Des chapeaux, des couleurs et des structures algébriques

Florent Benaych-Georges

http://dma.ens.fr/culturemath

Ce texte traite d'un problème, dont le premier énoncé est simple, un jeu mathématique accessible, en principe, à tout collégien. Chaque partie propose une version plus sophistiquée de la question posée initialement. Dans un premier temps, nous mettrons en évidence l'intérêt et le caractère naturel de certaines notions, comme celle de "valeur modulo n", qui généralise la notion de parité. Ensuite, dans des considérations plus théoriques, nous verrons apparaître les structures de groupe abélien, de corps et d'espace vectoriel, et nous montrerons de façon relativement simple comment munir tout ensemble infini d'une structure de corps.

La première partie est accessible dès le collège. Pour la deuxième partie, des connaissances relativement simples en arithmétique sont nécessaires : les élèves de premier cycle universitaire, de classe préparatoire scientifique et les bons élèves de terminale devraient pouvoir s'y retrouver. La partie 3 nécessite quelques notions de théorie des ensembles et la connaissance de la notion de groupe abélien : elle est accessible aux élèves de premier cycle universitaire et de classe préparatoire scientifique. La dernière partie nécessite certaines connaissances en théorie des ensembles et en algèbre : elle est accessible aux élèves de niveau licence en mathématiques.

Je tiens à remercier Mathieu Florence, qui m'a soumis le problème initial, ainsi que ses différentes sophistications.

1 Problème à deux couleurs et nombre fini de chapeaux

Commençons par une question simple.

Question : 100 personnes sont disposées en ronde (de façon à ce que chacun voit tous les autres), chacune a un chapeau, qui est soit jaune, soit bleu. Personne ne peut voir la couleur de son chapeau, mais tout le monde voit les chapeaux des autres. Le problème est de donner une stratégie qui permettra au plus grand nombre possible de personnes de connaître avec certitude la couleur de leur chapeau, les contraintes étant les suivantes :

- *une personne est désignée pour parler en premier, puis c'est le tour de la personne située à sa gauche, puis la personne suivante à gauche, et ainsi de suite ...*

– *chaque personne dit "jaune" ou "bleue", les autres entendent ce qui est dit, mais personne ne peut faire de signe, de grimace, ou quoi que ce soit qui sort de l'information binaire "jaune" et "bleue".*

Il s'agit donc de trouver une stratégie qui assurera au plus grand nombre possible de personnes de déterminer la couleur de leur chapeau en n'utilisant que les informations données par les chapeaux qu'elles voient sur les autres, et ce qu'elles ont entendu, c'est à dire les réponses données par ceux qui ont parlé avant.

Rappelons que nous cherchons une stratégie qui optimise le nombre de personnes qui sont **sûres** de donner la couleur de leur chapeau, pas le nombre moyen de personnes qui par hasard auraient dit juste, et que l'on ne fait aucune hypothèse statistique sur la distribution des chapeaux : elle est quelconque (ils peuvent être tous jaunes, tous bleus, moitié-moitié,. . .).

Exemples de stratégies :

1. une stratégie simple, qui permette à la $2^{\text{ème}}$ personne, la $4^{\text{ème}}$, la $6^{\text{ème}}$, la $8^{\text{ème}}$,. . . , la $98^{\text{ème}}$, la $100^{\text{ème}}$ de répondre juste est la suivante : la $1^{\text{ème}}$ personne à s'exprimer dit la couleur du chapeau de la $2^{\text{ème}}$, la $3^{\text{ème}}$ celle du chapeau de la $4^{\text{ème}}$,. . . , $99^{\text{ème}}$ celle du chapeau de la $100^{\text{ème}}$.
2. une stratégie qui permette à 2 personnes sur 3 d'être sures de répondre juste est la suivante : la $1^{\text{ère}}$ dit "bleue" si la $2^{\text{ème}}$ et la $3^{\text{ème}}$ ont des chapeaux de la même couleur, et "jaune" sinon. La $2^{\text{ème}}$ n'a alors qu'à regarder la couleur du chapeau de la $3^{\text{ème}}$ pour connaître la couleur du sien, et la $3^{\text{ème}}$ de même. Ensuite, la $4^{\text{ème}}$ dit "bleue" si la $5^{\text{ème}}$ et la $6^{\text{ème}}$ ont des chapeaux de la même couleur, et "jaune" sinon . . . .

Il existe une stratégie qui est meilleure que ces deux là, et meilleure, en fait, que toutes les autres :

Propriété 1.1 *Il existe une stratégie dans laquelle tous sauf le premier à parler sont assurés de connaître la couleur qu'ils portent.*

La stratégie est la suivante : le premier à parler compte le nombre de chapeaux bleus sur les têtes des autres. Si ce nombre est pair, il est convenu qu'il dit "jaune". Si ce nombre est impair, il dit "bleue". Ensuite, chacun détermine la couleur de son chapeau en comptant le nombre de chapeaux bleus portés par les autres, sans se compter (ce qui serait d'ailleurs impossible), et sans compter celui qui a parlé en premier. Si ce nombre a la parité exprimée par celui qui a parlé en premier, alors son chapeau est jaune, sinon, il est bleu. Cette stratégie permet à tous sauf au premier de déterminer avec certitude la couleur de leur chapeau. Notons qu'il n'existe pas de stratégie assurant à la personne qui s'exprime en premier de connaître la couleur de son chapeau.

2 Problème à n couleurs et nombre fini de chapeaux

Compliquons maintenant le problème en supposant que $n \geq 2$ couleurs (au lieu de deux) sont possibles pour les chapeaux. On les numérote de 0 à $n-1$. Chacun s'exprimera donc en donnant un nombre compris entre 0 et $n-1$.On note C_1 le numéro de la couleur du chapeau de la première personne, C_2 le numéro de la couleur du chapeau de la $2^{\text{ème}}$, etc. . . .

Question : existe-t-il encore une stratégie qui assure à tous sauf au premier de connaître leur couleur ?

Il pourrait sembler que c'était le caractère binaire du problème à deux couleurs qui permettait de s'en sortir en ne sacrifiant que le premier à s'exprimer. Il n'en est rien. On peut, dans cette situation, établir une stratégie analogue à la précédente.

La notion de parité sera ici remplacée par la valeur modulo n.

Définition 2.1 *Pour tout nombre entier x, on note $R_n(x)$ le reste de la division euclidienne de x par n, c'est à dire l'unique nombre de $\{0, \ldots, n-1\}$ tel que $x - R_n(x)$ soit un multiple de n.*

Exemples :
- pour $n = 10$, lorsque x est positif, $R_n(x)$ est le dernier chiffre de l'écriture décimale de x,
- pour $n = 2$, $R_n(x)$ est 0 si x est pair, et 1 si x est impair,
- pour $n = 5$,

$$\begin{aligned} R_n(0) = R_n(5) = R_n(10) = \ldots &= 0 \\ R_n(1) = R_n(6) = R_n(11) = \ldots &= 1 \\ R_n(2) = R_n(7) = R_n(12) = \ldots &= 2 \end{aligned}$$

Remarquons que dans la partie 1, l'information donnée par la première personne à s'exprimer était $x_0 = R_2(C_2 + \cdots + C_{100})$, où la couleur jaune correspond au numéro 0 et la couleur bleue correspond au numéro 1. Pour tout $k \in \{2, \ldots, 100\}$, la $k$ème personne compte alors le nombre $N_k = C_2 + \cdots + C_{k-1} + C_{k+1} + \cdots + C_{100}$ de chapeaux bleus, puis retrouve sa couleur C_k en utilisant le fait qu'il existe un unique $C_k \in \{0, 1\}$ tel que $R_2(N_k + C_k) = x_0$. Cette propriété reste vraie en remplaçant 2 par n :

Propriété 2.2

$$\forall N \in \mathbb{Z}, \forall x \in \{0, \ldots, n-1\}, \exists! C \in \{0, \ldots, n-1\} \text{ tel que } R_n(N + C) = x.$$

<u>*Démonstration*</u> : Ceci est dû au fait que l'on peut définir une loi de composition interne $+_n$ sur $\{0, \ldots, n-1\}$ par

$$\forall a, b \in \mathbb{Z}, R_n(a) +_n R_n(b) = R_n(a + b),$$

et que cette loi est une loi de groupe abélien : le nombre C en question est $x -_n R_n(N)$, soit $R_n(x - R_n(N))$.

Remarque 2.3 *Ceci se synthétise en disant qu'il existe une unique loi de composition interne $+_n$ sur $\{0, \ldots, n-1\}$ telle que l'application $R_n : (\mathbb{Z}, +) \to (\{0, \ldots, n-1\}, +_n)$ soit un morphisme, et de plus, $(\{0, \ldots, n-1\}, +_n)$ est un groupe abélien (que l'on note souvent $\mathbb{Z}/n\mathbb{Z}$). Le lecteur trouvera plus de détails, par exemple, dans [AF].*

Ainsi, pour le problème à n couleurs, la stratégie dans laquelle le premier donne l'information $x_0 = R_n(C_2 + \cdots + C_{100})$ et dans laquelle pour tout $k \geq 2$, le $k$ème retrouve C_k avec la formule

$$C_k = R_n(\underbrace{x_0}_{\substack{\text{donné} \\ \text{par le } 1^{\text{er}}}} - \underbrace{R_n(C_2 + \cdots + C_{k-1} + C_{k+1} + \cdots + C_{100})}_{\substack{\text{info. accessible au } k^{\text{ème}}\text{, puisqu'il voit} \\ \text{tous les chapeaux sauf le sien}}})$$

assure encore une fois à tous sauf au premier de connaître la couleur de leur chapeau.

3 Problème à ensemble infini de couleurs et nombre fini de chapeaux

Compliquons encore un peu le problème en supposant maintenant l'ensemble $\mathcal{C}$ des couleurs possibles infini.

Question : existe-t-il encore une stratégie qui assure à tous sauf au premier de connaître leur couleur ?

Ce qui est crucial dans les deux premiers problèmes est de pouvoir munir l'ensemble des couleurs d'une structure de **groupe abélien**. En effet, en notant $+$ la loi de ce groupe, le premier donnant l'information correspondant à $c_2 + \cdots + c_{100}$ ($c_1, \ldots, c_{100}$ correspondant aux couleurs respectives des individus, que l'on suppose maintenant appartenir à un groupe abélien dont la loi est notée $+$), chaque couleur c_k peut être retrouvée par la formule

$$c_k = \underbrace{c_2 + \cdots + c_{100}}_{\text{info. donnée par le } 1^{\text{er}}} - \underbrace{(c_2 + \cdots + c_{k-1} + c_{k+1} + \cdots + c_{100})}_{\substack{\text{info. accessible au } k^{\text{ème}}\text{, puisqu'il voit} \\ \text{tous les chapeaux sauf le sien}}}.$$

On est donc ramené, pour obtenir encore une stratégie dans laquelle seul le premier à s'exprimer doit se sacrifier, à montrer que sur tout ensemble infini $\mathcal{C}$, on peut mettre une structure de groupe abélien.

Remarque 3.1 *Prouver que tout ensemble $\mathcal{C}$* s'injecte *dans un groupe abélien (ce qui est très facile, car $\mathcal{C}$ s'injecte dans $\mathbb{Z}^{\mathcal{C}}$) n'est pas suffisant. En effet, si $c_2 + \cdots + c_{100}$ appartient à un groupe contenant $\mathcal{C}$, mais pas à $\mathcal{C}$, le premier ne peut l'exprimer comme une couleur.*

La proposition suivante répond donc de façon positive (quoique très théorique) à la question posée précédemment.

Propriété 3.2 *Tout ensemble $\mathcal{C}$ peut être muni d'une structure de groupe abélien.*

<u>*Démonstration*</u> : Remarquons tout d'abord que si ψ est une bijection entre $\mathcal{C}$ et un autre ensemble $\mathcal{C}'$ muni d'une structure de groupe abélien (dont la loi est notée $+_{\mathcal{C}'}$), alors on peut, par ψ, "transporter" la structure de groupe abélien en définissant sur $\mathcal{C}$ la loi $+_{\mathcal{C}}$ par

$$a +_{\mathcal{C}} b = \psi^{-1}(\psi(a) +_{\mathcal{C}'} \psi(b)).$$

Donc dans le cas où $\mathcal{C}$ est fini, la question a déjà été traitée à la partie 2.

Supposons $\mathcal{C}$ infini. L'ensemble

$$\mathbb{Z}^{(\mathcal{C})} = \{(z_c)_{c\in\mathcal{C}} | \{c \in \mathcal{C} | z_c \neq 0\} \text{ est fini}\}$$

est un groupe pour l'addition terme à terme. Nous allons montrer que cet ensemble est en bijection avec $\mathcal{C}$. Par ce qui précède, on pourra alors munir $\mathcal{C}$ d'une structure de groupe abélien.

À cette fin, nous allons utiliser la théorie de l'arithmétique des cardinaux, exposée de façon très claire dans l'avant-dernier chapitre de [H]. Pour X, Y ensembles, on notera $\operatorname{Card} X = \operatorname{Card} Y$ (resp. $\leq$) s'il existe une bijection (resp. une injection) de X dans Y. Le Théorème de Cantor-Bernstein (appelé aussi Théorème de Schröder-Bernstein) dit que

$$\operatorname{Card} X \leq \operatorname{Card} Y \text{ et } \operatorname{Card} Y \leq \operatorname{Card} X \Rightarrow \operatorname{Card} X = \operatorname{Card} Y.$$

L'arithmétique des cardinaux établit des égalités et des inégalités entre les cardinaux d'ensembles que l'on construit les uns à partir des autres (par union, produit cartésien, etc...).

On a clairement $\operatorname{Card} \mathcal{C} \leq \operatorname{Card} \mathbb{Z}^{(\mathcal{C})}$. Montrons l'autre inégalité. Notons $\mathcal{P}_f(\mathcal{C})$ l'ensemble des parties finies de $\mathcal{C}$, et, pour tout entier positif n, $\mathcal{P}_n(\mathcal{C})$ l'ensemble des parties de $\mathcal{C}$ de cardinal n. On a clairement

$$\operatorname{Card} \mathbb{Z}^{(\mathcal{C})} \leq \operatorname{Card} \bigcup_{F\in\mathcal{P}_f(\mathcal{C})} \mathbb{Z}^F.$$

Donc il suffit de montrer que

$$\operatorname{Card} \bigcup_{F\in\mathcal{P}_f(\mathcal{C})} \mathbb{Z}^F \leq \operatorname{Card} \mathcal{C}.$$

On sait que pour tout n entier, $\operatorname{Card} \mathbb{Z}^n = \operatorname{Card} \mathbb{Z}$ (cf chapitre 23 de [H]). Donc

$$\operatorname{Card} \bigcup_{F\in\mathcal{P}_f(\mathcal{C})} \mathbb{Z}^F = \operatorname{Card}(\mathbb{Z}\times\mathcal{P}_f(\mathcal{C})) = \operatorname{Card}(\mathbb{Z}\times\cup_{n=1}^{\infty}\mathcal{P}_n(\mathcal{C})) \leq \operatorname{Card}(\mathbb{Z}\times\cup_{n=1}^{\infty}\mathcal{C}^n).$$

Or il est démontré au chapitre 24 de [H] (en utilisant le lemme de Zorn), que pour tout n entier positif, $\operatorname{Card} \mathcal{C}^n = \operatorname{Card} \mathcal{C}$, donc

$$\operatorname{Card} \cup_{n=1}^{\infty}\mathcal{C}^n = \operatorname{Card} \mathbb{N}\times\mathcal{C} \leq \operatorname{Card} \mathcal{C}^2 = \operatorname{Card} \mathcal{C}.$$

Donc

$$\operatorname{Card}(\mathbb{Z}\times\cup_{n=1}^{\infty}\mathcal{C}^n) \leq \operatorname{Card} \mathcal{C}^2 = \operatorname{Card} \mathcal{C},$$

et on a bien $\operatorname{Card} \mathcal{C} = \operatorname{Card} \mathbb{Z}^{(\mathcal{C})}$.

Remarque 3.3 *La proposition 3.2 aurait aussi pu être vue comme une conséquence de la proposition 4.1.*

4 Problème à ensemble infini de couleurs et ensemble infini de chapeaux

Supposons maintenant le nombre de chapeaux non plus égal à 100, mais quelconque, éventuellement infini. Chacun aura remarqué que les techniques utilisées jusque là s'appliquent dans tous les cas où on a un nombre fini d'individus, que le nombre 100 ne joue pas un rôle particulier. On supposera donc l'ensemble I des individus infini. On supposera aussi l'ensemble $\mathcal{C}$ des couleurs infini (bien que, comme on va le voir à la remarque 4.2, les arguments utilisés pour résoudre le problème restent valides aussi dans le cas où l'ensemble des couleurs est fini, et son cardinal est une puissance d'un nombre premier).

Question : existe-t-il encore une stratégie qui assure à tous sauf au premier de connaître leur couleur ?

Le problème ici est que, même si l'on peut mettre, comme on l'a vu, une loi $+$ de groupe commutatif sur l'ensemble des couleurs, l'information donnée par le premier dans les stratégies présentées jusque là,

$$\sum_{i\in I} \text{couleur du chapeau de l'individu } i$$

n'a pas de sens si I est infini. Si I est dénombrable, on peut ésperer, avec de l'analyse, donner un sens à cette somme comme limite de sommes finies. Mais dans le cas général, il faut avoir recours à l'algèbre linéaire, et munir l'ensemble $\mathcal{C}$ des couleurs d'une structure de corps.

Propriété 4.1 *Tout ensemble infini $\mathcal{C}$ peut être muni d'une structure de corps commutatif.*

Remarque 4.2 *Il est connu (cf [P]) qu'on peut munir un ensemble fini d'une structure de corps commutatif si et seulement si son cardinal est une puissance d'un nombre premier.*

<u>*Démonstration*</u> : Par un argument de transport de structure analogue à celui du début de la preuve de la proposition 3.2, il suffit de montrer que si $\mathcal{C}$ et infini, il est en bijection avec l'ensemble

$$\mathbb{Q}((X_c)_{c\in\mathcal{C}})$$

des fractions rationnelles à coefficients rationnels et à indéterminées commutatives X_c indexées par $\mathcal{C}$.

Encore une fois nous allons utiliser l'arithmétique des cardinaux. $\mathcal{C}$ s'injecte clairement dans cet ensemble. Montrons que l'inverse est vrai aussi. $\mathbb{Q}((X_c)_{c\in\mathcal{C}})$ s'injecte dans l'ensemble

$$\mathbb{Q}[(X_c)_{c\in\mathcal{C}}]\times\mathbb{Q}[(X_c)_{c\in\mathcal{C}}]$$

des couples de polynômes à coefficients rationnels et à indéterminées commutatives X_c indexées par $\mathcal{C}$, qui est en bijection (par le chapitre 24 de [H] encore) avec $\mathbb{Q}[(X_c)_{c\in\mathcal{C}}]$. Il suffit donc de montrer que

$$\operatorname{Card}\mathbb{Q}[(X_c)_{c\in\mathcal{C}}] \leq \operatorname{Card}\mathcal{C}.$$

On a, avec les notations de la partie 3,

$$\operatorname{Card} \mathbb{Q}[(X_c)_{c\in\mathcal{C}}] = \operatorname{Card} \bigcup_{F\in\mathcal{P}_f(\mathcal{C})} \mathbb{Q}[(X_c)_{c\in F}],$$

or pour tout $F \in \mathcal{P}_f(\mathcal{C})$, $\mathbb{Q}[(X_c)_{c\in F}]$ est dénombrable, donc

$$\operatorname{Card} \mathbb{Q}[(X_c)_{c\in\mathcal{C}}] = \operatorname{Card}(\mathbb{N}\times\mathcal{P}_f(\mathcal{C})) = \operatorname{Card} \mathcal{C},$$

comme on l'a déjà vu.

La proposition suivante, comme nous allons l'expliquer, donne une réponse positive (mais très théorique) au problème dans le cas où l'ensemble $\mathcal{C}$ des couleurs et l'ensemble I des individus sont infinis.

Propriété 4.3 *On munit $\mathcal{C}$ d'une structure de corps commutatif. Alors il existe une forme linéaire φ sur le $\mathcal{C}$-espace vectoriel $\mathcal{C}^I$ (ensemble des fonctions de I dans $\mathcal{C}$) qui, à toute fonction f de support fini (i.e. nulle sauf en un nombre fini de points) associe*

$$\sum_{i\in I} f(i).$$

Expliquons tout d'abord en quoi cette proposition donne une réponse positive (bien que très théorique) au problème.

Considérons la fonction $C : I \to \mathcal{C}$ qui à tout individu $i \in I$ associe la couleur de son chapeau. Notons, pour $k, l \in I$, C_k (resp. $C_{k,l}$) la fonction de I vers $\mathcal{C}$ qui coïncide avec C sur $I\backslash\{k\}$ (resp. sur $I\backslash\{k,l\}$), et qui est nulle en k (resp. en k et en l). La stratégie sera la suivante : le premier individu à s'exprimer, que l'on appellera i_1, donnera la réponse $\varphi(C_{i_1})$ (il a bien accès à cette information, puisqu'il voit tous les chapeaux sauf le sien).

Tout individu $k \neq i_1$ retrouvera la couleur $C(k)$ de son chapeau en remarquant que $C(k)$ est l'image, par φ, de la fonction qui vaut $C(k)$ en k et qui est nulle ailleurs, soit

$$C(k) = \varphi(C_{i_1} - C_{i_1,k}) = \varphi(C_{i_1}) - \varphi(C_{i_1,k}),$$

que $\varphi(C_{i_1})$ est l'information donnée par i_1, et que $\varphi(C_{i_1,k})$ lui est accessible, puisqu'il voit tous les chapeaux sauf le sien.

Donnons maintenant la démonstration de la proposition 4.3.

Démonstration : Elle repose sur le lemme de Zorn. Ce résultat ([H]), que nous avions déjà utilisé de façon implicite pour affirmer que si $\mathcal{C}$ est infini (non dénombrable), alors $\operatorname{Card} \mathcal{C} = \operatorname{Card} \mathcal{C}^n$ pour tout entier n, s'énonce ainsi : si $(E, \leq)$ est un ensemble ordonné dans lequel toute sous-partie F totalement ordonnée a un majorant (i.e. $\exists m \in E, \forall x \in F, x \leq m$), alors E possède un élément maximal (i.e. un élément a tel que $\forall x \in E, a \leq x \Rightarrow a = x$).

Une conséquence facile du lemme de Zorn est que si une forme linéaire L est définie sur un sous-espace $\mathcal{W}$ d'un espace vectoriel $\mathcal{V}$, alors elle se prolonge en une forme linéaire sur $\mathcal{V}$. En effet, on munit l'ensemble

$$\{(\mathcal{X}, K) | \mathcal{W} \subset \mathcal{X} \text{ ss-ev de } \mathcal{V}, K \text{ forme linéaire sur } \mathcal{X} \text{ qui prolonge } L\}$$

de la relation d'ordre définie par :

$$(\mathcal{X}, K) \leq (\mathcal{X}', K') \Leftrightarrow \mathcal{X} \subset \mathcal{X}' \text{ et } K' \text{ prolonge } K,$$

on voit facilement que dans cet ensemble, toute sous-partie totalement ordonnée a un majorant, et il est aussi facile de voir que tout élément maximal de E est de la forme $(\mathcal{V}, K)$.

On conclut en remarquant que l'ensemble des fonctions de I dans $\mathcal{C}$ de support fini est un sous-espace vectoriel de $\mathcal{C}^I$, et que sur ce sous-espace l'application qui à toute fonction f associe $\displaystyle\sum_{i \in I} f(i)$ est une forme linéaire.

Références

[AF] Arnaudiès, Jean-Marie ; Fraysse, Henry *Cours de mathématiques. 1 Algèbre* Dunod, 1987

[H] Halmos, Paul R. *Introduction à la théorie des ensembles* Gauthier-Villars, 1967

[P] Perrin, Daniel *Cours d'algèbre* Ellipses, 1996