Lemme de Kronecker (la preuve à toto) et Lemme de Serre

Ce développement est inspiré de la vidéo de Philippe Caldero (auteur de CVA et NH2G2) sur sa chaîne YouTube : « Kronecker : la méthode à Toto ! ». Mais je vous écris ici la preuve, sous forme d'un développement tel que je l'aurais présenté, comme ça tout le monde est content. Il y a un prérequis sur le contenu, on va utiliser le lemme de Gauss.

On en déduit de façon classique le lemme de Serre sur les sous-groupes finis de $\mathrm{GL}_n(\mathbb{Z})$.

Le tout peut rentrer en 15 minutes ! Sinon vous enlevez des trucs (notamment la proposition I.0.2, que vous pouvez remplacer par la phrase « un corps de caractéristique nulle est parfait » à condition d'être prêt à donner des exemples de corps non parfaits au jury qui vous attendra au tournant (les corps finis sont parfaits, le corps $\mathbb{F}_2(X)$ ne l'est pas)).

I. Prérequis sur les polynômes

Proposition I.0.1. Gauss
Soit $Q \in \mathbb{Q}[X]$ un polynôme unitaire divisant (dans $\mathbb{Q}[X]$) un polynôme $P \in \mathbb{Z}[X]$ unitaire. Alors $Q \in \mathbb{Z}[X]$.

Preuve. Soit $R = P/Q \in \mathbb{Q}[X]$. Comme $Q, R \in \mathbb{Q}[X]$, il existe $a, b \in \mathbb{Z}^*$ (entiers non nuls) tq $aR, bQ \in \mathbb{Z}[X]$. Alors $aRbQ = abP$ donc par le lemme de Gauss sur le contenu, $c(aR)c(bQ) = ab$ (car $c(P) = 1$). Alors $\frac{aR}{c(aR)}\frac{bQ}{c(bQ)} = P$. En regardant les coefficients dominants, on trouve que celui de $\frac{bQ}{c(bQ)}$ est inversible, mais comme Q est unitaire, ça veut dire que $\frac{b}{c(bQ)}$ est inversible. Or, $\frac{bQ}{c(bQ)} \in \mathbb{Z}[X]$ (par définition du contenu) donc $Q \in \mathbb{Z}[X]$. Remarque : la même chose marche pour R. □

Proposition I.0.2. Un corps de caractéristique nulle est parfait
Soit P un polynôme irréductible sur $\mathbb{Q}$. Alors il est à racines complexes simples.

Preuve. Supposons que $\lambda \in \mathbb{C}$ est racine double de P donc que $(X-\lambda)^2 \mid P$ donc il existe $Q \in \mathbb{C}[X]$ tel que $P = (X-\lambda)^2 Q$ donc $P' = 2(X-\lambda)Q + (X-\lambda)^2 Q'$ donc $P \wedge P' \neq 1$ dans $\mathbb{C}[X]$ mais par invariance du pgcd par extension de corps, $P \wedge P' \neq 1$ dans $\mathbb{Q}[X]$. Mais c'est donc un diviseur non trivial de P dans $\mathbb{Q}[X]$ qui est irréductible donc $P \wedge P' = P$ donc $P' = 0$ (sinon on a une contradiction au niveau du degré) donc P est constant donc nul ou inversible donc n'est pas irréductible, ce qui est exclu. □

II. Le Lemme de Kronecker (la preuve super rapide)

Théorème II.0.1.
Soit $P \in \mathbb{Z}[X]$ unitaire à racines non nulles et de module $\leqslant 1$. Alors les racines de P sont des racines de l'unité.

Preuve. On veut se ramener au cas où P est à racines simples. Pour cela, décomposer P en irréductibles unitaires distincts P_i dans $\mathbb{Q}[X]$: $P = \prod_{i=1}^{r} P_i^{n_i}$. Par la proposition I.0.1, ils sont dans $\mathbb{Z}[X]$ et par le lemme I.0.2, ils sont à racines simples. Comme les P_i sont irréductibles et distincts, ils sont premiers entre eux deux à deux donc n'ont aucune racine commune dans $\mathbb{C}$. Donc le polynôme $\prod_{i=1}^{r} P_i$ est à racines complexes simples, et ses racines complexes sont les mêmes que celles de P.

Remarque : *Une façon classique de penser le problème est de constater que $P \wedge P'$ (le pgcd unitaire de P et P' dans $\mathbb{Q}[X]$) divise P selon les hypothèses du lemme I.0.1 ce qui montre que $P/P \wedge P'$ est encore unitaire dans $\mathbb{Z}[X]$. On veut donc remplacer P par ce dernier. Mais il faut encore prouver que ce dernier*

est bien à racines simples, et que ses racines sont exactement celles de P, et c'est pour ça qu'on a fait le travail de la section 1. Le polynôme $P/P \wedge P'$ est en fait exactement le produit des P_i (c'était une autre approche).

Afin de simplifier les notations, supposons que P a d'office ces propriétés-là. Prenons donc la matrice compagnon $C_P \in \mathcal{M}_n(\mathbb{Z})$ (car $P \in \mathbb{Z}[X]$), qui est diagonalisable car à valeurs propres toutes distinctes. Il existe donc $Q \in \mathrm{GL}_n(\mathbb{C})$ telle que $C_P = QDQ^{-1}$ où D est diagonale à éléments non nuls distincts et de module $\leqslant 1$. Alors la suite $(C_P^k)_{k\in\mathbb{N}}$ est bornée. Pour le voir, prenez votre norme matricielle favorite. Je prends la norme d'opérateur associée à la norme euclidienne. Ainsi, la norme d'une matrice diagonale est le max des valeurs absolues de ses coefficients. Donc $\left\|D^k\right\| \leqslant 1$ pour tout k. Donc, on a bien que $\left\|C_P^k\right\| \leqslant \|Q\|\left\|Q^{-1}\right\|$.

Donc cette suite vit dans $\mathcal{M}_n(\mathbb{Z})$ qui est discret et dans une boule fermée bornée qui est compacte car $\mathcal{M}_n(\mathbb{C})$ est de dimension finie. Mais l'intersection entre un discret et un fermé est finie ! Vient alors l'argument combinatoire : on ne peut pas plonger de l'infini dans du fini donc il existe $k \neq k' \in \mathbb{N}$ tq $C_P^k = C_P^{k'}$ donc, comme C_P est inversible (diagonalisable et ses valeurs propres sont non nulles), on trouve $C_P^{k-k'} = I_n$ donc C_P est diagonalisable à valeurs propres racines $k-k'$-ièmes de l'unité. Oui, cette preuve est totalement illégale mais ça marche. □

III. Application : le Lemme de Serre

Théorème III.0.1.
Soit G un sous-groupe fini de $\mathrm{GL}_n(\mathbb{Z})$. Si $m \geqslant 3$, alors la réduction modulo m donne un un morphisme de groupes injectif $G \hookrightarrow \mathrm{GL}_n(\mathbb{Z}/m\mathbb{Z})$.

Preuve. Ce morphisme a du sens car si $M \in \mathrm{GL}_n(\mathbb{Z})$, alors $\det(M) = \pm 1$ donc $\overline{M}$ est de déterminant $\overline{\pm 1}$ donc est encore inversible donc est dans $\mathrm{GL}_n(\mathbb{Z}/m\mathbb{Z})$. Soit maintenant G un sous-groupe fini de $\mathrm{GL}_n(\mathbb{Z})$.

On montre que le noyau est trivial, soit donc $M \in G$ telle que $\overline{M} = \overline{I_n}$, ce qui signifie qu'il existe $A \in \mathcal{M}_n(\mathbb{Z})$ telle que $M = I_n + mA$. Alors $A = \frac{M-I_n}{m}$. Mais M est un élément de G donc d'ordre fini donc diagonalisable à valeurs propres de module 1. Donc A est diagonalisable à valeurs propres de la forme $\frac{\lambda-1}{m}$ où λ parcourt l'ensemble des valeurs propres de M donc $|\lambda| = 1$. Donc $\left|\frac{\lambda-1}{m}\right| \leqslant \frac{|\lambda|+1}{m} < 1$. Par conséquent, les racines de χ_A sont soit 0 soit de module < 1. Si r est la X-valuation de χ_A, alors χ_A/X^r est un polynômes à racines non nulles de module $\leqslant 1$. Donc ses racines sont de module 1 par le lemme de Kronecker. Mais c'est contradictoire sauf si χ_A/X^r est constant. Donc $\chi_A = X^n$ (par comparaison des degrés et c'est un polynôme unitaire). Donc A est à valeurs propres nulles donc les $\frac{\lambda-1}{m}$ sont nuls donc toutes les $\lambda \in \mathrm{Sp}(M)$ sont égales à 1 donc, puisque M est diagonalisable, cela nous apprend simplement que $M = I_n$. □

Remarque III.0.2. Pour $m = 3$, on obtient une majoration du cardinal de G. Pour $m = 2$, il existe un résultat mais un peu plus subtil. Je crois qu'il donne une meilleure majoration du cardinal de G, mais, à ce sujet, faites vos propres recherches :))