Université Pierre et Marie Curie — Année 2014-2015
M2 Enseignement de Mathématiques — Préparation à l'écrit d'algèbre de l'Agrégation
Professeur : P. Charollois

Problème de Mathématiques Générales no. 2.

Préambule :

• a) on dit qu'une action d'un groupe G sur un ensemble X est **transitive** si l'orbite de tout élément $x \in X$ sous l'action de G est l'ensemble X tout entier.

• b) Lorsque p est un nombre premier, on note $\mathbb{F}_p$ le corps fini $\mathbb{Z}/p\mathbb{Z}$. On rappelle que le groupe multiplicatif L^* d'un corps fini L est un groupe abélien **cyclique**.

• c) Soit $n \geq 1$ un entier. On note $\mathcal{P}_n \subset \mathbb{C}^*$ l'ensemble des nombres complexes de la forme $z = e^{\frac{2ik\pi}{n}}$, $1 \leq k \leq n$ où $k \in \mathbb{N}$ est premier avec n. C'est l'ensemble des racines primitives n-ièmes de l'unité dans $\mathbb{C}$. On note $\varphi(n)$ le cardinal de $\mathcal{P}_n$.

• d) On rappelle que, pour tout entier $n \geq 1$, le n-ième polynôme cyclotomique $\Phi_n(X)$ est défini par

$$\Phi_n(X) = \prod_{\zeta \in \mathcal{P}_n} (X - \zeta).$$

Le polynôme Φ_n est dans $\mathbb{Z}[X]$. Cette famille de polynômes satisfait l'identité $X^n - 1 = \prod_{d|n} \Phi_d(X)$. De plus Φ_n est un polynôme **irréductible** de $\mathbb{Q}[X]$ et de $\mathbb{Z}[X]$.

• e) Pour tout nombre réel x, notons $\pi(x)$ le nombre de nombres premiers inférieurs ou égaux à x. On admettra les inégalités suivantes dues à Tchebychev : il existe deux constantes positives $c_1 > 0$ et $c_2 > 0$ telles que pour tout $x > 1$ on a $c_1 \frac{x}{\log x} \leq \pi(x) \leq c_2 \frac{x}{\log x}$.

• f) Soit p un nombre premier. On définit le symbole de Legendre associé à un entier $k \in \mathbb{Z}$ en posant

$$\left(\frac{k}{p}\right)_p = \begin{cases} 1 & \text{si } k \mod p \text{ est un carré non nul de } \mathbb{F}_p, \\ 0 & \text{si } p \text{ divise } k, \\ -1 & \text{si } k \mod p \text{ n'est pas un carré de } \mathbb{F}_p. \end{cases}$$

• g) Lorsque $P = a_r X^r + a_{r-1} X + \ldots + a_1 X + a_0$ et $Q = b_s X^s + b_{s-1} X^{s-1} + \ldots + b_1 X + b_0$ sont deux polynômes de $K[X]$ non-constants définis sur un corps K, de degrés respectifs r et s, on leur associe la matrice de Sylvester $Syl(P,Q) \in M_{r+s}(K)$ donnée par

$$Syl(P,Q) := \left(\begin{array}{cccccccc} a_r & a_{r-1} & a_{r-2} & \ldots & a_0 & 0 & \ldots & 0 \\ 0 & a_r & a_{r-1} & \ldots & a_1 & a_0 & 0 & \ldots \\ 0 & \ddots & \ddots & \ldots & \ldots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & a_r & \ldots & \ldots & a_1 & a_0 \\ b_s & b_{s-1} & \ldots & b_1 & b_0 & 0 & \ldots & 0 \\ 0 & b_s & b_{s-1} & \ldots & b_1 & b_0 & 0 & \ldots \\ 0 & \ddots & \ddots & \ldots & \ldots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & b_s & \ldots & \ldots & b_1 & b_0 \end{array} \right) \begin{array}{l} \left. \vphantom{\begin{array}{c} a \\ a \\ a \\ a \end{array}} \right\} s \text{ lignes similaires décalées} \\ \left. \vphantom{\begin{array}{c} a \\ a \\ a \\ a \end{array}} \right\} r \text{ lignes similaires décalées} \end{array}.$$

Le résultant $Res(P,Q)$ de P et Q est le déterminant de cette matrice :

$$Res(P,Q) := \det Sylv(P,Q).$$

Lorsque le polynôme P est **unitaire et scindé** sur K, de racines $\alpha_1, \ldots, \alpha_r \in K$, on rappelle la formule supplémentaire suivante :

$$Res(P,Q) = \prod_{j=1}^{r} Q(\alpha_j). \tag{1}$$

Dépendance relative des parties :

La partie I est une partie préliminaire, utilisée dans les parties II, III, IV, V. La partie II n'est pas utilisée dans les parties suivantes. La partie III n'est pas utilisée dans les parties suivantes. La partie VI n'utilise que la question de cours (0).

(0) (Question de cours). Soit $n \geq 2$ un entier, et $p_1, \cdots p_r$ les nombres premiers distincts tels que $n = p_1^{a_1} \cdots p_r^{a_r}$ avec $\forall j, a_j \geq 1$. Démontrer que la fonction φ d'Euler vérifie

$$\varphi(n) = n \prod_{j=1}^{r} (1 - \frac{1}{p_j}) = \prod_{j=1}^{r} p_j^{a_j - 1}(p_j - 1).$$

Partie I. Généralités sur les polynômes cyclotomiques.

1) Soit $\mu : \mathbb{N}^* \to \{0, \pm 1\}$ la fonction définie par $\mu(1) = 1$, $\mu(n) = 0$ si n est divisible par un facteur carré, et $\mu(p_1 \cdots p_r) = (-1)^r$ si $p_1, \ldots, p_r$ sont des premiers distincts. Démontrer que pour tout $n > 1$ on a

$$\sum_{d|n} \mu(d) = 0,$$

où la sommation porte sur tous les diviseurs $d \geq 1$ de n. (On pourra commencer par traiter le cas où $n = p^a$ pour un nombre premier p).

2) Démontrer que

$$\Phi_n(X) = \prod_{d|n} (X^{\frac{n}{d}} - 1)^{\mu(d)}. \tag{2}$$

(On pourra intervertir les produits $\prod_{d|n} \prod_{h|d} u_{h,d}$ pour des fractions rationnelles $u_{h,d} \in \mathbb{Q}(X)$ à déterminer).

3) Soit p un nombre premier et $a \geq 1$ un entier. Calculer les coefficients de $\Phi_p(X)$, et démontrer que $\Phi_{p^a}(X) = \Phi_p(X^{p^{a-1}})$.

4) Soit p un nombre premier, et $n \geq 1$ un entier.

4.a) Démontrer que, si p ne divise pas n, alors

$$\Phi_{pn}(X) = \frac{\Phi_n(X^p)}{\Phi_n(X)}. \tag{3}$$

4.b) Démontrer que, si p divise n, alors

$$\Phi_{pn}(X) = \Phi_n(X^p). \tag{4}$$

5.a) Soient $p_1, \ldots, p_r$ des nombres premiers distincts, et $a_1 \geq 1, \ldots, a_r \geq 1$ des entiers. Montrer que

$$\Phi_{p_1^{a_1} \cdots p_r^{a_r}}(X) = \Phi_{p_1 \cdots p_r}(X^{p_1^{a_1-1} \cdots p_r^{a_r-1}}). \tag{5}$$

5.b) Démontrer que, si $m \geq 1$ est un entier impair, alors $\Phi_{2m} = \Phi_m(-X)$.

6) Démontrer que, pour entier $n > 1$, on a les formules suivantes : $\Phi_n(0) = 1$, et

$$\begin{cases} \Phi_n(1) = p & \text{si } n = p^a \text{ pour un nombre premier } p \text{ et un entier } a \geq 1, \\ \Phi_n(1) = 1 & \text{sinon.} \end{cases}$$

Partie II. Formule de Ramanujan.

Dans cette partie, on définit pour $n \geq 2$ l'entier $c_1(n)$ comme le coefficient du monôme X dans le polynôme $\Phi_n(X)$. Par exemple, $\Phi_2(X) = X+1$ donc $c_1(2) = 1$, et $\Phi_6(X) = X^2-X+1$ donc $c_1(6) = -1$. On complète cette définition en posant $c_1(1) = -1$.

7) Calculer $c_1(3)$, $c_1(4), c_1(5), c_1(7), c_1(8)$. Démontrer que, si $n > 1$, on a $\sum_{d|n} c_1(d) = 0$.

8) Démontrer que, pour tout $n \geq 1$ on a $c_1(n) = -\mu(n)$.

Dans la question suivante, on fixe un entier $k \geq 1$ et l'on pose $d := pgcd(k, n)$ et $e := n/d$.

9.a) Montrer que l'application $f : z \mapsto z^k$ définit une application de $\mathcal{P}_n$ dans $\mathcal{P}_e$.

9.b) Montrer que l'on peut munir les ensembles $\mathcal{P}_n$ et $Im(f)$ d'une action transitive du groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$.

9.c) En déduire que f est surjective, et que pour tout $\theta \in \mathcal{P}_e$, l'ensemble $f^{-1}(\theta)$ possède $\varphi(n)/\varphi(e)$ éléments.

9.d) On définit le polynôme $\Psi_{k,n}(X) = \prod_{\zeta \in \mathcal{P}_n}(X - \zeta^k)$. Justifier que $\Psi_{k,n} = (\Phi_e)^{\frac{\varphi(n)}{\varphi(e)}}$.

9.e) Démontrer la formule de Ramanujan :

$$\sum_{\zeta \in \mathcal{P}_n} \zeta^k = -\mu(e)\frac{\varphi(n)}{\varphi(e)}.$$

Partie III. Coefficients de polynômes cyclotomiques.

Dans cette partie, et dans toute la suite du problème, p et q désignent deux nombres premiers impairs distincts.

10) Soit $m \geq 0$ un entier. Démontrer qu'il existe au plus un couple d'entiers $(a, b) \in \mathbb{N}^2$, avec $0 \leq a$ et $0 \leq b < p$, tels que $m = ap + bq$.

11) Démontrer que la série formelle $\frac{1}{(1-X^p)(1-X^q)} = \sum_{m \geq 0} a_m X^m \in \mathbb{Q}[[X]]$ a des coefficients $a_m \in \{0, 1\}$ pour tout entier m tel que $0 \leq m < pq$.

12) Déduire de la question précédente que les coefficients du polynôme cyclotomique $\Phi_{pq}(X)$ appartiennent à l'ensemble $\mathcal{L} := \{0, 1, -1\}$.

13) Démontrer que, si n est un entier tel que $1 \leq n \leq 104$, alors Φ_n est un polynôme dont tous les coefficients sont dans l'ensemble $\mathcal{L} = \{0, 1, -1\}$.

14.a) En utilisant la question (2) et en faisant un développement limité, calculer le coefficient de x^7 du polynôme $\Phi_{105}(x)$. En déduire que Φ_{105} possède au moins un coefficient qui n'appartient pas à l'ensemble $\mathcal{L} = \{0, 1, -1\}$.

Dans la suite de cette question on fixe un entier $t \geq 2$.

14.b) En utilisant le théorème de Tchebychev rappelé en préambule, démontrer qu'il existe t nombres premiers $p_1, \ldots, p_t$ qui vérifient simultanément les inégalités

$$2 < p_1 < p_2 < \cdots < p_t < p_1 + p_2.$$

14.c) Posons $n_t = p_1 \cdots p_t$. Calculer le coefficient de X^{p_t} du polynôme $\Phi_{n_t}(X)$. En déduire que, pour tout $M > 0$, il existe un polynôme cyclotomique qui possède au moins un coefficient supérieur à M.

Partie IV. Réduction modulo ℓ de polynômes cyclotomiques.

15) Justifier que Φ_n et Φ_m sont premiers entre eux dans $\mathbb{Z}[X]$ si $n \neq m$.

16.a) Soit K un corps, et $n \geq m \geq 1$ deux entiers. Dans l'anneau $\mathbb{Z}$, la division euclidienne de n par m s'écrit $n = mq + r$ avec $0 \leq r < n$. Calculer, en fonction de q et de r, le quotient et le reste de la division euclidienne dans $K[X]$ de $X^n - 1$ par $X^m - 1$.

16.b) Montrer que le pgcd de $X^n - 1$ et $X^m - 1$ dans $K[X]$ est $X^{\mathrm{pgcd}(n,m)} - 1$.

16.c) Soit ℓ un nombre premier. Démontrer que si $m \geq 2$ et $n \geq 2$ sont deux entiers premiers entre eux, alors les polynômes $(\Phi_m \mod \ell)$ et $(\Phi_n \mod \ell)$ sont premiers entre eux dans $\mathbb{F}_\ell[X]$.

17) Soit $m \geq 1$ et $n \geq 1$ des entiers, et ℓ un nombre premier. On suppose dans toute cette question que ℓ ne divise ni m ni n.

17.a) Démontrer que le polynôme $X^{mn} - 1 \mod \ell$ est premier avec sa dérivée dans $\mathbb{F}_\ell[X]$.

17.b) Justifier que $X^{mn} - 1 \mod \ell$ ne possède par de facteur carré dans $\mathbb{F}_\ell[X]$.

17.c) En déduire que les polynômes $(\Phi_m \mod \ell)$ et $(\Phi_n \mod \ell)$ sont premiers entre eux dans $\mathbb{F}_\ell[X]$.

Dans cette partie encore, et dans toute la suite du problème, p et q désignent des nombres premiers impairs distincts.

18) En utilisant la question (2), montrer que

$$\Phi_p(X) \bmod p \equiv (X-1)^{p-1} \bmod p, \quad \text{et } \Phi_{pq} \bmod p \equiv (\Phi_q)^{p-1} \bmod p. \tag{6}$$

19) Déterminer tous les nombres premiers $\ell \geq 2$ tels que $(\Phi_{pq} \mod \ell)$ et $(\Phi_p \mod \ell)$ ne sont pas premiers entre eux dans $\mathbb{F}_\ell[X]$.

20) Démontrer que le résultant $Res(\Phi_p, \Phi_q)$ est un entier relatif, et que cet entier est congru à q^{p-1} modulo p.

21.a) Déduire de la question précédente que

$$Res(\Phi_p, \Phi_q) = 1. \tag{7}$$

21.b) Quelles sont les racines complexes de Φ_p ? En déduire la formule

$$\prod_{j=1}^{p-1}\prod_{k=1}^{q-1}\left(e^{\frac{2i\pi k}{p}}-e^{\frac{2i\pi j}{q}}\right)=1. \tag{8}$$

21.c) Démontrer que $Res(\Phi_p,\Phi_{pq})=q^{p-1}$. (on pourra utiliser la relation (3)).

22) (**factorisation modulo ℓ des polynômes cyclotomiques**).

Soit $n\geq 1$ un entier et $\ell\geq 2$ un nombre premier qui ne divise pas n. Notons r l'ordre de ℓ dans le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$.

22.a) Justifier que r divise $\varphi(n)$. Démontrer que les polynômes $X^n-1 \bmod \ell$ et $\Phi_n \bmod \ell$ sont sans facteurs carrés dans $\mathbb{F}_\ell[X]$.

22.b) Soit A un anneau unitaire intègre. On note $\widetilde{\Phi_n}$ l'image naturelle de Φ_n dans $A[X]$. Montrer que les racines de $\widetilde{\Phi_n}$ dans A sont exactement les racines primitives n-ièmes de l'unité contenues dans A.

22.c) Démontrer que $(\Phi_n \bmod \ell)$ se factorise dans $\mathbb{F}_\ell[X]$ en un produit de $\varphi(n)/r$ facteurs irréductibles distincts, tous de même degré, et que r est ce degré commun.

22.d) Soit ℓ un nombre premier. Démontrer que le polynôme $(\Phi_8 \bmod \ell)$ n'est pas irréductible dans $\mathbb{F}_\ell[X]$.

22.e) Soient ℓ,p,q trois nombres premiers, tels que p et q sont impairs et distincts. Démontrer que le polynôme $(\Phi_{pq} \bmod \ell)$ n'est pas irréductible dans $\mathbb{F}_\ell[X]$.

Partie V. Loi de réciprocité quadratique, selon la méthode d'Eisenstein.

Dans cette partie, p et q désignent deux nombres premiers impairs distincts.

23.a) Démontrer que, pour tout entier $d\geq 1$, il existe un polynôme $H_d\in\mathbb{Z}[X]$, unitaire et de degré d tel que $X^d+X^{-1/d}=H_d(X+1/X)$.

23.b) Justifier qu'il existe un unique polynôme $T_p\in\mathbb{Z}[X]$ à coefficients entiers, unitaire, de degré $\frac{p-1}{2}$, tel que $X^{-\frac{p-1}{2}}\Phi_p(X)=T_p(X+1/X)$.

24.a) Déterminer les racines réelles de T_p.

24.b) Démontrer que $T_p(X)\equiv (X-2)^{\frac{p-1}{2}} \bmod p$.

25.a) Démontrer que pour tout $p\geq 3$, $T_p(X)$ est un polynôme irréductible dans $\mathbb{Q}[X]$.

25.b) Soit p est un nombre premier tel que $p\equiv 3 \bmod 4$. Quelle est la dimension du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}(\cos(\frac{2\pi}{p}))$? En déduire que le nombre réel $\sqrt{p}$ n'appartient pas au corps $\mathbb{Q}(\cos\frac{2\pi}{p})$.

26.a) Démontrer la formule $\sum_{k=0}^{p-1}\left(\frac{k}{p}\right)_p=0$.

26.b) Pour p un nombre premier impair on pose $\tau_p:=\sum_{k=1}^{p-1}\left(\frac{k}{p}\right)_p e^{\frac{2i\pi k}{p}}\in\mathbb{C}$. Démontrer que

$$\tau_p^2=\left(\frac{-1}{p}\right)_p p.$$

(on pourra effectuer un changement de variable judicieux pour faire apparaître τ_p^2 comme une somme de sommes géométriques).

26.c) En déduire que si p est un nombre premier impair tel que $p \equiv 1 \mod 4$, alors $\sqrt{p}$ appartient au corps $\mathbb{Q}(\cos(\frac{2\pi}{p}))$.

27) Démontrer que $Res(T_p, T_q)$ est un entier de $\mathcal{L} := \{0, 1, -1\}$. (on pourra utiliser la question 17.b)).

28) Démontrer que $Res(T_p \mod p, T_q \mod p) \equiv q^{\frac{p-1}{2}} \mod p$.

29) Démontrer la loi de réciprocité quadratique : si p et q sont des premiers impairs, alors

$$\left(\frac{q}{p}\right)_p \left(\frac{p}{q}\right)_q = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

30) Démontrer la formule d'Eisenstein

$$\left(\frac{q}{p}\right)_p = (-4)^{\frac{(p-1)(q-1)}{4}} \prod_{k=1}^{\frac{p-1}{2}} \prod_{j=1}^{\frac{q-1}{2}} \left(\sin^2(\frac{2k\pi}{p}) - \sin^2(\frac{2j\pi}{q})\right).$$

31) Pour tout entier $n \geq 0$ on pose $F_n = 2^n+1$. Déduire de la loi de réciprocité quadratique que F_n est premier si et seulement si $5^{\frac{F_n-1}{2}} = -1 \mod F_n$.

Partie VI. Variations de $\varphi(n)$.

(Cette partie est totalement indépendante des parties précédentes : elle n'utilise que le Préambule et la question de cours (0)).

32) Déterminer les entiers $n \geq 1$ tels que $\varphi(n) \leq 2$, puis les entiers $n \geq 1$ tels que $\varphi(n) \leq 3$.

33) Soit $\mathcal{N} \subset \mathbb{N}$ une partie de l'ensemble des entiers naturels. Démontrer que si la partie $\varphi(\mathcal{N})$ est bornée, alors $\mathcal{N}$ est également bornée.

34) Soit K un sous-corps de $\mathbb{C}$ tel que K est une extension de degré fini d de $\mathbb{Q}$. Démontrer que K ne contient qu'un nombre fini de racines de l'unité.

(35) Démontrer que $\varphi(n)$ tend vers $+\infty$ quand n tend vers $+\infty$.