise l'ordre de x et celui de* $y^{-i}$ *divise l'ordre de y. L'ordre de* $x^i$ *divise donc* $\mathrm{pgcd}(2, 3) = 1$. *On a donc :*

$$x^i = y^i = e.$$

*De façon équivalente i est un multiple de l'ordre de x et de celui de y, c'est-à-dire de* $6 = \mathrm{ppcm}(2, 3)$. *On obtient que le groupe* $G = \langle xy\rangle$ *est cyclique, donc isomorphe à* $\mathbb{Z}/6\mathbb{Z}$.

(d) *On suppose que G n'est pas cyclique. L'ordre de ses éléments est donc* $1, 2$ *ou* 3. *Si G n'a pas d'éléments d'ordre* 3, *on a* $\forall x \in G\colon x^2 = e$. *On en déduit que* $|G|$ *est une puissance de deux, une contradiction. Donc G a un élément d'ordre* 3.

(e) *L'inverse d'un élément x d'ordre* 3 *est pair et distinct de x (sinon on aurait* $x^2 = e$). *On peut donc arranger les éléments d'ordre* 3 *en paires : en particulier le nombre d'éléments d'ordre* 3 *est pair.*

(f) *Le neutre est d'ordre* 1 *et le nombre d'éléments d'ordre* 3 *est pair, donc le nombre d'éléments d'ordre* 2 *est impair. En particulier ce nombre est non-nul.*

(g) *Le sous-groupe* $\{e, x\}$ *est inclus dans le sous-groupe* $\mathrm{Stab}(x)$, *donc par le théorème de Lagrange, l'ordre de* $\mathrm{Stab}(x)$ *est pair. C'est aussi un diviseur de* 6. *C'est donc* 2 *ou* 6. *Si c'est* 6, *x est dans le centre de G, et il commute avec l'élément d'ordre* 3. *D'après la question* (c), *G est cyclique, ce qui est exclu. L'ordre du stabilisateur de x est donc* 2 *et ainsi* $\mathrm{Stab}(x) = \{e, x\}$.

(h) *On a par la formule des classes :*

$$\#(G \cdot x) = |G|/|\mathrm{Stab}(x)|,$$

*d'où* $\#(G \cdot x) = 3$.

(i) *L'orbite* $\omega$ *est stable par l'action de G. On peut donc définir la restriction de l'application* $h \mapsto g \cdot h$ *à* $\omega$ *à la source et au but. Elle est injective comme restriction d'un application injective. Elle est bijective comme injection entre deux ensembles finis de même taille. Elle respecte les axiomes des actions par restriction à* $\omega$ *des propriétés vraies dans G.*

*Soit* $\mu\colon G \to S_\omega$ *le morphisme de groupes correspondant. On a*

$$\ker(\mu) = \bigcap_{g \in \omega} \mathrm{Stab}(g) \subseteq \mathrm{Stab}(x) = \{e, x\}.$$

*Par ailleurs,* $\mathrm{Stab}(x) = \mathrm{Fix}(x) = \{e, x\}$, *donc x ne peut pas fixer les* 3 *éléments de* $\omega$. *On a donc* $\ker(\mu) = \{e\}$. *L'application* $G \to S_\omega$ *est donc un morphisme injectif entre deux*


darondeau@imj-prg.fr

*groupes finis de même ordre. On en conclut que c'est un morphisme bijectif, c'est-à-dire un isomorphisme.*

**Exercice 5.** *(a) Si $x_1x_2\cdots x_p = 1$, alors en simplifiant $x_1^{-1} = x_2\cdots x_p$. Donc $x_2\cdots x_px_1 = 1$. On a $\sigma^p = \mathrm{id}$ et $p$ premier donc l'ordre de $\sigma$ est 1 ou $p$. Si $p > 2$ et $\sigma = \mathrm{id}$, comme pour tout $g \in G$, $(g, g^{-1}, e, \ldots, e) \in E$, on a $g = e$. Alors $G = \{e\}$ donc $|G|$ n'a pas de facteur premier. On conclut que $\sigma$ est d'ordre $p$.*

*[ Si $p = 2$ et $\sigma = \mathrm{id}$, comme pour tout $g \in G$, $(g, g^{-1}) \in E$, on obtient que tous les éléments sont de 2-torsion. Comme $|G| \geq 2$, on obtient un élément $g \neq e$, qui est nécessairement d'ordre 2. Ceci finit l'exercice. On suppose donc dans la suite que $\sigma$ est d'ordre 2. ]*

*(b) On considère l'action de $\langle\sigma\rangle$ sur $E$. Remarquons que pour $\sigma^i \neq \mathrm{id}$, l'élément $(x_1, \ldots, x_p)$ est fixé par $\sigma^i$ si et seulement si $x_1 = \cdots = x_p$. En particulier ceci ne dépend pas de $i$. On note $\Omega$ le quotient de $E$ par l'action de $\langle\sigma\rangle$. La formule de Burnside donne :*

$$\#\Omega * p = \#E + (p-1)\#(E^\sigma).$$

*Le nombre $p$ est premier et il divise $\#E = |G|^{p-1}$, donc il divise $(p-1)\#(E^\sigma)$ et donc $\#(E^\sigma)$. D'autre part $(e, \ldots, e) \in E^\sigma$. Donc $\#(E^\sigma)$ est un multiple strictement positif de $p$. Il est en particulier supérieur à 2.*

*Rappelons que l'élément $(x_1, \ldots, x_p)$ est fixé par $\sigma$ si et seulement si $x_1 = \cdots = x_p$. L'existence d'au moins deux points fixes fournit donc l'existence d'un élément $x \neq e$ tel que $x^p = e$.*

**Exercice 6.** *(a) L'ordre de $G/H$ est $p > 1$. Soit $g \in G$ tel que $[g] \neq [e]$. alors $f(g)([e]) = [g]$. L'élément $f(g)$ est non-trivial donc $f(G)$ est non-trivial.*

*(b) L'ordre de $G/H$ est $p$ donc le cardinal de $S_{G/H}$ est $p!$.*

*(c) L'image du groupe $G$ par le morphisme $f$ est un sous-groupe de $S_{G/H}$. Par le théorème de Lagrange, son ordre divise $|S_{G/H}| = p!$ Les facteurs premiers de $|f(G)|$ sont donc tous inférieurs à $p$. Si le plus petit facteur premier de $|f(G)|$ est $p$ alors $|f(G)| = p$, car $v_p(p!) = 1$. Sinon, $|f(G)| > 1$ admet un diviseur premier $q$ strictement inférieur à $p$. Par le théorème de Noether on a aussi $|f(G)|$ divise $|G|$. L'entier $p$ étant le plus petit facteur premier de $|G|$, on aboutit à une contradiction.*

*(d) Le groupe $f(G)$ est d'ordre $p$, or par le théorème d'isomorphisme de Noether,*

$$|G| = |f(G)||\ker(f)|.$$

*On en déduit que $\ker(f)$ est d'indice $p$. Or si $g \in \ker(f)$, alors $g \cdot [e] = [g] = [e]$, donc $g \in H$. En résumé $\ker(f)$ est un sous-groupe de $H$ de même indice, donc $\ker(f) = H$.*

*En conclusion, le sous-groupe $H$ est le noyau d'un morphisme de groupes, donc il est distingué.*

**Exercice 7.** *(a) Soit $T_n$ l'ensemble des matrices triangulaires supérieures avec des 1 sur la diagonale. Cet ensemble est non-vide et stable par produit et passage à l'inverse. C'est un sous-groupe de $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$. En considérant la partie triangulaire supérieure stricte, on compte que $T_n$ a $p^{n(n-1)/2}$ éléments. En conclusion, c'est un $p$-groupe.*

*Comme $T_n$ est un $p$-groupe, tous ses sous-groupes sont des $p$-groupes (par Lagrange). La conjugaison par un élément est une bijection, donc tous les conjugués des sous-groupes de $T_n$ sont aussi des $p$-groupes.*

*(b) Le groupe $G$ agit sur l'espace $X = (\mathbb{Z}/p\mathbb{Z})^n$. Supposons que $G \subseteq \mathrm{Gl}_n(\mathbb{Z}/p\mathbb{Z})$ soit un $p$-groupe. On sait que le cardinal d'une orbite divise $|G|$, donc c'est une puissance de*


darondeau@imj-prg.fr

*$p$. En particulier $p$ divise le cardinal d'une orbite sauf si l'orbite est un point fixe. Par ailleurs $X$ est la réunion disjointe de ses orbites. On en déduit que*

$$\#X \equiv \#X^G \mod p.$$

*Or $p \mid \#X$, donc $p \mid \#X^G$. Le point $0$ étant fixé, on a $\#X^G \geq p \geq 2$. Il existe au moins un point fixe non-nul.*

*On a prouvé qu'il existe $X_1$ tel que pour tout $M \in G$, on ait $(M - I_n)X_1 = 0$. On raisonne par récurrence. Supposons qu'on ait une famille $(X_1, \ldots, X_i)$ telle que pour tout $i$, et pour tout $M \in G$ : $(M - I_n)X_i \in \mathrm{Vect}(X_1, \ldots, X_{i-1})$. La famille $(X_1, \ldots, X_i)$ est libre (c'est un exercice élémentaire d'algèbre linéaire). On la complète en une base de $E$, et on considère la matrice $M'$ de l'endomorphisme sur le supplémentaire $E'$ de $\mathrm{Vect}(X_1, \ldots, X_i)$ induit par $M$ (on restreint à la source et au but). Par triangularité par blocs, pour deux matrices $M_1, M_2 \in G$ on a $(M_1M_2)' = (M_1)'(M_2)'$, donc l'image $G'$ de $G$ est un sous-groupe de $M_{n-i}(\mathbb{Z}/p\mathbb{Z})$. De plus par Noether $G'$ est un groupe quotient du $p$-groupe $G$. C'est donc un $p$-groupe. On en déduit qu'il existe un vecteur $Y$ fixé par tous les $M' \in G'$. Soit $X_{i+1}$ l'image de $Y$ par l'injection $E' \subseteq E$ donnée par notre choix de base. On a pour tout $M \in G$ : $(M - I_n)(X_{i+1}) \in \mathrm{Vect}(X_1, \ldots, X_i)$, puisque la projection $(M' - I)(Y)$ sur $E'$ est nulle.*

*On obtient finalement une base $\mathcal{B} = (X_1, \ldots, X_n)$ telle que pour tout $i$, et pour tout $M \in G$ : $(M - I_n)X_i \in \mathrm{Vect}(X_1, \ldots, X_{i-1})$. Soit $P$ la matrice de passage de la base canonique à $\mathcal{B}$. Pour tout $M \in G$, la matrice $P^{-1}(M - I_n)P$ est triangulaire supérieure stricte.*



darondeau@imj-prg.fr