Leçon de mathématiques pour l'informatique (29/06)

Couplage Leçon choisie : **123 – Corps finis. Applications.**
Alternative : *223 – Suites numériques. Convergence, valeurs d'adhérence. Exemples et applications.*

Étant passé sur la leçon *Nombres premiers* pendant l'année, j'étais ravi de pouvoir profiter de ma préparation spécifique ainsi que des remarques de Claudine Picaronny. Mon plan était :

1. Rappels de théorie des corps (caractéristique, extensions finies)
2. Cartographie des corps finis (existence et unicité, inclusions, clôture algébrique)
3. Groupe multiplicatif $\mathbb{F}_q^*$, carrés (cyclicité avec applications au petit théorème de Fermat et au théorème de Wilson, puis les histoires de symbole de Legendre etc.)
4. Algèbre linéaire et bilinéaire sur $\mathbb{F}_q$ (groupes GL_n / SL_n, formes quadratiques)
5. Polynômes irréductibles (Eisenstein, Berlekamp)

Mes références étaient Perrin, Demazure (pour l'algorithme de Berlekamp) et Caldero–Germoni, aussi connu sous le nom de H2G2 (pour les formes quadratiques et les développements).

Pendant la défense du plan j'ai dessiné au tableau le trellis de tous les corps finis d'une caractéristique p fixée.

Développements proposés Deux jolis développements tirés de H2G2 tome premier.
Choix du jury : **Loi de réciprocité quadratique** (en comptant les points de coniques sur $\mathbb{F}_q^p$).
Alternative : *Non-isomorphisme exceptionnel des groupes simples* $\mathrm{PSL}_3(\mathbb{F}_4)$ *et* $\mathrm{PSL}_4(\mathbb{F}_2)$.

Je n'ai pas fait tenir le développement dans les 15 minutes : il m'a fallu sauter une partie calculatoire pour arriver à la conclusion. À part ça, ça s'est pas trop mal passé.

J'avais écrit $u \in \mathrm{GL}(\mathbb{F}_q^p)$ au tableau, un examinateur m'a demandé « N'y a-t-il pas une notation plus canonique, que vous utilisez dans votre plan ? ». J'ai expliqué que je notais $\mathrm{GL}(\mathbb{F}_q^p)$ pour un groupes d'applications linéaires et $\mathrm{GL}_p(\mathbb{F}_q)$ pour un groupe de matrices. Réaction : « Ah, bon, d'accord. ».

Ils m'ont ensuite demandé de compléter le développement, j'ai commencé à faire le calcul en montrant où le $(-1)^{(p-1)(q-1)/4}$ allait apparaître, ils ont proposé de passer à autre chose.

Comme je parlais d'hyperplans affines dans le développement, ils m'ont demandé le nombre d'hyperplans affines dans $\mathbb{F}_q^n$.

Sur l'autre développement, ils ont juste demandé : « Vous affirmez que ces deux groupes sont de même cardinal, quel est ce cardinal ? — 20160, si je ne m'abuse. — Ah, vingt mille, quand même ! ». J'ai rajouté que c'était le plus petit cardinal où l'on trouve deux groupes simples non isomorphes.

Questions Elles étaient nombreuses ; souvent, une fois que le jury était convaincu que ça allait aboutir, on passait tout de suite à un autre exercice. Les voici, pas forcément dans l'ordre :

— *Que pouvez-vous dire de* $\mathrm{GL}_2(\mathbb{F}_2)$ *?* C'est la même chose que $\mathrm{PSL}_2(\mathbb{F}_2)$, dont j'avais mis dans mon plan qu'il est isomorphe à $\mathfrak{S}_3$. *Démonstration ?* J'ai décrit l'action de $\mathrm{GL}_2(\mathbb{F}_2)$ sur $\mathbb{F}_2^2 \setminus \{0\}$, puis ils ont voulu que je prouve proprement la bijectivité du morphisme dans $\mathfrak{S}_3$ correspondant. *À quel sous-groupe correspond* $\mathfrak{A}_3$ *?* J'ai explicité les matrices correspondantes.

— *Démonstration de la cyclicité de* $\mathbb{F}_q^*$ *?* J'ai honteusement hésité sur ce grand classique, mais j'ai quand même fini par retrouver la preuve sans indication, ils étaient plutôt convaincus sans que je détaille tout.

— *Si un groupe fini est d'exposant 2, que peut-on dire ?* Réponse : on peut montrer que c'est abélien, c'est un $\mathbb{F}_2$-espace vectoriel, donc isomorphe à $(\mathbb{Z}/2\mathbb{Z})^n$. Vu que je connaissais déjà le truc ils ne m'ont pas demandé la démonstration.
— *L'application $\mathbb{F}_p$-linéaire $u : x \in \mathbb{F}_{p^2} \mapsto x^p$ est-elle diagonalisable ?* Il m'a demandé d'abord pourquoi c'était linéaire (réponse : c'est un automorphisme de corps qui fixe $\mathbb{F}_p$) et en particulier pourquoi ça préserve les sommes (« Quelle propriété des coefficients binomiaux utilisez-vous ? — $p \mid C_p^k$ »). Ensuite j'ai tout de suite remarqué que le polynôme minimal de u était $X^2 - 1$ et le tour était joué. (À un moment, j'ai dit que $X^2 - 1 = (X-1)^2$ en pensant à mon développement sur $\mathrm{PSL}_4(\mathbb{F}_2)$ et en oubliant de préciser « en caractéristique 2 »…)
— *Quelle est la classe d'équivalence de $q(x) = x^2 + xy + y^2 + z^2$ sur $\mathbb{F}_5$?* Il suffit de calculer le discriminant et de tester si c'est un carré.
— *Comment déterminer les polynômes irréductibles de degré 2 sur $\mathbb{F}_2$?* En éliminant les produits de polynômes de degré 1. Après avoir constaté qu'il y a avait 3 polynômes scindés je ne me suis pas rendu compte qu'il n'en restait qu'un seul d'irréductible…
— *Savez-vous décrire les p-Sylow de $\mathrm{GL}_n(\mathbb{F}_p)$?* Ça ne me disait pas grand-chose, mais après avoir calculé $v_p(|\mathrm{GL}_n(\mathbb{F}_p)|) = p^{n(n-1)/2}$, j'ai dit que ça évoquait des matrices antisymétriques ou triangulaires. L'examinateur m'a dit de partir sur cette dernière idée, et en fait à partir de là c'est facile. Après l'épreuve je me suis rappelé que c'était dans la preuve du premier théorème de Sylow dans le Perrin (qui vient apparemment de J.-P. Serre).
— *Exemple d'application du critère d'Eisenstein ?* L'irréductibilité du p-ième polynôme cyclotomique, en regardant $\Phi_p(X+1)$, a semblé plaire au jury. Sans doute aurait-il été préférable d'inclure l'exemple dans le plan…
— *Connaissez-vous d'autres preuves de la réciprocité quadratique ?* J'ai cité les mots-clés « somme de Gauss » et « équivalent asymptotique de la fonction thêta » (*cf. annexe*). « Donc il en existe beaucoup, des démonstrations différentes de la réciprocité quadratique ? — Oui, il y en a plein ! — Et comment est-ce que ça s'inscrit dans la théorie du corps des classes ? — Désolé, je ne connais pas grand-chose en théorie algébrique des nombres… ». Puis un autre membre du jury, amusé : « Je crois que ce n'est pas au programme de l'agrég, ça ! »
— La question pour finir : *Pouvez-vous décrire tous les morphismes de $\mathrm{PSL}_4(\mathbb{F}_2)$ dans $\mathfrak{S}_3$?* J'ai séché pendant quelques secondes, puis l'examinateur me dit « Je n'ai pas choisi ce groupe par hasard, il est dans votre plan ! » et en effet une fois qu'on se souvient que c'est un groupe simple, la question devient, justement, simple.

Dernière remarque : le partage du temps de parole était très inégal, l'un des membres du jury a posé la grande majorité des questions pendant qu'une autre ne disait quasiment rien (peut-être était-ce une analyste ?).

Annexe : réciprocité des sommes de Gauss et fonction thêta

Ceci est une tentative inaboutie de fabriquer un développement original pour les leçons sur les séries et les développements asymptotiques. Elle m'aura donc malgré tout servi à répondre à une question du jury ! Il y a une arnaque dans la démonstration ci-dessous ; **avis aux amateurs : je suis à la recherche d'une solution satisfaisante**.

Référence livresque : Richard Bellman [1], *A brief introduction to theta functions*. Voir aussi l'article d'Anders Karlsson, *Applications of heat kernels on abelian groups : $\zeta(2n)$, quadratic reciprocity, Bessel integrals*, qui raconte également d'autres applications fort jolies. Cependant, aucun des deux ne fournit de preuve rigoureuse complète.

Dans tout ce qui suit, on fixe $p, q \in \mathbb{N}^*$ premiers entre eux. La *somme de Gauss* associée est :

$$S(p,q) = \sum_{k \in \mathbb{Z}/q\mathbb{Z}} \exp(-i\pi k^2 p/q)$$

Rappelons aussi que la *fonction θ de Jacobi* est définie sur $\{\mathrm{Re}(z) > 0\}$ par

$$\theta : z \mapsto \sum_{n \in \mathbb{Z}} e^{-\pi n^2 z}$$

et vérifie la formule d'inversion (avec le prolongement analytique de $\sqrt{\cdot}$ à $\{\mathrm{Re}(z) > 0\}$)

$$\theta(1/z) = \sqrt{z}\theta(z)$$

(preuve : via formule de Poisson, fait dans le TD d'analyse de Fourier…).

On va montrer le résultat suivant, à partir duquel la loi de réciprocité quadratique se déduit :

Théorème (Réciprocité des sommes de Gauss)**.** $\sqrt{p}S(p,q) = e^{-i\pi/4}\sqrt{q}\overline{S(q,p)}$, *i.e.*

$$\frac{1}{\sqrt{q}} \sum_{k \in \mathbb{Z}/q\mathbb{Z}} \exp\left(\frac{-i\pi k^2 p}{q}\right) = \frac{e^{-i\pi/4}}{\sqrt{p}} \sum_{k \in \mathbb{Z}/p\mathbb{Z}} \exp\left(\frac{i\pi k^2 q}{p}\right)$$

Cette identité exacte peut en fait être obtenue à partir du développement asymptotique de $\theta(x + ip/q)$ pour $x \to 0^+$.

Lemme. *Soit $k \in \mathbb{N}^*$. Quand $x \to 0^+$,* $\displaystyle\sum_{l=0}^{+\infty} \exp(-\pi(k+lq)^2 x) \sim \frac{1}{2q\sqrt{x}}$.

Démonstration. La fonction $f : t \mapsto \exp(-\pi(k+tq)^2 x)$ est décroissante et intégrable sur $\mathbb{R}_+$, donc par comparaison série-intégrale,

$$\sum_{l \geq 1} f(l) \leq \int_0^{+\infty} f(t)\,dt \leq \sum_{l \geq 0} f(l) \quad \text{soit} \quad 0 \leq \sum_{l \geq 0} f(l) - \int_0^{+\infty} f(t)\,dt \leq f(0) = e^{-\pi k^2 x} \leq 1$$

Calculons l'intégrale :

$$\int_0^{+\infty} \exp(-\pi(k+tq)^2 x)\,dt = \frac{1}{q\sqrt{\pi x}} \int_{k\sqrt{\pi x}}^{+\infty} e^{-u^2}\,du \underset{x \to 0^+}{\sim} \frac{1}{2q\sqrt{x}} \qquad (u = \sqrt{\pi x}(k+tq))$$

□

1. Un analyste qui a aussi eu une carrière fructueuse de mathématicien appliqué : il est l'inventeur de la *programmation dynamique*, qui est au programme de l'agrég option D en algorithmique, mais intervient aussi en recherche opérationnelle et théorie du contrôle.

Proposition. *Quand* $x \to 0^+$, $\theta\left(x + i\frac{p}{q}\right) \sim \frac{S(p,q)}{q\sqrt{x}}$.

Démonstration. Par une interversion de sommes, justifiée par la sommabilité de la famille considérée, on obtient facilement que

$$\sum_{n\in\mathbb{N}^*} \exp\left(-\pi n^2\left(x + i\frac{p}{q}\right)\right) = \sum_{k=1}^{q}\left(\sum_{l\in\mathbb{N}} \exp(-\pi(k+lq)^2 x)\right)\exp\left(\frac{-i\pi k^2 p}{q}\right)$$

Grâce au lemme, on sait que les sommes intérieures sont équivalentes à $1/2q\sqrt{x}$, donc

$$\theta\left(x + i\frac{p}{q}\right) = 1 + 2\sum_{n\in\mathbb{N}^*} \exp\left(-\pi n^2\left(x + i\frac{p}{q}\right)\right) \underset{x\to 0^+}{\sim} \frac{S(p,q)}{q\sqrt{x}}$$

□

Maintenant, écrivons l'équation fonctionnelle de θ :

$$\theta\left(\frac{1}{x + ip/q}\right) = \sqrt{x + i\frac{p}{q}} \times \theta\left(x + i\frac{p}{q}\right) \underset{x\to 0^+}{\sim} e^{i\pi/4}\sqrt{\frac{p}{q}} \times \frac{S(p,q)}{q\sqrt{x}}$$

D'autre part, on a

$$\frac{1}{x - ip/q} \underset{x\to 0^+}{=} x\frac{q^2}{p^2} + i\frac{q}{p} + O(x^2)$$

Arnaquons maintenant allègrement en considérant que notre équivalent asymptotique, valable quand $z \to ip/q$ en suivant une demi-droite parallèle à $\mathbb{R}_+$, le reste en suivant un courbe qui finit par être tangente à cette demi-droite. Alors

$$\theta\left(\frac{1}{x + ip/q}\right) = \overline{\theta\left(\frac{1}{x - ip/q}\right)} \underset{x\to 0^+}{\sim} \frac{\overline{S(q,p)}}{p\sqrt{xq^2/p^2}}$$

On voit donc apparaître du $S(q,p)$! En simplifiant et en comparant nos deux équivalents asymptotiques, on obtient l'identité arithmétique désirée.

Pour que ça marche vraiment, il faudrait étendre le cadre de validité du lemme, en faisant une comparaison série-intégrale plus subtile, peut-être en utilisant une formule du genre

$$\int_0^{+\infty} f(t)\,dt - \sum_{n=1}^{+\infty} f(n) = \int_0^{+\infty} (t - \lfloor t \rfloor) f'(t)\,dt$$

On pourrait dire qu'en fin de compte, on obtient la loi de réciprocité quadratique par une comparaison série-intégrale !