Correction d'un exercice : Préparation à l'agrégation - mathématiques
2014-2015

Correction de l'exercice II (5), feuille 2 :

Calculer les polynômes cyclotomiques Rappel : Par les exercices déjà corrigés, on sait que $\Phi_n(X)$ est un polynôme irréductible unitaire avec coefficients dans $\mathbf{Z}$ de degré $\varphi(n)$. Les racines sont $\{\eta^k\}$ pour $1 \leq k \leq n-1$ et k premier avec n. Si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, où $p_1, \ldots, p_r$ sont premiers et distincts, et $\alpha_1, \ldots, \alpha_r \geq 1$, alors $\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1)$.

On a aussi : $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

(a) Si tout les premiers qui divisent m divisent aussi n, alors, $\Phi_{mn} = \Phi_n(X^m)$.
(b) Si p est premier et p ne divise pas n, alors $\Phi_{pn}(X) = \Phi_n(X^p)$.
(c) (Cas de Φ_p si p est premier.)
(d) Trouver $\Phi_{24}(X)$.
(e) Trouver $\Phi_{2^k}(X)$.

(a) Corrigé en cours. On remarque que les deux polynômes sont unitaires et ont le même degré. On montre que chaque racine (complexe) de $\Phi_{mn}(X)$ est aussi racine de $\Phi_n(X^m)$.

(b) D'abord on remarque que $\deg(\Phi_{pn}(X) = (p-1)\varphi(n) = \deg(\Phi_n(X^p)) - \deg(\Phi_n(X))$. Donc $\Phi_{pn}(X) * \Phi_n(X)$ a la même degré que $\Phi_n(X^p)$, les deux facteurs sont irréductibles et distincts (donc le produit est à racines simples). Comme le degré est égal au degré de $\Phi_n(X^p)$, il suffit de montrer que chaque racine de $\Phi_n(X)$ et de $\Phi_{np}(X)$ est racine de $\Phi_n(X^p)$. On peut argumenter comme pour la partie (a).

(c) On a $\Phi_2(X) = X + 1$. Donc $\Phi_6(X) = \Phi_2(X^3)/\Phi_2(X) = (X^3+1)/(X+1) = X^2 - X + 1$. $\Phi_{24}(X) = \Phi_6(X^4) = X^8 - X^4 + 1$.

(d) $\Phi_{2^k}(X) = \Phi_2(X^{2^{k-1}}) = X^{2^{k-1}} + 1$.

Théorème de Wedderburn : Exercice III, feuille 2 : Indications pour la correction

(1) La somme, différence, produit de deux éléments du centre est dans le centre. L'inverse d'un élément dans le centre est dans le centre. K est un $Z(K)$-espace vectoriel Car K est un groupe additif, muni d'une loi de multiplication par $Z(K)$ qui satisfait les hypothèses de l'espace vectoriel. Si K est de dimension k comme $Z(K)$-espace vectoriel, et si $|Z(K)| = q$, alors $|K| = q^k$.

(2)(a) K_x est un sous-corps (pas nécessairement abélien) de K qui contient $Z(K)$. Ainsi K_x est un $Z(K)$ sous-espace vectoriel, donc la cardinalité de K_x est q^d avec $(d \leq n)$.

Remarque : On peut aussi montrer que $d|n$, car K est un K_x-module libre à gauche, où K_x est un anneau, pas nécessairement abélien. Mais nous allons démontrer ceci plus tard, sans utiliser la théorie des modules à gauche (ou de l'espace vectoriel sur un corps non-commutatif).

(2)(b) Le sous-groupe d'isotropie de x est $K_x \backslash \{0\}$. Donc l'ordre de l'orbite est : $(|K|-1)/(|K_x|-1) = (q^n-1)/(q^d-1)$.

(2)(c) On va d'abord montrer que d divise n (voir remarque de (2)(a)). On a, de (2)(b) que q^d-1 divise q^n-1. Par la divison euclidienne, il existe $Q, r \in \mathbf{Z}$ avec $n = Qd + r$, et $0 \leq r \leq d-1$. Alors q^d-1 divise $q^n - 1 - (q^{n-d} + d^{n-2d} + \cdots + q^{n-Qd})(q^d-1) = q^{n-Qd} - 1 = q^r - 1$. Comme r est strictement plus petit que d, on a que $q^d - 1 < q^r - 1$. L'unique possibilité est donc que $r = 0$, et d divise n.

On sait que $X^n - 1 = \prod_{k|n} \Phi_k(X)$, et $X^d - 1 = \prod_{k|d} \Phi_k(X)$. Comme $d|n$, on a $X^n - 1 = (X^d - 1) \prod_{k \not| d, k|n} \Phi_k(X)$. En posant $X = q$, on a : $q^n - 1 = (q^d - 1) \prod_{k \not| d, k|n} \Phi_k(q)$, ou bien $(q^n-1)/(q^d-1) = \prod_{k \not| d\ , k|n} \Phi_k(q)$. En particulier, si $n \neq d$, on a que $\Phi_n(q)$ divise $(q^n-1)/(q^d-1)$.

(3) Pour chaque $x \in K^* \setminus Z(K)$, il existe $d_x < n$ tel que $|\omega(x)| = (q^n-1)/(q^{d_x}-1)$. On a alors :

$$q^n - 1 = |K^*| = |Z(K)| - 1 + \sum \frac{q^n - 1}{q^{d_i} - 1}.$$

$\Phi_n(q)$ divise chaque terme de la somme et $q^n - 1$. Donc $\Phi_n(q)$ divise $|Z(K)| - 1 = q - 1$.

(4) On a $\Phi_n(q) = \prod_{1 \leq k \leq n, pgcd(n,k)=1} (q - \eta^k) \in \mathbf{C}$, ou $\eta = e^{2\pi i/n}$. Si on considère le module $|\Phi_n(q)|$, comme $|q - \eta^k| > q - 1 \geq 1$ pour chaque k, on a $\Phi_n(q) = |\Phi_n(q)| > |q-1|^{\varphi(n)} \geq (q-1)$. Ceci contredit (3).