Groupes. Piqûre de rappel.

On présente ici le prérequis de théorie des groupes pour le M1 d'algèbre.

1 Groupes, morphismes et actions de groupes.

Un groupe $(G, *)$, ou plus simplement G, est un ensemble muni d'une opération interne * vérifiant les propriétés suivantes :
G1 : L'opération est associative, ie $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$
G2 : G possède un élément neutre e, ie $e * g = g * e = g$
G3 : Tout élément g de G possède un symétrique g', ie $g' * g = g * g' = e$.

Dans ce cas, on sait montrer qu'un élément neutre est unique et que pour tout g de G, son symétrique est unique, il sera noté g^{-1}. Remarquons en passant que $(g^{-1})^{-1} = g$ et que $(h * g)^{-1} = g^{-1} * h^{-1}$, on dit que l'inversion est un antiautomorphisme involutif. On a plus généralement que tout élément de G est régulier, ie pour tout g de G $g * a = g * b$ implique que $a = b$.
Si de plus * est commutative, ie $g_1 * g_2 = g_2 * g_1$, alors on dit que G est abélien.
Exemple fondamental. Si X est un ensemble, l'ensemble des bijections de X dans X muni de la composition des applications est un groupe, noté $\mathcal{S}(X)$. De la même manière que l'individu n'est pas grand chose sans connexion, les groupes ne sont rien sans leurs morphismes :

Définition 1 *Soient $(G, *)$ et $(H, .)$ deux groupes et ϕ une application de G dans H. On dit que ϕ est un morphisme de groupes si ϕ vérifie*

$$\phi(g_1 * g_2) = \phi(g_1).\phi(g_2).$$

Dans ce cas, on montre que ϕ envoie l'élément neutre de G sur l'élément neutre de H et le symétrique de g sur le symétrique de $\phi(g)$.
On dit que ϕ est un isomorphisme s'il est de plus bijectif (dans ce cas son inverse est aussi un morphisme) et que c'est un automorphisme si de plus $H = G$.
Un exemple célèbre et incontournable d'automorphisme est l'automorphisme intérieur que l'on peut construire pour tout g de G. On pose $\phi_g(h) := ghg^{-1}$ et on montre que ϕ_g est un automorphisme de G appelé automorphisme intérieur. Bien sûr, si G est abélien, cet automorphisme n'est rien d'autre que l'automorphisme trivial : l'identité.
L'efficacité et l'ubiquité des groupes proviennent de leur action sur des ensembles :

Définition 2 *Soit $(G, *)$ un groupe et X un ensemble. On dit que G agit sur X s'il existe une application $\varphi : G \times X \to X$, $(g, x) \mapsto g.x$ qui vérifie :*
A1 : $e.x = x$
A2 : $g_1.(g_2.x) = (g_1 * g_2).x$.

Une façon équivalente, plus abstraite, mais plus féconde, de définir une action du groupe G sur l'ensemble X, se fait par un morphisme ϕ de G vers $\mathcal{S}(X)$. Effectivement, on construit ϕ à partir de φ par

$$\phi : G \to \mathcal{S}(X), \text{ avec } \phi(g)(x) = \varphi(g, x).$$

Inversement, on construit φ à partir de ϕ par

$$\varphi : G \times X \to X, \ (g, x) \mapsto \phi(g)(x).$$

Remarque. Notons que si G agit sur X, alors G agit sur l'ensemble des applications de X dans un ensemble Y par $g.f = f \circ \phi(g^{-1})$, et il agit sur l'ensemble des applications de Y vers X par $g.f = \phi(g) \circ f$.
Une première propriété importante d'une action de groupe est qu'elle partitionne l'ensemble X :

Définition 3 *Soit G un groupe agissant sur un ensemble X. On appelle orbite pour l'action tout sous-ensemble de X de la forme $\mathcal{O}_x := \{g.x, \ g \in G\}$, où x est fixé dans X. On appelle en particulier $\mathcal{O}_x$ l'orbite de x.*

Proposition 1 *Si G est un groupe agissant sur X, alors les orbites pour cette action forment une partition de X.*

2 Sous-groupes, classes à gauche, groupes quotients.

Les sous-groupes et les classes qu'on peut leur associer jouent un rôle important dans l'étude des actions. De plus, lorsque le sous-groupe sera *distingué*, on pourra définir une notion de groupe quotient. Les notions de sous-groupes et de groupes quotient permettent souvent de diviser en deux la complexité liée à un groupe.
Soit $(G, *)$ un groupe et H un sous-ensemble de G, H est appelé naturellement sous-groupe de G si H muni de l'opération * est aussi un groupe. On préfère l'axiomatisation plus simple suivante :

Définition 4 *Soit $(G, *)$ un groupe et H un sous-ensemble de G, alors H est appelé sous-groupe de G s'il vérifie*
SG1 : H est non vide
SG2 : Si h_1, h_2 sont dans H, alors $h_1 * h_2^{-1}$ est aussi dans H.

Exemple Un exemple classique de sous-groupe est l'image $\mathrm{Im}(\phi)$ d'un morphisme ϕ.
Le sous-groupe H agit alors sur G par $H \times G \to G$, $(h, g) \mapsto h * g$ et les orbites pour cette action sont appelées classes à droite de G. Les orbites sont de la forme $H * g = \{h * g,\ h \in H\}$ qui sera souvent notée $[g]$ dans le contexte. Les classes à droite forment donc une partition de G et on pose $H\backslash G = \{[g], g \in G\}$.
De même, on définit les classes à gauche : $g * H = \{g * h,\ h \in H\}$ et l'ensemble des classes forment aussi une partition (même si $G \times H \to G$, $(g, h) \mapsto g * h$ ne définit pas une action car A2 n'est pas vérifiée). On notera G/H l'ensemble des classes à gauche.
Les classes à gauche ont un lien important avec les orbites :

Proposition 2 *Soit G un groupe agissant sur un ensemble X et soit x dans X. Alors,*
(i) Le stabilisateur $G_x := \{g \in G,\ g.x = x\}$ de x est un sous-groupe de G
(ii) L'application $G/G_x \to \mathcal{O}_x$, $[g] \mapsto g * x$ est bien définie et établit une bijection (ensembliste)
(iii) Si $y = g * x$ est dans l'orbite de x alors $g * G_y * g^{-1} = G_x$, et donc les sous-groupes G_y et G_x sont isomorphes via un automorphisme intérieur de G.

Preuve : Seul (ii) demande une preuve. Le reste est laissé à titre d'exercice.
Soit g_1 pris quelconque dans la classe de g, alors on peut ecrire $g_1 = g * h$, avec $h \in G_x$. Il vient que $g_1.x = (g * h).x = g.(h * x) = g.x$. Ce qui prouve que l'application est bien définie.
La surjectivité est claire par définition d'une orbite.
Montrons l'injectivité. Supposons pour cela que g_1 et g_2 vérifient $g_1 * x = g_2 * x$. Alors, on a $(g_2^{-1} * g_1).x = g_2^{-1}.(g_1.x) = g_2^{-1}.(g_2.x) = (g_2^{-1} * g_2).x = e.x = x$. Conclusion, $g_2^{-1} * g_1 \in G_x$, donc $g_1 \in g_2 G_x$ et on a bien $[g_1] = [g_2]$. $\diamond$

En particulier, si l'action est transitive, ie s'il n'y a qu'une seule orbite, alors X est en bijection avec un quotient de G. C'est là une des clefs de l'importance des groupes en mathématiques.

Le problème est maintenant de savoir si G/H est muni d'une structure naturelle de groupe, c'est à dire si l'on peut définir une opération (encore notée *) telle que

$$[g_1 * g_2] = [g_1] * [g_2].$$

La proposition suivante donne des conditions nécessaires et suffisantes pour que cette loi soit cohérente, c'est-à-dire ne dépende pas du choix de g_1 et de g_2 dans leur classe (on multiplie en fait deux ensembles !).

Proposition 3 *Soit G un groupe et H un sous-groupe. Les conditions suivantes sont équivalentes :*

(i) G/H est muni d'une structure naturelle de groupe
(i') $H\backslash G$ est muni d'une structure naturelle de groupe
(ii) Toute classe à droite est aussi une classe à gauche, ie $g * H = H * g$ pour tout g
(iii) H est stable par tout automorphisme intérieur de G, ie $g * H * g^{-1} \subset H$ pour tout g.

Preuve : (i)⇒(iii). (i) implique en particulier que $[e] * [g^{-1}] = [e * g^{-1}] = [g^{-1}]$ et donc que $H * (g^{-1} * H) = g^{-1} * H$, en particulier comme e est dans H, $H * g^{-1} = H * g^{-1} * e \in g^{-1} * H$. Il vient que $g * H * g^{-1} \subset H$, d'où la stabilité.
(iii)⇒(ii). On a donc $g * H * g^{-1} \subset H$, mais aussi en changeant g en g^{-1}, $g^{-1} * H * g \subset H$, c'est à dire $H \subset g * H * g^{-1}$. D'où l'égalité $g * H * g^{-1} = H$ et donc $g * H = H * g$.
(ii)⇒(i). Comme (ii) est vrai, on a

$$[g_1] * [g_2] = (g_1 * H) * (g_2 * H) = g_1 * (H * g_2) * H = g_1 * (g_2 * H) * H$$

$$= (g_1 * g_2) * (H * H) = (g_1 * g_2) * H = [g_1 * g_2].$$

Comme (i) et (i') jouent des rôles similaires, on a bouclé la proposition.

◇

Définition 5 *Un sous-groupe H vérifiant une de ces conditions est appelé sous-groupe distingué de G.*

Remarques. Si G est abélien alors tout sous-groupe de G est distingué.
Si $\#G/H = 2$ alors H est distingué. (TD).

Un stabilisateur n'est en général pas distingué et il ne faut donc pas s'attendre à une structure de groupe sur G/G_x, la bijection entre quotient et orbite reste une bijection et il sera encore moins question d'isomorphisme.

Un exemple trivial de sous-groupe distingué est justement le sous-groupe trivial $\{e\}$.
Un exemple important de sous-groupe distingué est le centre d'un groupe : on appelle centre du groupe G et on notera $Z(G)$ l'ensemble des éléments qui commutent avec tous les autres éléments.

$$Z(G) := \{z \in G,\ g * z = z * g,\ \forall g \in G\}.$$

On voit facilement que $Z(G)$ est un sous-groupe et comme $z \in G$ est équivalent à $g * z * g^{-1} = z$, on a en particulier que $Z(G)$ est stable par tout automorphisme intérieur et il est donc distingué.
On montre facilement que la préimage d'un sous-groupe distingué par un morphisme est encore un sous-groupe distingué (ce n'est d'ailleurs pas vrai pour

l'image). En particulier le noyau d'un morphisme est un sous-groupe distingué du groupe de départ. Rappelons qu'on appelle noyau du morphisme $\phi : G \to H$ l'ensemble $\ker \phi = \phi^{-1}\{e_H\}$. Son importance réside dans le fait qu'il mesure l'injectivité d'un morphisme : un morphisme est injectif ssi son noyau est trivial.
D'ailleurs on retrouve ainsi que le centre est un sous-groupe distingué puisque le centre n'est rien autre que le noyau du morphisme pour l'action de conjugaison.
Il vient donc que $G/\ker\phi$ a une structure de groupe et on a le théorème fondamental suivant dit d'isomorphisme canonique :

Proposition 4 *Soit ϕ un morphisme d'un groupe G vers un groupe H, alors l'application $[g] \mapsto \phi(g)$ définit bien un isomorphisme canonique $\bar{\phi}$ entre les groupes $G/\ker\phi$ et $Im\phi$.*

Remarque. Cela signifie qu'un morphisme est de façon purement probabiliste une chose rare chez les groupes. Effectivement, si chez les espaces vectoriels de dimension finie, deux espaces sont isomorphes si et seulement si ils ont même dimension, la classification des groupes à isomorphisme près est beaucoup plus complexe et beaucoup plus variée. Il existe par exemple 6 groupes d'ordre 8 deux à deux non isomorphes.
Cette proposition est importante dans le sens qu'elle réduit un morphisme ϕ à l'essentiel : dans le groupe de départ, elle tue le noyau, dans le groupe d'arrivée, elle ne garde que l'image. Mais aussi importante qu'elle soit, elle n'est qu'un cas particulier du "passage au quotient" :

Proposition 5 *Soit ϕ un morphisme d'un groupe G vers un groupe H, et soit K un sous-groupe de $\ker\phi$, alors l'application $[g] \mapsto \phi(g)$ définit bien un morphisme $\bar{\phi}$ entre les groupes G/K et H. Le noyau de $\bar{\phi}$ est le quotient $\ker\phi/K$ et son image est $Im\phi$.*

3 Groupes finis.

L'étude des groupes finis reprend les résultats précédents mais utilise aussi l'arithmétique, c'est-à-dire ici, la relation "divise".
L'ordre d'un groupe est par définition son cardinal. Dans les groupes finis, les bijections obtenues précédemment donnent des égalités de cardinaux. Par exemple le théorème de Lagrange peut s'obtenir en faisant agir un sous-groupe H par multiplication à gauche sur le groupe G, le stabilisateur d'un élément étant trivial par la propriété de régularité, toutes les orbites ont $\#H$ éléments. Et donc :

Théorème 1 *L'ordre d'un sous-groupe divise l'ordre du groupe.*

On appelle ordre d'un élément g de G le plus petit entier m, $m > 0$ tel que $g^m = e$. L'ordre d'un élément g n'est rien autre que l'ordre du sous-groupe qu'il

engendre, c'est à dire le plus petit sous-groupe de G qui contient g, ou si on préfère $\{g^k,\, k \in \mathbb{Z}\}$. A l'aide d'une division euclidienne, on voit que la minimalité de m donne que

$$g^n = e \Leftrightarrow m \text{ divise } n.$$

Corollaire 1 *Si G est un groupe fini, l'ordre d'un élément divise l'ordre de G.*

Si G est un groupe fini agissant sur un ensemble fini X, on sait que X est partitionné en orbites, ce qui donne, via la bijection quotient/orbite la fameuse équation des classes :

$$\#X = \sum_{x \in X/G} \#G/\#G_x,$$

où X/G désigne l'ensemble des orbites de l'action. On note en passant que si le sous-groupe G_x dépend du choix de x dans son orbite, son ordre, lui, n'en dépend pas. On sait aussi dans ce cas calculer le nombre d'orbites, par une formule très pratique, un peu plus délicate à démontrer, la formule de Burnside :

$$\#X/G = \frac{1}{\#G} \sum_{g \in G} \#X_g,$$

où $X_g = \{x \in X,\, g.x = x\}$.

Preuve : L'idée est de calculer de deux façons différentes le cardinal de l'ensemble $R := \{(x, g), g.x = x\}$.
Si on fixe x on a $\#G_x$ possibilités pour g et on peut regrouper tous les x d'une même orbite puisque leurs stabilisateurs, étant isomorphes, ont même ordre. Cela donne :

$$\#R = \sum_{x \in X} \#G_x = \sum_{\mathcal{O}_x \in X/G} \#G_x/\#\mathcal{O}_x = \sum_{\mathcal{O}_x \in X/G} \#G_x(\#G/\#G_x) =$$

$$\sum_{\mathcal{O}_x \in X/G} \#G = (\#X/G)(\#G).$$

Si maintenant on fixe g, alors on a $\#X_g$ possibilités pour x :

$$\#R = \sum_{g \in G} \#X_g.$$

D'où l'égalité par comparaison des deux formules obtenues. ◇

Les exemples d'applications de cette formule sont nombreux, en particulier en dénombrement, par exemple dans les problèmes de coloriage ou de colliers de perles.
Une application incontournable de l'équation aux classes est dans son application à l'étude des p-groupes. Un p-groupe est un groupe dont l'ordre est une puissance de p.

Proposition 6 *Le centre d'un p-groupe est non trivial.*

Preuve : Soit G un p-groupe. Faisons agir G sur lui-même par conjugaison, ie $g.h = g * h * g^{-1}$. L'équation aux classes donne alors :

$\#G = \sum_{\mathcal{O}} \#\mathcal{O}$, où $\#\mathcal{O}$ est un quotient de $\#G$, donc une puissance de p.
Or, $z \in Z(G)$ ssi $g.z = z$ pour tout g, c'est à dire ssi l'orbite $\mathcal{O}_z$ est réduite à un point, le point z. On peut donc regrouper l'égalité précédente en $\#G = \#Z(G) + \sum_{\mathcal{O}} \#\mathcal{O}$, où cette fois-ci les $\#\mathcal{O}$ de la somme sont des puissances de p divisibles par p. Conclusion, p divise $\#Z(G)$ et ainsi, $Z(G)$ ne peut pas être réduit à l'identité. ◇

On pourrait dire que finalement, on ne sait pas grand chose sur le p-groupe G puisqu'en somme, on a juste un maigre renseignement sur son centre. Mais, en regardant de plus près, la donnée conjointe du sous-groupe $Z(G)$ et du groupe quotient $G/Z(G)$ donne des renseignements précieux sur G. De plus, $Z(G)$ est un groupe abélien fini et $G/Z(G)$ est encore un p-groupe plus "petit" que G.
En fait, on se rend compte que la classification des groupes d'ordre fini n à isomorphisme près dépend de la complexité arithmétique de n, c'est-à-dire de la complexité de sa décomposition en nombres premiers. Par exemple, il n'y a qu'un seul groupe d'ordre p premier à isomorphisme près. Effectivement, le théorème de Lagrange montre facilement qu'un tel sous-groupe est isomorphe à $\mathbb{Z}/p\mathbb{Z}$. La proposition précédente est donc un premier pas dans cette classification. Les théorèmes de Sylow, en M1-algèbre, en seront un second.

Conseil : Il faut évidemment bien connaître les théorèmes sur les groupes et leurs actions, mais la théorie des groupes se fait aussi de façon botanique. Il est bon de se familiariser (sans tomber non plus dans l'amour platonique) avec certaines classes de groupes, et certains types d'actions naturelles associées, parce que finalement, on rencontre souvent les mêmes en pratique. Citons en quelques uns.
Groupes : Groupes finis abéliens, groupes symétriques, groupes alternés, groupes (spécial)linéaires (sur n'importe quel corps, y compris les corps finis), groupes (spécial)orthogonaux.
Actions : Action naturelle ($S(X)$ sur X, $\mathrm{GL}_n(k)$ sur k^n, $\mathrm{O}_n(\mathbb{R})$ sur la $(n-1)$-sphère). Action par multiplication à gauche (d'un groupe sur lui-même), action par conjugaison.