Université Claude Bernard Lyon 1

MASTER Mathématiques et Applications

M1-ALGEBRE

EXAMEN-CORRECTION

8 Janvier 2018

Problème 1

1. Soit G un groupe d'ordre 2018. Comme $p := 1009$ est premier (admis), G possède un p-Sylow d'ordre p (théorème de Sylow), donc cyclique et d'indice 2 dans G. Il est donc distingué. De même, il possède un sous-groupe d'ordre 2. On peut appliquer le théorème des produits semi-directs : G est le produit semi-direct $\mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.

   Il reste à classifier les produits semi-directs $\mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$. Un tel groupe est entièrement déterminé par un morphisme de $\mathbb{Z}/2\mathbb{Z}$ vers $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z}^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$, c'est-à-dire, un élément a de $\mathbb{Z}/(p-1)\mathbb{Z}$ tel que $2a = 0$.

   Or, on sait (réciproque de Lagrange dans le cas cyclique) que dans un groupe cyclique $\mathbb{Z}/n\mathbb{Z}$, si d divise n, il y a exactement d éléments vérifiant $da = 0$.

   Il y a donc, à isomorphisme près, 2 groupes d'ordre 2018, un abélien, forcément $\mathbb{Z}/2018\mathbb{Z}$, et l'autre, non abélien, forcément le groupe diédral D_{1009}.

2. Dans le premier cas, le groupe est abélien et même cyclique. Si ω est une racine primitive 2018-ième de l'unité, alors les représentations irréductibles sont données par $\chi_{\omega^k}(\overline{1}) := \omega^k$, pour $0 \leq k \leq 2017$. Il y en a 2018 de degré 1.

   Dans le cas du groupe diédral, d'après le cours (D_n, n impair), il y en a deux de degré 1, et $\frac{n-1}{2} = 504$ de degré 2. Pour les représentations de degré 2, la classification ne pose pas de problème (une triviale et l'autre non). Les représentations de degré 2 sont classifiées par leur caractère. On choisit dans D_n une rotation r d'ordre 1009 et une symétrie s d'ordre 2. Alors, $\chi(r) = 2\cos(\frac{2k\pi}{1009})$, $1 \leq k \leq 504$.

Problème 2

1. La dérivée du polynôme $X^q - X$ est $qX^{q-1} - 1 = -1$, puisque l'on est en caractéristique p. En particulier, cette dérivée ne s'annule jamais, et donc le polynôme ne possède que des racines simples.

2. Soit A l'ensemble des racines (non nulles) de $X^q - X$. C'est l'ensemble des racines $(q-1)$-ième de 1, appartenant à K. Comme K est abélien, ceci constitue un groupe abélien. De plus, A est fini (d'ordre inférieur à $q-1$), puisque c'est un ensemble de racines d'un polynôme sur un corps.

   On peut donc lui appliquer le théorème de structure des groupes abéliens finis : il est produit direct de groupe cyclique $\mathbb{Z}/a_i\mathbb{Z}$, pour i de 1 à k, avec a_{i+1} divise a_i. Pour montrer qu'il est cyclique, il suffit de montrer que $k = 1$.

   On cherche le nombre d'éléments x de A tels que $x^{a_1} = 1$. Comme a_1 est multiple de tous les a_i, on sait que tous les éléments de A sont racines. Il y en a donc en tout $a_1 a_2 \cdots a_k$.

D'autre part, comme on calcule le nombre de racines d'un polynôme de degré a_1 sur un corps, on sait qu'il y en a un nombre inférieur à a_1. Conclusion,$a_1 a_2 \cdots a_k \leq a_1$, ce qui donne $k = 1$.

3. On applique 2) en remplaçant q par q^n. Les racines (non nulles) de $X^{q^n} - X$ appartenant à K, forment un groupe cyclique, engendré par un élément α. Le corps de décomposition K_n contient donc K et α ; il contient $K[\alpha]$.

   Réciproquement, $K[\alpha]$ contient K et toutes les racines de $X^{q^n} - X$, puisque α les engendrent (à part zéro qui ne pose pas de problème) ; il contient donc K_n. D'où l'égalité.

4. (a) On prend le même α que pour la question précédente. Soit $\mu_{\alpha,K}$ le polynôme minimal de α sur K. Comme $X^{q^n} - X \in K[X]$ annule α, $\mu_{\alpha,K}$ divise $X^{q^n} - X$. Or, $X^{q^n} - X$ se décompose en produit de $(X - \beta)$ où β parcourt $\mathbb{F}_{q^n}$. Donc, $\mu_{\alpha,K}$, qui est un produit des $X - \beta$, est bien à coefficients dans $\mathbb{F}_{q^n}$. D'où l'assertion.

   (b) Par définition m est le degré de $K[\alpha]$ sur K ; c'est donc le degré de $\mu_{\alpha,K}$. Soit m' le degré de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_{q^n} \cap K$. Comme $\mathbb{F}_{q^n} = \mathbb{F}_q[\alpha]$ et que K contient $\mathbb{F}_q$, on a $\mathbb{F}_{q^n} = (\mathbb{F}_{q^n} \cap K)[\alpha]$. Donc, m' est le degré du polynôme minimal de α sur $\mathbb{F}_{q^n} \cap K$. Or, d'après la question précédente, les deux polynômes minimaux sont égaux. Donc, $m' = m$ et on a l'assertion.

   (c) (bonus)

      i. Comme m est égal au degré de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_{q^n} \cap K$, il divise le degré de de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$, par le théorème de la base télescopique. Il divise donc n.

      ii. Soit k l'entier tel que $n = km$. On a donc $\mathbb{F}_{q^n} \cap K = \mathbb{F}_{q^k}$. Par le théorème de classification des corps finis, l'ensemble des diviseurs (positifs) de m est en bijection avec l'ensemble des corps intermédiaires entre $\mathbb{F}_{q^n}$ et $\mathbb{F}_{q^k}$ par $d \mapsto \mathbb{F}_{q^{kd}}$. De plus, on construit une bijection entre l'ensemble de ces corps intermédiaires et l'ensemble des corps intermédiaires entre K_n et K par $F' \mapsto F'K$, dont la réciproque est $K' \mapsto \mathbb{F}_{q^n} \cap K'$.

Problème 3 (Représentation par permutation de $\mathfrak{S}_5$ sur ses 5-Sylow)

1. (a) On a
$$\langle \chi_{\text{triv}}, \chi_{\text{perm}} \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_{\text{perm}}(g) = \frac{1}{|G|} \sum_{g \in G} |X|^g .$$
   C'est donc égal au nombre d'orbites par la formule de Burnside.

   (b) On a
$$\rho_{\text{perm}}(g)\Big(\sum_{x \in X} e_x \Big) = \sum_{x \in X} e_{g \cdot x} = \sum_{x \in X} e_x,$$
   par un changement de variable. D'où le résultat.

   (c) Ce supplémentaire existe par le théorème de Maschke. Deux représentations supplémentaires ont même caractère et sont donc isomorphes.

2. Le nombre n_5 de 5-Sylow de $\mathfrak{S}_5$ est congru à 1 modulo 5, et il divise 24. Comme $n_5 \neq 1$ (car $\mathfrak{S}_5$ n'a pas de sous-groupe distingué d'ordre 5), on a $n_5 = 6$. [1]

   Or, chaque 5-Sylow est engendré par un 5-cycle, donc, ces sous-groupes sont aussi les six 5-Sylow de $\mathfrak{A}_5$. Il en résulte, comme tous les 5-Sylow de $\mathfrak{A}_5$ sont conjugués, que la restriction reste transitive.

1. On peut trouver une méthode plus constructive !

3. Le noyau de ϕ est distingué ; s'il est non trivial, cela ne peut être que $\mathfrak{S}_5$, $\mathfrak{A}_5$. Comme l'action sur les six sous-groupes de Sylow est transitive le stabilisateur d'un élément est forcément d'ordre égal à $120/6 = 20$, et donc le noyau, qui lui est inclus, est forcément trivial.

   Un 5-cycle est donc envoyé sur un élément d'ordre 5 de $\mathfrak{S}_6$: l'image d'un 5-cycle est donc encore un 5-cycle. Une double transposition est un élément d'ordre 2 dans $\mathfrak{A}_5$, qui est le sous-groupe dérivé, $D(\mathfrak{S}_5)$, de $\mathfrak{S}_5$. Il en résulte qu'une double transposition est envoyée sur un élément d'ordre 2 de $D(\mathfrak{S}_6) = \mathfrak{A}_6$; cela ne peut être qu'une double transposition.

4. (a) Le normalisateur d'un 5-Sylow dans $\mathfrak{S}_5$ est d'ordre $\frac{120}{6} = 20$. Si, par l'absurde, un 3-cycle appartient à un tel normalisateur, on a par Lagrange que 3 divise 20, absurde.

   (b) L'image d'un 3-cycle σ par ϕ est un élément d'ordre 3 de $\mathfrak{S}_6$; c'est donc, soit un 3-cycle, soit un produit de deux 3-cycles à supports disjoints. Dans le premier cas, σ stabilise au moins un 5-Sylow (il en stabilise exactement 3), donc, σ est dans le normalisateur d'un 5-Sylow, ce qui est absurde. Ainsi, $\phi(\sigma)$ est un double 3-cycle.

5. On calcule la norme du caractère :

$$\langle \chi_{\text{perm}} - \chi_{\text{triv}}, \chi_{\text{perm}} - \chi_{\text{triv}} \rangle_{\mathfrak{A}_5} = \frac{1}{60}(5^2 + 15 \times 1^2 + 20 \times (-1)^2 + 24 \times 0^2) = 1.$$

   L'action de $\mathfrak{S}_5$ sur ses 5-Sylow fournit donc une représentation irréductible de degré 5. Par un résultat classique, l'irréductiblité implique le fait que l'action est doublement transitive [2].

2. On peut le faire par une méthode qui n'utilise pas la théorie des représentations : soit σ un 5-cycle de $\mathfrak{S}_5$. Il a pour image un 5-cycle $\phi(\sigma)$ de $\mathfrak{S}_6$ qui laisse donc fixe un unique 5-Sylow P. On fixe un 5-Sylow Q distinct de P et on veut montrer que pour tout couple (P', Q') de 5-Sylow distincts, il existe g qui envoie (P', Q') sur (P, Q). Il suffit de prendre $\phi(\sigma)^k h$, où h envoie P' sur P et où k est tel que $\phi(\sigma)^k(Q') = Q$.