Concours Agrégation, Mathématiques générales

Leçon 44- Racines d'un polynôme. Fonctions symétriques élémentaires.

Commentaires du jury 2015 : Il s'agit d'une leçon au spectre assez vaste. On peut y traiter de méthodes de résolutions, de théorie des corps (voire théorie de Galois si affinités), de topologie (continuité des racines) ou même de formes quadratiques. Il peut être pertinent d'introduire la notion de polynôme scindé, de citer le théorème de d'Alembert-Gauss et des applications des racines (valeurs propres, etc.). On pourra parler des applications de la réduction au calcul d'approximations de racines. Notons le lien solide entre la recherche des racines d'un polynôme et la réduction des matrices. Les valeurs propres de la matrice compagnon d'un polynôme permet d'entretenir ce lien. Les problèmes de localisation des valeurs propres, comme les disques de Gershgorin, sont tout à fait appropriés à ce contexte.
Commentaires du jury 2016 : Dans cette leçon on peut présenter des méthodes de résolutions, de la théorie des corps, des notions de topologie (continuité des racines) ou même des formes quadratiques. Il peut être pertinent d'introduire la notion de polynôme scindé, de citer le théorème de d'Alembert-Gauss et des applications des racines (valeurs propres, etc.). Notons le lien solide entre la recherche des racines d'un polynôme et la réduction des matrices ; les valeurs propres de la matrice compagnon d'un polynôme permet d'entretenir ce lien. S'ils le désirent, les candidats peuvent s'aventurer en théorie de Galois ou s'intéresser à des problèmes de localisation des valeurs propres, comme les disques de Gershgorin.

Remarque : Les disques de Gershgorin se déduisent du théorème de Hadamard de la diagonale dominante. Pour les méthodes d'approximation des racines on peut lire
http ://iml.univ-mrs.fr/∼ritzenth/agregation/cours-polynomes2.pdf

Dans la rubrique localisation des zéros d'un polynôme on peut citer le théorème de Gauss-Lucas [Fr. MMG] p. 20, la règle de Descartes [F. M. 1] $n°110$ voir aussi [B. R.] ou le théorème de Sturm [F. M. 1] $n°109$.

Bibliographie

[F. M. 1] Fresnel J., Matignon M. *Algèbre et Géométrie* (Hermann 2011)
[F. M. 1'] Errata, https ://www.math.u-bordeaux.fr/∼mmatigno/Errata-Alg-Géom.pdf
[F. M. 2] Fresnel J., Matignon M. *Algèbre et Géométrie-81 thèmes pour l'agrégation* (ellipses 2017)
[F. M. 2'] Compléments et errata, https ://www.math.u-bordeaux.fr/∼mmatigno/Errata-FM2.pdf
[Fr. F] Fresnel J. *Anneaux* (Hermann 2001)
[Fr. MMG] Fresnel J. *Méthodes modernes en géométrie* (Hermann 1996, 2010)
et
[B. R.] Boyer P. ,Risler J.-J. *Algèbre pour la licence 3* (Dunod 2006)
[F. G.] Francinou Gianella *Exercices de mathématiques pour l'agrégation Algèbre 1* (Elsevier Masson 1995)
[Sa.] Samuel P. *Théorie algébrique des nombres* (Hermann 1997)

Développements conseillés :

(1) Théorème de continuité des racines d'un polynôme à coefficients complexes et applications. Une preuve séquentielle : [F. G.] p. 232. La preuve dans [F. M. 1] $n°32$ question 2 est plus conceptuelle mais correspond parfaitement au titre de la leçon. Voir exercice ci-dessous. Pour les applications voir [F. M. 1] $n°32$ questions 3 et 4.

(2) Un théorème de Kronecker et application aux matrices de $\mathrm{GL}_n(\mathbb{Z})$, [Fr. F] p. 201 et exercice ci-dessous.

(3) Le corps des nombres complexes est algébriquement clos, [Sa.] Appendice, attention à veiller dans l'application du théorème de structure des polynômes symétriques à introduire des indéterminées.

(4) Signature de la matrice de Hankel associée aux racines d'un polynôme à coefficients réels, [F. M. 1] $n°40$ (il faut bien noter que l'on se donne les coefficients du polynôme (et pas une approximation

ce qui modifierait les multiplicités des racines ...) et pas les racines puisque il n'y a pas de formules de résolution par radicaux ... par contre les sommes de Newton se calculent algébriquement à partir des coefficients du polynôme et alors l'algorithme de Gauss donne la signature ; en fin de compte on obtient donc un algorithme pour compter le nombre de racines réelles distinctes ou complexes non réelles et distinctes.

Exercice 1 Continuité des racines d'un polynôme à coefficients complexes, [F. M. 1] $n°32$, voir en particulier les applications.

(1) Soient $P(X) = \prod_{1\leq i\leq r}(X-a_i)_i^{\alpha} = p_0 + p_1X + ... + p_{n-1}X^{n-1} + X^n \in \mathbb{C}[X]$ avec a_i 2 à 2 distincts. et $0 < \delta < \inf_{i\neq j}\frac{1}{2}|a_i - a_j|$. Alors il existe $\epsilon(P,\delta) > 0$ qui possède la propriété suivante : soit $Q(X) = q_0 + q_1X + ... + q_{n-1}X^{n-1} + X^n \in \mathbb{C}[X]$ avec $\max_{0\leq j<n}|p_j - q_j|\epsilon(P,\delta)$, alors chaque disque de centre a_i et de rayon δ contient α_i racines de Q en tenant compte de la multiplicité).

Dans [F. M. 1] cela est traduit par la bicontinuité de l'application entre espaces métriques $f : \mathbb{C}^n/S_n \to C^n$ définie par $f((x_1,....,x_n)) = \prod_{1\leq i\leq n}(X - x_i)$.

(2) Une autre approche traduit cela par la continuité séquentielle de f^{-1}, [F. G.] p. 232.

La méthode consiste à considérer une suite $Q_k(X) = q_{n,0} + q_1X + ... + q_{n-1}X^{n-1} + X^n$ qui converge vers P. On note $x_{k,i}$ les n racines de $Q_k(X)$ en comptant la multiplicité.

(a) Montrer qu'il existe $M > 0$ avec $\forall i, k\ |x_{k,i}| < M$

(b) Soit α la multiplicité d'une racine a de P. En raisonnant par l'absurde montrer que pour tout $\epsilon > 0$ il existe $k_0 \leq 0$ tel que pour tout $k \geq k_0$ il y a au moins α racines $x_{k,i}$ vérifiant $|a - x_{k,i}| \leq \epsilon$.

(c) Conclure en remarquant que les degrès de P et de Q_k sont égaux.

Exercice 2 Le théorème de Gauss-Lucas, [Fr. MMG] p. 20.
Soit $P := \prod_{1\leq i\leq s}(Z - z_i)^{\mu_i} \in \mathbb{C}[Z]$ avec $z_i \neq z_j$ et $\mu_i > 0$.

(1) Montrer que les racines de P' sont dans l'enveloppe convexe $Conv(P)$ des $z_i, 1 \leq i \leq s$.

(2) On suppose que les racines de P sont dans $\mathbb{R}$, montrer qu'il en est de même pour les racines de P'.

(3) On suppose que les affixes des zéros P dans $\mathbb{C}$ ne sont pas alignés (on identifie $\mathbb{C}$ au plan affine réel). Montrer que si $P'(z) = 0$ alors $P(z) = 0$ (et donc z est racine multiple de P) ou bien z est à l'intérieur de l'enveloppe convexe des zéros de P.

Preuve. Notons z une racine de P'. On suppose que z est au bord $Conv(P) - Conv(P)^\circ$ de l'enveloppe convexe des zéros de P (notez que $Conv(P)$ est un fermé de $\mathbb{C}$ d'intérieur $Conv(P)^\circ$ non vide). Si $P(z) \neq 0$ alors il existe $z_1 \neq z_2$ des racines de P telles que z_1, z_2, z soient alignés (faire un dessin). Soit $D := z_1 + \mathbb{R}(z_2 - z_1)$ et projetons orthogonalement sur $D^\perp$ la relation barycentrique $\sum_{1\leq i\leq s}\frac{1}{|z-z_i|^2}(z - z_i) = 0$. Puisque $Conv(P)$ est dans le même demi-espace fermé défini par la droite D on obtient une contradiction. ///

(4) Dans le cas où P est de degré 3 on a une caractérisation géométrique des racines de P', [F. M. 1] $n°126$.

Exercice 3 Soit $P(X,Y) \in \mathbb{C}[X,Y]$ et n son degré total. On veut montrer que les zéros de $P(X,Y)$ dans $\mathbb{C}\times\mathbb{C}$ ne sont pas isolés, [F. M. 2] lemme p. 309.
Quitte à faire une translation on suppose que $P(0,0) = 0$

(1) Montrer qu'il existe $c \in \mathbb{C}$ avec $P(X + cY, Y) = p_0(X) + p_1(X)Y + ... + p_n(X)Y^n$ avec $p_i(X) \in \mathbb{C}[X]$, et $deg_i(p_i(X)) \leq n - i$ et $p_n(X) \in \mathbb{C} - \{0\}$.

Preuve. $P = \sum_{0\leq i\leq n} P_i$ la décomposition de P en composantes homogènes alors $P_n \neq 0$. Puisque le degré total de P est égal à n, seul P_n est susceptible de contribuer au coefficient de Y^n dans $P(X+$

$cY, Y)$. *On écrit alors* $P_n = \sum_{0\leq k\leq n} a_k X^{n-k}Y^k$, *alors le coefficient de* Y^n *dans* $P_n(X + cY, Y)$ *vaut* $\sum_{0\leq k\leq n} a_k c^{n-k}$. *Puisque* $(a_0, a_1, ..., a_n) \neq (0, 0, ..., 0)$ *il suit qu'il existe* $c \in \mathbb{C}$ *avec* $\sum_{0\leq k\leq n} a_k c^{n-k} \neq 0$. ///

(2) On suppose donc que $P = p_0(X)+p_1(X)Y+...+p_n(X)Y^n$ avec $p_n(X) \in \mathbb{C}-\{0\}$ et $P(0, 0) = 0$. Pour pour tout $k > 0$ on note $Q_k(Y) := P(\frac{1}{k}, Y)$, et on note $y_i(k), 1 \leq i \leq n$ les n racines de $Q_k(Y)$ dans $\mathbb{C}$ avec $|y_1(k)| \leq |y_2(k)|... \leq |y_n(k)|$. Montrer que la suite $(\frac{1}{k}, y_1(k))$ converge vers $(0, 0)$ et conclure.

Preuve. En effet $|y_1(k)|^n \leq \prod_{1\leq i\leq n} |y_i(k)| = \frac{|p_0(\frac{1}{k})|}{|p_n|} \to 0$. ///

Exercice 4 Les premiers qui divisent les valeurs d'un polynôme, [Fr. F.] ex. 1.9.36 p. 59.
Soit $P(X) \in \mathbb{Z}[X]$ non constant.

(1) On suppose que $P(0) = 1$. En considérant les diviseurs premiers de $P(n!)$, montrer que P a une racine modulo p pour une infinité de nombre premiers p.
Preuve. Puisque P *n'est pas constant il existe* $A > 0$ *avec* $|P(x)| > 1$ *pour tout* $x > A$. *Ainsi si* $n \in \mathbb{N}$ *avec* $n! > A$ *alors* $P(n!) \in \mathbb{Z} - \{-1, 0, 1\}$, *ainsi il existe* p_n *un diviseur premier de* $P(n!)$ *et donc* $n!$ mod p_n *est une racine de* P *modulo* p_n. *Puisque* $P(0) = 1$ *il suit que* $p_n \nmid n!$ *et donc que* $p_n > n$. ///

(2) Même question dans le cas général (si $P(0) \neq 0$, on pourra considérer le polynôme $\frac{P(XP(0))}{P(0)}$).
Preuve. Si $P(0) = 0$ *le résultat est trivial. Supposons que* $P(0) \neq 0$ *alors* $P = a_0 + a_1X + ... + a_dX^d$ *avec* $d > 0$, $a_k \in \mathbb{Z}$, *et* $a_0a_d \neq 0$. *Alors* $Q(X) := \frac{P(XP(0))}{P(0)} \in \mathbb{Z}[X]$ *et* $Q(0) = 1$. *On applique la question précédente à* Q. ///

Exercice 5 Un théorème de Kronecker et une application aux matrices $\in \mathrm{GL}_n(\mathbb{Z})$: les polynômes unitaires de $\mathbb{Z}[X]$ dont les racines complexes vérifient $0 < |z| \leq 1$ sont les produits de polynômes cyclotomiques, [Fr. F] p. 201.
Soit $P(X) \in \mathbb{Z}[X]$ un polynôme unitaire à coefficients entiers, de degré $n \geq 1$. On suppose que les racines complexes de $P(X)$ sont de module ≤ 1.

(1) Notons $s_1, ..., s_n \in \mathbb{Z}[X_1, ..., X_n]$ les polynômes symétriques élémentaires. Soit $r \geq 1$, on note $\rho : \mathbb{Z}[X_1, ..., X_n] \to \mathbb{Z}[X_1, ..., X_n]$ l'unique homomorphisme tel que $\rho(a) = a$ pour $a \in \mathbb{Z}$ et $\rho(X_i) = X_i^r$ pour tout $1 \leq i \leq n$ (c'est la propriété universelle des anneaux de polynômes). Montrer en utilisant ρ que $\forall\sigma \in S_n$ on a $s_k(X^r_{\sigma(1)}, ..., X^r_{\sigma(n)}) = s_k(X_1^r, ..., X_n^r)$, en déduire que pour tout $k \leq n$, il existe $P_{r,k}(S_1, ..., S_n) \in \mathbb{Z}[S_1, ..., S_n]$ tel que $s_k(X_1^r, ..., X_n^r) = P_{r,k}(s_1, ..., s_n)$.

(2) Calculer $s_k(1, ..., 1)$.

(3) Notons $\theta_1, ..., \theta_n$ les racines complexes (éventuellement répétées) de $F(X)$. Montrer que pour tout $r \geq 1$ et tout $k \leq n$, on a
$$s_k(\theta_1^r, ..., \theta_n^r) \in \mathbb{Z}, \quad |s_k(\theta_1^r, ..., \theta_n^r)| \leq \binom{n}{k}.$$

(4) Montrer que l'ensemble $\{\theta_i^r \mid 1 \leq i \leq n, r \geq 1\}$ est fini.

(5) En déduire que pour toute racine θ de $P(X)$, il existe $r \geq 2$ tel que $\theta^r = \theta$. Conclure.

(6) En déduire la décomposition en irréductible de P dans $\mathbb{Z}[X]$.

(7) Une application du théorème de Kronecker.
Soit $M \in \mathrm{GL}_n(\mathbb{Z})$, on suppose que la suite $M^k, k \in \mathbb{N}$ est bornée. Montrer que M est d'ordre fini.
Preuve. Si $\lambda \in \mathbb{C}$ *est racine de* χ_M *alors la suite* λ^k *est bornée ainsi* $|\lambda| \leq 1$. *Le théorème de Kronecker, [Fr. F] exercice 4.4.2 p. 201, appliqué au polynôme* χ_M *implique que les racines de* χ_M *sont des racines de l'unité ; ainsi il existe* $m > 0$ *avec* $\chi_{M^m} = (X - 1)^n$ *alors* $M^m = Id + N$ *où* N *est nilpotente. Montrons que* $N = 0$. *Pour cela nous allons montrer que si* $m_N(X) = X^d$ *avec* $d \geq 2$ *alors la suite*

M^{mk} est non bornée pour $k \to \infty$. La somme $\mathbb{C}N^0 + \mathbb{C}N + ... + \mathbb{C}N^{d-1} \subset M_n(\mathbb{C})$ est directe ainsi par l'équivalence des normes en dimension finie il existe $c > 0$ avec $\| \sum_{0 \leq i \leq d-1} a_i N^i \| \geq c \max_{0 \leq i \leq d-1} |a_i|$. Puisque $M^{mk} = (Id + N)^k = Id + \binom{k}{1} N + ... + \binom{k}{d-1} N^{d-1}$ et que $d \geq 2$, le résultat suit. ///

A propos des ordres des éléments de $\mathrm{GL}_n(\mathbb{Z})$ voir [F. M. 1] $n°26$ p. 46.

Exercice 6 Le lemme de Descartes, [F. M. 1] $n°110$, voir aussi [B. R.].

Soit $(a) := (a_0, a_1, ..., a_d)$, une suite finie de nombres réels. On appelle variation $V(a)$ de la suite (a) le nombre de changements de signes dans la suite privée des zéros. Soit $P(X) := a_0 + a_1 X + ... + a_d X^d \in \mathbb{R}[X]$ de degré d et $V(P) := V(a)$ et on note $Q(X) := P(-X)$. Soit $\nu_+(P)$ le nombre de racines > 0 de P comptées avec leurs multiplicités, alors $\nu_-(P) := \nu_+(Q)$ est le nombre de racines < 0 de P comptées avec leurs multiplicités. Alors $\nu_+(P) \leq V(P)$ et $\nu_+(P) = V(P) \mod 2$ resp. $\nu_-(P) \leq V(Q)$ et $\nu_-(P) = V(Q) \mod 2$.

(1) Soit $P = X^7 + 2X^6 - 3X^5 - X^2 + 7X - 8$. Montrer que $\nu_+(P) = 1$ ou 3.

(2) Soit $P = X^3 + 3X^2 - X - 2$. Montrer que $\nu_+(P) = 1$ et que $\nu_-(P) = 0$ ou 2. En remarquant que $Q(-1) = 1$, montrer que $\nu_-(P) = 2$.

(3) Soit $P = \prod_{1 \leq i \leq d} (X - x_i)$ avec $x_i \in \mathbb{R} - \{0\}$. Montrer que $V(P) + V(Q) \leq d$ et en déduire les égalités $\nu_+(P) = V(P)$ et $\nu_-(P) = V(Q)$.

(4) Soit $S \in Sym_n(\mathbb{R})$, montrer que la signature de S est (p, q) avec $p = V(\chi_S(X))$ et $q = V(\chi_S(-X))$.

Exercice 7 L'application $\mathrm{Sym}_n(\mathbb{R}) \to \mathbb{N} \times \mathbb{N}$ qui à S associe sa signature $(p(S), q(S))$ est continue sur $\mathrm{Sym}(\mathbb{R}) \cap \mathrm{GL}_n(\mathbb{R})$, [F. M. 1] $n°43$ p. 100.

Exercice 8 Discriminant, [F. M. 1] $n°112$ p.321 et en particulier les applications topologiques des questions 3 et 4.

Exercice 9 Résolution par radicaux de l'équation $\{x \in \mathbb{C},\ P(x) = 0\}$ avec $P(X) := X^3 + pX + q \in \mathbb{C}[X]$ et polynômes symétriques.

Notations. On note $\mathcal{S}_3$, le groupe symétrique sur $\{1, 2, 3\}$, il est engendré par les cycles $r := (1, 2, 3)$ et $s := (2, 3)$. Le groupe $\mathcal{S}_3$ agit sur $\mathbb{C}[X_1, X_2, X_3]$ par $\sigma \star P(X_1, X_2, X_3) = P(X_{\sigma(1)}, X_{\sigma(2)}, X_{\sigma(3)})$ et $\mathbb{C}[X_1, X_2, X_3]^{\mathcal{S}_3}$ est le sous-anneau des polynômes symétriques.

Enfin $j := e^{2i\pi/3} \in \mathbb{C}$, $U := X_1 + jX_2 + j^2 X_3$ et $V := s \star U$.

(1) (a) Montrer que $r \star U^3 = U^3$.
Preuve. On a $r \star U = X_2 + jX_3 + j^2 X_1 = j^2 U$. ///

(b) En déduire que $S := U^3 + V^3 \in \mathbb{C}[X_1, X_2, X_3]^{\mathcal{S}_3}$.
Preuve. Puisque $s \star U = V$ et que $s^2 = Id$ il suit que $s \star S = S$. Enfin $r \star V = rs \star U = sr^{-1} \star U = s \star U = V$. Ainsi $\mathcal{S}_3$ agit trivialement sur S. ///

(c) Montrer que $S(X_1, X_2, 0) = 2(X_1 + X_2)^3 - 9X_1X_2(X_1 + X_2)$.
Preuve. On calcule $S(X_1, X_2, 0) = (X_1 + jX_2)^3 + (X_1 + j^2 X_2)^3 = X_1^3 + 3j^2 X_1^2 X_2 + 3jX_1 X_2^2 + X_2^3 + X_1^3 + 3jX_1^2 X_2 + 3j^2 X_1 X_2^2 + X_2^3 = 2(X_1 + X_2)^3 - 9X_1X_2(X_1 + X_2)$. ///

(d) En déduire que $S - 2(X_1 + X_2 + X_3)^3 + 9(X_1X_2 + X_2X_3 + X_3X_1)(X_1 + X_2 + X_3) = \lambda X_1X_2X_3$.
Preuve. On applique l'algorithme vu dans la leçon. On remarque que $T := S - 2(X_1 + X_2 + X_3)^3 + 9(X_1X_2 + X_2X_3 + X_3X_1)(X_1 + X_2 + X_3) \in \mathbb{C}[X_1, X_2, X_3]^{\mathcal{S}_3}$ et que $T(X_1, X_2, 0) = 0$, ainsi $T \in X_3\mathbb{C}[X_1, X_2, X_3]$. Ainsi $T = r \star T \in X_1\mathbb{C}[X_1, X_2, X_3]$ et $T = r^2 \star T \in X_2\mathbb{C}[X_1, X_2, X_3]$. Ainsi dans la décomposition de T sur la base $X_1^{i_1} X_2^{i_2} X_3^{i_3}$ les coefficients des monômes avec $i_1 i_2 i_3 = 0$ sont nuls ainsi $T \in X_1X_2X_3\mathbb{C}[X_1, X_2, X_3]$. Pour conclure on remarque que T est homogène de degré 3. ///

(e) Calculer λ.

Preuve. On évalue l'égalité précédente en $(1,1,1)$. *Ainsi* $0-2.3^3+9.3.3=27=\lambda$. ///

(2) Soit $P:=X^3+pX+q=(X-x_1)(X-x_2)(X-x_3)\in\mathbb{C}[X]$. On note $u:=U(x_1,x_2,x_3), v:=V(x_1,x_2,x_3)$.

(a) En remarquant que $UV=(X_1+X_2+X_3)^2-3(X_1X_2+X_2X_3+X_3X_1)$, exprimer x_1,x_2,x_3 à l'aide de radicaux en p,q.

Preuve. On a $(X-x_1)(X-x_2)(X-x_3)=X^3-(x_1+x_2+x_3)X^2+(x_1x_2+x_2x_3+x_3x_1)X-x_1x_2x_3$. *Ainsi* $x_1+x_2+x_3=0$, $x_1x_2+x_2x_3+x_3x_1=p$ *et* $x_1x_2x_3=-q$. *Ainsi* $u^3+v^3=S(x_1,x_2,x_3)=-27q$ *et* $uv=-3p$. *Il suit que* u^3,v^3 *sont les deux racines du polynôme* $X^2+27q-27p^3$. *Son discriminant est* $\Delta=27(4p^3+27q^2)=\varpi^2$ *avec* $\varpi\in\mathbb{C}$. *Alors* $u^3=\frac{-27q+\varpi}{2}, v^3=\frac{-27q-\varpi}{2}$. *Quitte à permuter les* x_i *on a le système :* $x_1+x_2+x_3=0$, $x_1+jx_2+j^2x_3=u$, $x_1+j^2x_2+jx_3=v$ *d'où* $x_1=\frac{u+v}{3}$, $x_2=\frac{j^2u+jv}{3}$, $x_3=\frac{ju+j^2v}{3}$ *avec* $u^3=\frac{-27q+\varpi}{2}, v^3=\frac{-27q-\varpi}{2}$ *et* $uv=-3p$. ///

(b) Soit $P:=(X-1)(X^2+X+2)$. Déduire de la question précédente que

$$\sqrt{3}=\sqrt[3]{2\sqrt{7}+3\sqrt{3}}-\sqrt[3]{2\sqrt{7}-3\sqrt{3}}$$

.

Preuve. Puisque le discriminant de X^2+X+2 *est* -7, 1 *est la seule racine réelle de* P. *Avec les formules précédentes on obtient que* $x_1==\frac{u+v}{3}=\frac{1}{3}\sqrt{3}(\sqrt[3]{2\sqrt{7}+3\sqrt{3}}-\sqrt[3]{2\sqrt{7}-3\sqrt{3}})\in\mathbb{R}$ *est racine de* P. ///

Exercice 10 Formules de Newton et de Waring, [A. F.] p. 428-430, [Fr. F] exercice 4.4.13 p. 207, voir aussi [F. M. 1] remarque 4. 3. 5 p 329.

Dans l'exercice A désigne un anneau commutatif. Soit $S(T):=\sum_{k\geq 0}s_kT^k\in A[[T]]$. la série $D(S)(T):=\sum_{k\geq 1}ks_kT^{k-1}\in A[[T]]$ s'appelle la dérivée de $S(T)$.

(1) (a) Soit $S(T):=\sum_{k\geq 0}T^k\in A[[T]]$. Montrer que $(1-T)S(T)=1$.

Preuve. On développe $(1-T)S(T)=S(T)-TS(T)=1$. ///

(b) Soient $U(T),V(T)\in A[[T]]$. Montrer que $D(U(T)V(T))=U(T)D(V(T))+V(T)D(U(T))$.

Preuve. Si $U(T)=\sum_m u_mT^m$ *et* $V(T)=\sum_n v_nT^n$ *on a* $U(T)D(V(T))+V(T)D(U(T))=\sum_k(\sum_{n+m-1=k}u$ $\sum_k(\sum_{n+m-1=k}mu_mv_n)T^k=\sum_k(\sum_{n+m-1=k}(n+m)u_mv_n)T^k=D(U(T)V(T))$. ///

(c) Soit $U(T)\in TA[[T]]$. Montrer que $D(S(U(T)))=D(U)(T)[D(S)(U(T))]$ (traiter d'abord le cas où $S(T)=T^m$).

Preuve. Si $S(T)=T^m$ *alors* $S(U(T))=U(T)^m$ *et on vérifie la formule par récurrence sur* m *avec la formule précédente. Dans le cas général* $S(T)=\sum_m s_mT^m$ *et on doit montrer que* $D(S(U(T)))=D(\sum_m s_mD(U(T)^m))$. *Cette égalité est satifaite* $\forall k>0$ *modulo l'idéal* $T^kA[[T]]$ *parce que* $D(U(T)^m))\in T^{m-1}A[[T]]$ *et que l'égalité se déduit de celle pour* $S=\sum_{0\leq m<k}s_mT^m$ *(i.e.* $s_m=0$ *pour* $m\geq k$*) et qui vient de la linéarité de* D. ///

(d) On suppose que $\mathbb{Q}\subset A$. On définit la série formelle "logarithme" par $L(T):=\sum_{k\geq 1}(-1)^{k-1}\frac{T^k}{k}\in A[[T]]$. Soient $U(T),V(T)\in TA[[T]]$. En utilisant la dérivation montrer que $L((1+U(T))(1+V(T))-1)=L(U(T))+L(V(T))$.

Preuve. Puisque $D(L)(T)=\sum_{k\geq 1}(-1)^{k-1}T^{k-1}=(1+T)^{-1}$ *il suit de la question précédente que* $D(L(U(T))=D(U(T))(1+U(T))^{-1}$ *et* $D(L((1+U(T))(1+V(T))-1))=D((1+U(T))(1+V(T))-1)((1+U(T))^{-1}(1+V(T))^{-1})=D(L(U(T))+D(L(V(T))$. *Ainsi* $D[L((1+U(T))(1+V(T))-1)-L(U(T))-L(V(T))=0$ *et puisque la caractéristique de* A *est nulle il suit que* $L((1+U(T))(1+V(T))-1)-L(U(T))-L(V(T))\in A\cap TA[[T]]=0$. ///

(2) Dans ce qui suit on note $A := \mathbb{Q}[X_1, ..., X_n]$. Pour $k \geq 0$ on note $p_k := \sum_{1\leq i\leq n} X_i^k$, ainsi $p_0 = n$. On note $P(Z) := \prod_{1\leq i\leq n}(Z - X_i) = Z^n - s_1 Z^{n-1} + ... + (-1)^i s_i Z^{n-i} + .. + (-1)^n s_n$ et $Q(T) := \prod_{1\leq i\leq n}(1 - X_i T) = 1 - s_1 T + ... + (-1)^i s_i T^i + .. + (-1)^n s_n T^n$.

(a) *Formules de Newton*

(i) Soit $F(T) := \sum_{k\geq 0} p_k T^k \in A[[T]]$. Montrer que $F(T) = \sum_{1\leq i\leq n} \frac{1}{1-X_i T}$.
Preuve. C'est une conséquence immédiate de la question 1. ///

(ii) En déduire que

$$(1 - s_1 T + ... + (-1)^i s_i T^i + .. + (-1)^n s_n T^n) F(T) =$$
$$= n - (n-1)s_1 T + (n-2)s_2 T^2 + ... + (-1)^{n-1} s_{n-1} T^{n-1}.$$

Preuve. Cette formule exprime l'égalité $F(T)Q(T) = nQ - TD(Q(T))$ qui résulte du calcul de la dérivé logarithmique de $Q(T)$. ///

(iii) En déduire que $p_0 = n$, $p_1 = s_1$, $p_2 = s_1 p_1 - 2s_2$, ...,$p_i = s_1 p_{i-1} - s_2 p_{i-2} + ... + (-1)^{i-2} s_{i-1} p_1 + (-1)^{i-1} i s_i$ pour $i \leq n$ et $p_i = s_1 p_{i-1} - s_2 p_{i-2} + ... + (-1)^{n-1} s_n p_{i-n}$ pour $i > n$.
Preuve. On identifie $n - (n-1)s_1 T + (n-2)s_2 T^2 + ... + (-1)^{n-1} s_{n-1} T^{n-1}$ à $(1 - s_1 T + ... + (-1)^i s_i T^i + .. + (-1)^n s_n T^n)(\sum_{k\geq 0} p_k T^k)$. ///

(b) *Formules de Waring*

(i) En considérant la série $L(Q(T) - 1)$ montrer que pour $h \geq 1$

$$\frac{1}{h} p_h = (-1)^n \sum_{i_1 + 2i_2 + ... + n i_n = h} (-1)^{\sum i_k} \frac{(i_1 + i_2 + ... + i_n - 1)!}{i_1! i_2! ... i_n!} s_1^{i_1} s_2^{i_2} ... s_n^{i_n}$$

(on rappelle que $(Z_1 + Z_2 + .. + Z_n)^h = \sum_{i_1+i_2+...+i_n=h} \frac{h!}{i_1! i_2! ... i_n!} Z_1^{i_1} ... Z_n^{i_n}$) *Preuve. On a* $L(Q(T) - 1) = \sum_{1\leq i\leq n} L(-X_i T) = -\sum_{1\leq i\leq n} \sum_{h\geq 1} \frac{X_i^h T^h}{h} = -\sum_{h\geq 1} \frac{1}{h} p_h T^h = -\sum_{h\geq 1} \frac{1}{h}(-s_1 T + ... + (-1)^i s_i T^i + .. + (-1)^n s_n T^n)^h$. ///

(ii) On considère la suite $(u_n)_{n\in\mathbb{N}}$ définie par $u_0 = 3$, $u_1 = 0$, $u_2 = 2$ et pour $n \geq 0$ par $u_{n+3} = u_n + u_{n+1}$. On pose $Q_0(T) := 1 - T^2 - T^3 = (1 - x_1 T)(1 - x_2 T)(1 - x_3 T)$ avec $x_i \in \mathbb{C}$. Montrer que $\forall k \in \mathbb{N}$, $u_k = x_1^k + x_2^k + x_3^k = p_k(x_1, x_2, x_3) \in \mathbb{Z}$ et que pour tout nombre premier ℓ on a $u_\ell \equiv 0 \mod \ell$.
Preuve. Les formules de Newton donnent pour $i > 3$, $p_i = s_1 p_{i-1} - s_2 p_{i-2} + s_3 p_{i-3}$ (notez que cette formule est immédiate : il suffit de remarquer que $Z^{i-3} P(Z) = Z^i - s_1 Z^{i-1} + s_2 Z^{i-2} - s_3 Z^{i-3}$ et donc $0 = X_1^{i-3} P(X_1) + X_2^{i-3} P(X_2) + X_3^{i-3} P(X_3) = p_i - s_1 p_{i-1} + s_2 p_{i-2} - s_3 p_{i-3}$. Et puisque $s_1 = 0, s_2 = -1, s_3 = 1$ il suit que $p_i = p_{i-2} + p_{i-3}$ si $i > 3$. Ainsi pour vérifier l'égalité $u_k = p_k(x_1, x_2, x_3)$ il suffit de la vérifier aux rangs $0, 1, 2$. Or $L(Q_0(T)) = L(-T^2 - T^3) = -T^2 - T^3 \mod T^4 = -p_1 T - \frac{p_2}{2} T^2 \mod T^3$ ainsi $p_0 = 3 = u_0$, $p_1 = 0 = u_1$ et $p_2 = 2 = u_2$. La récurrence montre aussi que $u_k \in \mathbb{Z}$. Enfin la congruence suit du développement de $L(-T^2 - T^3)$ qui redonne la formule de Waring : puisque $s_1 = 0$ on a $\frac{1}{\ell} p_\ell = \sum_{2i_2+3i_3=\ell} (-1)^{i_2+i_3} \frac{(i_2+i_3-1)!}{i_2! i_3!} s_2^{i_2} s_3^{i_3} = \sum_{2i_2+3i_3=\ell} (-1)^{i_3} \frac{1}{i_2+i_3} \binom{i_2+i_3}{i_3}$. Ainsi $v_\ell(p_\ell) \geq 1$. Voir [FM] p. 328, remarques 4.3.4 et 4.3.5. pour une autre preuve moins calculatoire. //

(iii) Montrer que $Q(T) = \prod_{1\leq h\leq n} E(\frac{-1}{h} p_h T^h) \mod T^{n+1}$ où $E(T) = \sum_{k\geq 0} \frac{1}{k!} T^k$ est la série formelle "exponentielle".
Preuve. On montre que $H(T) := E(L(T)) = 1 + T$. Pour cela on calcule $D(H(T))) = D(L(T))E(L(T)) = (1 + T)^{-1} H(T)$. Ainsi $(1 + T)D(H(T))) = H(T)$. On écrit $H(T) = \sum_k h_k T^k$ et on traduit l'égalité précédente. Ainsi $Q(T) = E(L(Q(T) - 1)) = E(-\sum_{h\geq 1} \frac{1}{h} p_h T^h) = \prod_{1\leq h\leq n} E(\frac{-1}{h} p_h T^h \mod T^{n+1}$.
Notez qu'en développant modulo T^{n+1} on obtient les formules exprimant s_i dans $\mathbb{Q}[p_1, ..., p_n]$, [A. F.] p. 430. ///

Exercice 11 Racines de l'unité.

Déterminer les n-uplets $(z_1, z_2, ..., z_n)$ de n nombres complexes non nuls avec $\sum_{1\leq i\leq n} z_i^k = 0$ pour $k = 1, 2, ..., n-1$.

Exercice 12 Somme des racines primitives n-ièmes de l'unité, [F. M. 2] question 2. du théorème p.249

Montrer que $S(n) := \sum_{1\leq k\leq n,\ (n,k)=1} e^{2i\pi\frac{k}{n}} = \mu(n)$ où $\mu(.)$ est la fonction de Mobius. En déduire que $\Phi_n(X) = X^{\varphi(n)} - \mu(n)X^{\varphi(n-1)} + ...$

Preuve : Une propriété caractéristique de la fonction de Möbius est que $\sum_{d|n}\mu(d) = 0$ pour $n > 1$ et $\mu(1) = 1$. D'autre part puisque la somme des racine n-ièmes de l'unité pour $n > 1$ est nulle, il suit que pour $n > 1$ on a $\sum_{d|n} S(d) = 0$ et puisque $S(1) = 1$, l'égalité suit par récurrence sur n.

Exercice 13 Un complément à l'exercice précédent. Sommes de Newton relatives aux racines du polynôme cyclotomique, [F. M. 2'] complément à la page 249.

Soit $n > 0$ un entier. On note U_n le sous-groupe de $\mathbb{C}^\times$ des racines n-ièmes de l'unité et U'_n le sous-ensemble des racines primitives n-ièmes de l'unité. Par définition le n-ième polynôme cyclotomique est $\Phi_n := \prod_{z\in U'_n}(X - z)$.

Soit $h \in \mathbb{N}$, la h-ième somme de Newton relative à Φ_n est $p_h(n) := \sum_{z\in U'_n} z^h$. Dans la littérature on les appelle sommes de Ramanujan.

(1) Montrer que si $(n, m) = 1$, alors l'application $f :\ (z, z') \in U_n \times U_m \to zz' \in U_{nm}$ est un isomorphisme de groupes. Il suit que f induit une bijection entre $U'_n \times U'_m$ et U'_{nm}.
Preuve. L'application f est clairement un homomorphisme de groupes. Si $f((z, z')) = 1$ avec $(z, z') \in U_n \times U_m$, alors $z = z'^{-1}$ et si $un + vm = 1$ est une relation de Bézout on a donc $z = z^{un+vm} = 1$. Ensuite on remarque que $|U'_n| = \varphi(n)$ et donc $|U'_n \times U'_m| = |U'_{nm}|$.

(2) En déduire que pour h fixé, la fonction $n \in \mathbb{N}^\star \to p_h(n)$ est une fonction arithmétique multiplicative i.e. si $(n, m) = 1$, alors $p_h(nm) = p_h(n)p_h(m)$.
Preuve. On a $p_h(n)p_h(m) = (\sum_{z\in U'_n} z^h)(\sum_{z'\in U'_m} z'^h) = \sum_{(z,z')\in U'_n\times U'_m} z^h z'^h = p_h(nm)$.

(3) Plus généralement montrer que $p_h(n) = \sum_{d|(n,h)} d\mu(n/d)$.
Preuve. On remarque que $\sum_{d|n}\sum_{z\in U'_d} z^h = \sum_{z\in U_n} z^h = 0$ si $n \nmid h$ et n si $n \mid h$. Ainsi la formule est conséquence de la formule d'inversion de Möbius.

(4) Une autre formule.
Déduire de 2) et 3) que $p_h(n) = \frac{\mu(\frac{n}{(n,h)})\varphi(n)}{\varphi(\frac{n}{(n,h)})}$.
Preuve. Puisque $n \to p_h(n)$ et $n \to \frac{\mu(\frac{n}{(n,h)})\varphi(n)}{\varphi(\frac{n}{(n,h)})}$ sont des fonctions arithmétiques multiplicatives (à priori à valeurs dans $\mathbb{Q}$), il suffit de vérifier l'égalité pour $n = p^k$ où p est un nombre premier et $k \in \mathbb{N}$. On a $p_h(p^k) = \sum_{z\in U_{p^k}} z^h - \sum_{z\in U_{p^{k-1}}} = 0$ si $p^{k-1} \nmid h$, $-p^{k-1}$ si $p^{k-1}\|h$ et $p^k - p^{k-1}$ si $p^k|h$. On vérifie facilement que ces formules sont aussi vérifiées par la fonction arithmétique multiplicative $n \to \frac{\mu(\frac{n}{(n,h)})\varphi(n)}{\varphi(\frac{n}{(n,h)})}$.

Exercice 14 Les entiers algébriques, [Fr. F] exercice 4.4.4 p. 202. Cette preuve utilise les polynômes symétriques. On peut aussi utiliser le résultant ou bien le théorème de Cayley-Hamilton, [F. M. 2] théorème 2 p. 169.

Exercice 15 Étude de la suite $u_0 = 3, u_1 = 0, u_2 = 2$ et $u_{n+3} = u_n + u_{n+1}$. Pour tout nombre premier p on a $u_p = 0 \mod p$, [F. M. 1] remarque 4.3.4 et 4.3.5 p. 329.

(1) Soit A un anneau commutatif et $S(T) := \sum_{k\geq 0} T^k \in A[[T]]$. Montrer que $(1-T)S(T) = 1$.

(2) Dans ce qui suit on note $A := \mathbb{Z}[X_1, ..., X_n]$. Pour $k \geq 0$ on note $p_k := \sum_{1\leq i\leq n} X_i^k$. On note $P(Z) := \prod_{1\leq i\leq n}(Z - X_i) = Z^n - s_1 Z^{n-1} + ... + (-1)^i s_i Z^{n-i} + .. + (-1)^n s_n$.

(a) Soit $F(T) := \sum_{k\geq 0} p_k T^k \in A[[T]]$. Montrer que $F(T) = \sum_{1\leq i\leq n} \frac{1}{1-X_i T}$.

(b) En déduire que
$$(1 - s_1 T + ... + (-1)^i s_i T^i + .. + (-1)^n s_n T^n) F(T) =$$
$$= n - (n-1)s_1 T + (n-2)s_2 T^2 + ... + (-1)^{n-1} s_{n-1} T^{n-1}.$$

(c) En déduire que $p_0 = n$, $p_1 = s_1$, $p_2 = s_1 p_1 - 2s_2$, ...,$p_i = s_1 p_{i-1} - s_2 p_{i-2} + ... + (-1)^{i-2} s_{i-1} p_1 + (-1)^{i-1} i s_i$ pour $i \leq n$ et $p_i = s_1 p_{i-1} - s_2 p_{i-2} + ... + (-1)^{n-1} s_n p_{i-n}$ pour $i > n$.

(d) On considère la suite $(u_n)_{n\in\mathbb{N}}$ définie par $u_0 = 3$, $u_1 = 0$, $u_2 = 14$ et pour $n \geq 0$ par $u_{n+3} = -6u_n + 7u_{n+1}$. On pose $P(Z) := Z^3 - 7Z + 6 = (Z-1)(Z-2)(Z+3)$. Montrer que $u_k = p_k(1, 2, -3)$ et en déduire que pour tout nombre premier q et tout entier $k > 0$ on a $u_{kq} = u_k \mod q$.

(e) Soit q un nombre premier. Montrer que $p_{kq} - {p_k}^q \in qA$ pour tout $k \in \mathbb{N}$.

(f) En déduire que $p_{kq} - {p_k}^q \in q\mathbb{Z}[s_1, s_2, ..., s_n]$

(g) On considère la suite $(u_n)_{n\in\mathbb{N}}$ définie par $u_0 = 3$, $u_1 = 0$, $u_2 = 2$ et pour $n \geq 0$ par $u_{n+3} = u_n + u_{n+1}$. On pose $P(Z) := Z^3 - Z - 1 = (Z - x_1)(Z - x_2)(Z - x_3)$, montrer que $u_k = p_k(x_1, x_2, x_3)$ et en déduire que pour tout nombre premier q et tout entier $k > 0$ on a $u_{kq} = u_k \mod q$.