Université Claude Bernard Lyon 1

MASTER M1G

Algèbre

Feuille de développements pour l'agrégation

Fiche 1

Automorphismes de $\mathbb{Z}/n\mathbb{Z}$ + $(\mathbb{Z}/p^n\mathbb{Z})^*$ cyclique pour p impair (Exercice 2)

Idées. Tout automorphisme de $\mathbb{Z}/n\mathbb{Z}$ est de la forme $x \mapsto ax$, $a \in \mathbb{Z}/n\mathbb{Z}^*$. On a un isomorphisme $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/n\mathbb{Z}^*$. On se ramène à $(\mathbb{Z}/p^kZ)^*$ par le lemme chinois. Celui-ci est cyclique pour p impair (on trouve à la main un élément d'ordre $p-1$ et un d'ordre p^{k-1}). Voir le Cours d'Algèbre de Perrin.

Classification des groupes simples d'ordre 60 (Exercice 10)

Idées. On fait agir ce groupe G sur ses six 5-Sylow (transitivement !). Le groupe simple G s'injecte dans $\mathfrak{S}_6$, puis dans $\mathfrak{A}_6$ par dérivation. Puis, $\mathfrak{A}_6$ agit transitivement sur $\mathfrak{A}_6/G$ de cardinal 6, d'où un morphisme de G sur $\mathfrak{S}_6$ qui stabilise un élément. On obtient donc un morphisme de G dans $\mathfrak{S}_5$ que l'on dérive, et on a gagné. C'est fait dans le Szpirglas...

Fiche 2

Isomorphisme de Harish-Chandra : $\mathbb{C}[\mathcal{M}_n]^{\mathrm{GL}_n} \simeq \mathbb{C}[X_1, \cdots, X_n]^{\mathfrak{S}_n}$(Exercice 8)

Idées. On regarde le morphisme de restriction qui va de l'algèbre des polynômes GL_n-invariants sur une matrice vers l'algèbre des polynômes sur la diagonale. Pour l'injectivité, on utilise le fait que les matrices diagonalisables complexes sont denses dans l'espace des matrices. Pour la surjectivité, on utilise les polynôme symétriques élémentaires. Voir Nouvelles histoires hédonistes, exercice III-D.29.

Fiche 3-4

Pour $\mathbb{K}$ sous-corps de $\mathbb{C}$, deux matrices $\mathbb{C}$-semblables sont $\mathbb{K}$-semblables (Exercice 8)

Il est bien, pour se familiariser, de regarder d'abord le cas où $\mathbb{K} = \mathbb{R}$. On utilise le fait qu'un polynôme non nul possède un nombre fini de zéros. Dans le cas général, on utilise le fait que l'on peut identifier polynômes et fonctions polynômes à plusieurs indéterminées (sur $\mathbb{K}$, qui est infini). Il faut aussi se ramener à une extension finie de $\mathbb{K}$ en prenant le corps de décomposition du polynôme caractéristique.

Une équation de Mordell : $x^3 - 2 = y^2$ (Exercice 12)

Idées. On montre par un considération de la taille de mailles du réseau que l'anneau $\mathbb{Z}[i\sqrt{2}]$ est euclidien. Ensuite, on peut dire qu'il est factoriel et utiliser l'unicité de la décomposition de $(y + i\sqrt{2})(y - i\sqrt{2}) = x^3$ après avoir montré que $(y + i\sqrt{2})$ et $(y - i\sqrt{2})$ sont premiers entre eux (en considérant par l'absurde un diviseur premier commun d et en prenant la norme). Il y a des équations de Mordell dans le Francinou-Gianella, et dans le Szpirglas.

Fiche 5

Version faible du théorème de progression arithmétique de Dirichlet (Exercice 7)

Idées. On montre tout d'abord que $X^n - 1$ n'a pas de racine multiple modulo p (si p ne divise pas n). On prend N assez grand et on considère $\phi_n(a)$ pour un $a > N$. Pour tout nombre premier p divisant $\phi_n(a)$, on déduit de ce qui précède que a est d'ordre n dans $\mathbb{F}_p^*$. Donc n divise $p - 1$ par Lagrange et on a gagné. Voir le Francinou-Gianella.

Fiche 6

Théorème de décomposition en deux carrés (pour p puis pour n) (Exercice 2)

Idées. On montre que $\mathbb{Z}[i]$ est factoriel, et que si p est congru à 1 modulo 4, -1 est un carré de $\mathbb{F}_p$ (symbole de Legendre). Un tour de passe-passe montre que $\mathbb{F}_p[X]/(X^2 + 1)$ est isomorphe à $\mathbb{Z}[i]/(p)$. Comme le premier anneau n'est pas intègre, le second non plus, et donc p n'est pas premier dans $\mathbb{Z}[i]$, qui est factoriel. Donc, p n'est pas irréductible et il ne reste plus qu'à prendre la norme d'une décomposition de p. Voir le Francinou-Gianella.

Théorème de Chevalley-Warning+Erdös (Exercice 5)

Idées. Séries géométriques, corps finis, Lagrange, polynômes à plusieurs indéterminées. Lagrange permet de donner la fonction caractéristique d'un ensemble algébrique sous forme polynomiale. On étudie de prés ce polynôme... Voir le Zavidovique.

Réduction modulo p des polynômes cyclotomiques (Exercice 7)

Idées. On veut voir si ϕ_n, qui est irréductible sur $\mathbb{Z}$, le reste après réduction sur $\mathbb{F}_p$. La condition est que p soit générateur de $\mathbb{Z}/n\mathbb{Z}^*$. On part d'une racine α de ϕ_n dans une extension de $\mathbb{F}_p$ et on fait agir le Frobenius jusqu'à retomber sur α. On obtient encore des racines de ϕ_n et le nombre m de racines obtenues est égal à l'ordre de p dans $\mathbb{Z}/n\mathbb{Z}^*$. De plus, le produit des $X - \beta$ quand β parcourt l'ensemble de ces m racines est Frobenius-invariant, donc, dans $\mathbb{F}_p[X]$. On obtient donc un polynôme (minimal de α) de degré m et divisant ϕ_n sur $\mathbb{F}_p$. Voir le Francinou-Gianella.

Fiche 7

Représentation par permutations/Burnside/critère de double transitivité (Exercice 6)

Idées. A partir d'une action d'un groupe fini G sur un ensemble fini X, on obtient une représentation par matrices de permutations sur la base canonique de $\mathbb{C}^X$. Le caractère de cette représentation est donné par le nombre d'invariants. On montre, par la formule de Burnside, que la multiplicité de la représentation triviale dans la représentation de permutation est égal au nombre d'orbites de G sur X. Si cette action est transitive, on peut prendre un supplémentaire W de la représentation triviale (qui est donc de multiplicité 1), et le caractère est le « nombre d'invariants moins 1 ». On peut faire alors facilement le lien entre l'irréductibilité de W et la double transitivité de l'action. Voir Nouvelles histoires hédonistes partie 2, à paraître (ou H2G2 tome 2 déjà paru)

Fiche 8

Table des caractères des groupes non abéliens d'ordre 8 (Exercice 6)

Idées. On utilise le fait que si un groupe G, quotienté par un sous-groupe central est cyclique, alors G est abélien. Cela permet de voir que le centre d'un groupe G non abélien d'ordre 8 est d'ordre 2, puis, que le quotient par le centre est isomorphe au groupe de Klein. On voit alors que G possède 5 classes de conjugaison, donc 5 caractères irréductibles. On en trouve 4 d'ordre 1 en relevant les caractères du groupe de Klein, puis, le dernier est donné par une méthode classique. On finit en disant que D_4 et H_8 sont deux groupes non isomorphes ayant la même table de caractères ! Voir Nouvelles histoires hédonistes partie 2

Représentations du groupe du cube (Exercice 7)

Idées. On sait que $\mathfrak{S}_4$ est le groupe des isométries positives du cube, et on peut trouver sa table de caractères juste en observant le cube, grâce à des actions par permutations (modulo triviale). On agit sur les 4 paires de sommets opposés pour obtenir une représentation

de degré 3, sur les deux tétraèdres inscrits dans le cube, pour obtenir une représentation de degré 1 (la signature !), sur les 3 paires de faces opposées pour obtenir une représentation de degré 2. A la fin, il ne reste plus qu'une représentation que l'on trouve par la méthode usuelle. Voir Nouvelles histoires hédonistes partie 2

Fiche 9

Treillis des sous-groupes distingué de G + critère de simplicité (Exercices 2 et 4)

Idées. Tout part du théorème de Lagrange qui assure que les valeurs propres de l'action de g dans G (fini !) sont des racines de l'unité, donc de module 1. Comme la trace est la somme des valeurs propres, on peut, par exemple, par l'inégalité triangulaire, montrer que $\chi_\rho(g) = \chi_\rho(e)$ est équivalent à $g \in \ker(\rho)$. On voit donc certains sous-groupes distingués sur la table de caractères (ces noyaux !). Réciproquement, si H est distingué dans G, on considère la représentation régulière de G/H, qui est fidèle, que l'on compose par la surjection canonique $G \to G/H$, pour montrer, par Maschke, que H (qui devient le noyau de cette nouvelle représentation) est intersection des noyaux $\ker(\rho)$. Voir Nouvelles histoires hédonistes partie 2

Table des caractères de $\mathfrak{A}_5$.

Idées. Le groupe $\mathfrak{A}_5$ vient naturellement avec une représentation par permutations de degré 4. On peut faire agir sur les 5-Sylow pour obtenir une représentation irréductible de degré 5. Il reste ensuite à trouver deux représentations de degré 3. On montre tout d'abord que le caractère est réel (par l'absurde, avec la représentation duale), puis, on resout des équations pour finir les deux lignes restantes. Voir Nouvelles histoires hédonistes partie 2