Lycée Louis-Le-Grand, Paris
MPSI 4 – Mathématiques
A. Troesch

Pour le 04/04/2019

DM n° 16 : Polynômes

Correction du problème 1 – Théorème de d'Alembert-Gauss

Partie I – Démonstration analytique

1. On a, d'après l'inégalité triangulaire :
$$|P(z)| > |a_n||z|^n - |a_{n-1}||z|^{n-1} - \cdots - |a_0|.$$
Cette minoration nous ramène à la recherche d'une limite en $+\infty$ d'une fonction polynomiale en la variable réelle $|z|$. Le coefficient dominant $|a_n|$ étant strictement positif, et $n > 0$ (le polynôme est non constant),
$$\lim_{|z|\to+\infty} |a_n||z|^n - |a_{n-1}||z|^{n-1} - \cdots - |a_0|,$$
et le théorème de minoration amène : $\boxed{\lim_{|z|\to+\infty} |P(z)| = +\infty}$.
Soit donc M tel que pour tout $z \in \mathbb{C}$, $|z| \geqslant M \Longrightarrow |P(z)| > |P(0)|$ (notez qu'on impose l'inégalité large $|z| \geqslant M$, ce qui est un peu plus fort que ce que demande l'énoncé).
2. Soit $(z_n)_{n\in\mathbb{N}}$ une suite d'éléments de $\overline{B}(0, M)$. Par procédé diagonal, on peut en extraire une suite (z_{φ_n}) convergeante. Plus précisément, on extrait d'abord une suite telle que la partie réelle converge (possible car la partie réelle est bornée), puis on extrait de cette suite une nouvelle suite assurant cette fois la convergence de la partie imaginaire.
On a alors, pour tout $n \in \mathbb{N}$, $z_{\varphi(n)} \in \overline{B}(0, M)$, donc $|z_{\varphi(n)}| \leqslant M$, et par passage à la limite, le module étant continu :
$$\lim_{n\to+\infty} z_{\varphi(n)} \leqslant M.$$
Ainsi, on a pu extraire de (z_n) une suite convergeant dans $\overline{B}(0, M)$. On en déduit que $\boxed{\overline{B}(0, M) \text{ est compact.}}$
3. Par théorème de compacité, la fonction $z \mapsto |P(z)|$ étant continue sur le compact $\overline{B}(0, M)$, $\boxed{\text{elle admet un maximum}}$ sur cet ensemble. On note z_0 un point en lequel ce maximum est atteint.
4. On a $b_0 = Q(0) = P(z_0)$. Par hypothèse, $P(z_0) \neq 0$, donc $\boxed{b_0 \neq 0}$.
5. On a :
$$|f(t)| = \left|1 + \frac{b_\ell}{b_0}c^\ell t^\ell + \sum_{k=\ell+1}^{n} b_k c^k t^k\right| = \left|1 - t^\ell + \sum_{k=\ell+1}^{n} b_k c^k t^k\right| \leqslant |1 - t^\ell| + \left|\sum_{k=\ell+1}^{n} b_k c^k t^k\right|.$$
Pour tout $t \in]0, 1[$, on a alors :
$$|f(t)| \leqslant 1 - t^\ell + \left|\sum_{k=\ell+1}^{n} b_k c^k t^k\right|.$$
Or, $\left|\sum_{k=\ell+1}^{n} b_k c^k t^k\right| = o(t^\ell)$, donc il existe $\eta > 0$ tel que pour tout $t \in]0, \eta[$,
$$\left|\sum_{k=\ell+1}^{n} b_k c^k t^k\right| \leqslant \frac{t^\ell}{2}.$$
On en déduit que pour tout $t \in]0, \eta[$
$$|f(t)| \leqslant 1 - t^\ell + \frac{t^\ell}{2} = 1 - \frac{t^\ell}{2} \qquad \text{donc:} \qquad \boxed{|f(t)| < 1}.$$

6. Il est alors possible de trouver des réels t au voisinage de 0^+ tels que $|Q(tc)| < |b_0|$, donc tels que $|P(z_0+tc)| < |b_0| = |P(z_0)|$.

   Cependant, si z_0 est sur le bord du disque $\overline{B}(0,M)$, cela ne permet pas de conclure immédiatement. Mais cette situation est rendue impossible par l'inégalité $|P(z)| > |P(O)| \geqslant |P(z_0)|$ pour tout $z \geqslant M$. Ainsi, $z_0 \in B(0,M)$, et pour tout t suffisamment petit $z_0+tc \in B(0,M)$. L'inégalité $|P(z_0+tc)| < |P(z_0)|$ contredit alors la définition de z_0.

   Ainsi, $P(z_0) = 0$, et on a bien trouvé une racine du polynôme P, ce qui prouve le théorème de d'Alembert-Gauss.

Partie II – Corps de décomposition d'un polynôme

1. Comme (Q) est un sous-groupe du groupe abélien $\mathbb{K}[X]$, la loi + passe au quotient, et définit sur $(\mathbb{K}_1, +)$ une structure de groupe.

   Par ailleurs, la multiplication passe aussi au quotient (c'est un fait général lorsqu'on qootiente un anneau commutatif par un idéal) : si a et a' sont dans la même classe modulo (Q), ainsi que b et b', on a alors $a - a' \in (Q)$, et $b - b' \in (Q)$. Ainsi, il existe R et S tels que

   $$a' = a + RQ \qquad \text{et} \qquad b' = b + SQ.$$

   En effectant le produit, on obtient sans peine que $ab - a'b' \in (Q)$, ce qui assure que le produit passe au quotient.

   La structure de monoïde commutatif, ainsi que la distributivité s'obtiennent alors facilement à partie de la structure initiale d'anneau sur $\mathbb{K}[X]$. Ainsi, le quotient $\mathbb{K}_1$ est également muni d'une structure d'anneau. Il reste à prouver que $\mathbb{K}_1$ est muni d'une structure de corps. Pour cela, on montre l'inversibilité de tous les éléments non nuls de $\mathbb{K}_1$.

   Soit $x \in \mathbb{K}_1$, non nul, et P un représentant de x dans $\mathbb{K}[X]$. Comme $x \neq 0$, P n'est pas dans (Q). Comme Q est irréductible, on en déduit que $P \wedge Q = 1$, et par conséquent, d'après le théorème de Bézout, il existe U et V des polynômes tels que $UP + VQ = 1$. L'image dans $\mathbb{K}_1$ donne alors $xy = 1$, où y est la projection canonique de U dans $\mathbb{K}_1$. Ainsi, x est inversible.

   On en déduit que $\mathbb{K}_1$ est un corps.

2. Le fait que φ soit un morphisme d'anneau provient du respect de la structure (le fait que les opérations soient une congruence modulo Q, ce qui est la propriété qui nous a permis de définir les lois quotients)

   La restrition de φ à $\mathbb{K}$ est donc un morphisme d'anneau, du corps $\mathbb{K}$ sur le corps $\mathbb{K}_1$, c'est donc par définition un morphisme de corps. Or, un morphisme de corps est toujours injectif.

   Ainsi, la restriction de φ à $\mathbb{K}$ est injective. est injective.

   On peut donc identifier $\mathbb{K}$ à son image $\Phi(\mathbb{K}) \subset \mathbb{K}_1$. Via cette identification, on considérera désormais que $\mathbb{K} \subset \mathbb{K}_1$.

3. On note $P = QR$. On a alors :

   $$P(\theta) = \varphi(P(X)) = \varphi(Q(X)R(X)) = \varphi(Q(X))\varphi(R(X)) = 0,$$

   puisque par définition, $\varphi(Q) = 0$. Ainsi, $\theta \in \mathbb{K}_1$ est une racine de P.

4. On montre par récurrence sur le degré $n \geqslant 1$ de P, que pour tout polynôme P de degré n, sur un corps $\mathbb{K}$, il existe un corps $\mathbb{K}_2$ contenant $\mathbb{K}$ tel que P soit scindé dans $\mathbb{K}_2$.

   La propriété est triviale si $n = 1$. Supposons $n > 1$, et supposons la propriété vraie pour tout polynôme de degré strictement inférieur à n, sur tout corps $\mathbb{K}'$.

   On commence par trouver $\mathbb{K}_1$ tel que P admette une racine dans $\mathbb{K}_1$ (question précédente), et on factorise dans $\mathbb{K}_1$: $P = (X - \theta)\tilde{P}$. Le polynôme $\tilde{P}$ étant de degré $n-1$, à coefficients dans $\mathbb{K}_1$ contenant $\mathbb{K}$, il existe, par hypothèse de récurrence, un corps $\mathbb{K}_2$ contenant $\mathbb{K}_1$ donc aussi $\mathbb{K}$, tel que $\tilde{P}$ soit scindé sur $\mathbb{K}_2$. Alors P aussi est scindé sur $\mathbb{K}_2$.

   Par principe de récurrence, pour tout polynôme P non constant, il existe un corps $\mathbb{K}_2$ dans lequel P est scindé.

5. Il suffit de prendre l'intersection de tous les sous-corps de $\mathbb{K}_2$ contenant $\mathbb{K}$ et dans lequel P est scindé. Il y en a au moins 1, et leur intersection est encore un corps. C'est clairement le plus petit des sous-corps vérifiant les propriétés requises.

Partie III – Polynômes symétriques

1. S est un sous-ensemble de $\mathbb{K}[X_1,\dots,X_n]$, contenant 0, et stable par différence et produit puisque : pour tout P, Q de S et tout σ de $\mathfrak{S}_n$, on a :

$$\begin{aligned}(P-Q)(X_{\sigma(1)},\dots,X_{\sigma(n)}) &= P(X_{\sigma(1)},\dots,X_{\sigma(n)}) - Q(X_{\sigma(1)},\dots,X_{\sigma(n)})\\ &= P(X_1,\dots,X_n) - Q(X_1,\dots,X_n) = (P-Q)(X_1,\dots,X_n),\end{aligned}$$

et de même pour la multiplication. Ainsi, $\boxed{S \text{ est un sous-anneau de } \mathbb{K}[X_1,\dots,X_n]}$.

2. Soit P un polynôme symétrique, et $aX_1^{\alpha_1}\dots X_n^{\alpha_n}$ son monôme directeur. Si on n'a pas $\alpha_1 \geqslant \alpha_2 \geqslant \dots \geqslant \alpha_n$, il existe une permutation σ telle que pour l'ordre lexicographique

$$(\alpha_1,\alpha_2,\dots,\alpha_n) < (\sigma(\alpha_1),\sigma(\alpha_2),\dots,\sigma(\alpha_n))$$

(il suffit d'échanger deux termes consécutifs α_i et α_{i+1} tels que $\alpha_i < \alpha_{i+1}$). Or, P étant symétrique, le monôme $aX_{\sigma^{-1}(1)}^{\alpha_1}\cdots X_{\sigma^{-1}(n)}^{\alpha_n}$ égal à $aX_1^{\sigma(\alpha_1)}\cdots X_n^{\sigma(\alpha_n)}$, est aussi un monôme de P, ce qui contredit la maximalité de $(\alpha_1,\dots,\alpha_n)$ pour l'ordre lexicographique.
Ainsi, on a bien $\boxed{\alpha_1 \geqslant \alpha_2 \geqslant \dots \geqslant \alpha_n}$.

3. Ce résultat découle de façon immédiate du respect de l'ordre lexicographique par la somme : soit $X = (x_1,\dots,x_n)$, $Y = (y_1,\dots,y_n)$, $Z = (z_1,\dots z_n)$ et $T = (t_1,\dots,t_n)$ tels que, pour l'ordre lexicographique, $X \leqslant Z$ et $Y \leqslant T$. Alors $X+Z \leqslant Y+T$, et de plus, si l'une des deux inégalités initiales est strite, l'inégalité finale aussi. Démontrons cela :
   - Supposons $X \leqslant Y$ et $Z \leqslant T$. Si les deux inégalités sont des égalités, il n'y a rien à démontrer.
   - Si $X < Y$ et $Z \leqslant T$ (ou l'inverse), il existe k tel que $x_1 = y_1,\dots,x_{k-1} = y_{k-1}$ et $x_k < y_k$. Quitte à échanger le rôle de (X,Y) et (Z,T), on peut supposer que pour tout $i \in [\![1,k-1]\!]$, $z_i = t_i$ et $z_{k+1} \leqslant t_{k+1}$. On a alors aussi :

$$x_1+z_1 = y_1+t_1,\dots,x_{k-1}+z_{k-1} = y_{k-1}+t_{k-1} \qquad \text{et} \qquad x_k+z_k < y_k+t_k.$$

   Ainsi, $X+Y < Z+T$.

Cela démontre bien notre assertion sur l'ordre lexicographique.

Or, les monômes de PQ sont obtenus en faisant le produit des monômes de P et des monômes de Q. Notons A et B les suites des exposants des monômes directeurs respectivement de P et de Q. Alors pour tout monôme M_1 de P, de suite d'exposants C et tout monôme M_2 de Q, de suite d'exposants D, on a $C \leqslant A$ et $D \leqslant B$, par définition, et les exposants de M_1M_2 sont $C+D \leqslant A+B$, l'inégalité étant stricte, sauf lorsque $C = A$ et $D = B$, c'est à dire lorsque $M_1 = \mathrm{MD}(P)$ et $M_2 = \mathrm{MD}(Q)$.

Ainsi, les produits des monômes sont tous d'exposant strictement inférieur à $A+B$, sauf le produit des monômes directeurs. Ainsi, le monôme directeur de PQ est égal à ce produit des monômes directeurs, c'est-à-dire :

$$\boxed{\mathrm{MD}(PQ) = \mathrm{MD}(P)\mathrm{MD}(Q)}.$$

4. La question précédente nous permet d'affirmer que

$$\mathrm{MD}(\Sigma_1^{\alpha_1-\alpha_2}\cdots\Sigma_{n-1}^{\alpha_{n-1}-\alpha_n}\Sigma_n^{\alpha_n}) = \mathrm{MD}(\Sigma_1)^{\alpha_1-\alpha_2}\cdots\mathrm{MD}(\Sigma_{n-1})^{\alpha_{n-1}-\alpha_n}\mathrm{MD}(\Sigma_n)^{\alpha_n}.$$

Or, la description de Σ_k amène trivialement

$$\mathrm{MD}(\Sigma_k) = X_1X_2\dots X_k.$$

Ainsi,

$$\mathrm{MD}(\Sigma_1^{\alpha_1-\alpha_2}\cdots\Sigma_{n-1}^{\alpha_{n-1}-\alpha_n}\Sigma_n^{\alpha_n}) = \prod_{k=1}^{n}(X_1\dots X_k)^{\alpha_k-a_{k+1}},$$

en ayant posé $\alpha_{n+1} = 0$. Ainsi :

$$\mathrm{MD}(\Sigma_1^{\alpha_1-\alpha_2}\cdots\Sigma_{n-1}^{\alpha_{n-1}-\alpha_n}\Sigma_n^{\alpha_n}) = \prod_{i=1}^{n}X_i^{(\alpha_i-\alpha_{i+1})+\dots+(\alpha_n-\alpha_{n+1})} = \prod_{i=1}^{n}X_i^{\alpha_i}.$$

On obtient bien la relation voulue :

$$\boxed{\mathrm{MD}(\Sigma_1^{\alpha_1-\alpha_2}\cdots\Sigma_{n-1}^{\alpha_{n-1}-\alpha_n}\Sigma_n^{\alpha_n}) = X_1^{\alpha_1}\cdots X_n^{\alpha_n}}.$$

5. La récurrence paraît immédiate : on initialise pour $(\alpha_0, \dots, \alpha_n) = 1$, en remarquant que $1 = \Sigma_0$ (somme d'un unique terme, constitué d'un produit vide, donc égal à 1). On baisse ensuite le degré du monôme directeur dans l'ordre lexicographique en considérant $P - \Sigma_1^{\alpha_1-\alpha_2} \cdots \Sigma_{n-1}^{\alpha_{n-1}-\alpha_n} \Sigma_n^{\alpha_n}$. Ceci nous permet de montrer l'argument par récurrence. Mais qu'est-ce qui valide cette récurrence sur un ensemble, certes muni d'un ordre total, mais non isomorphe à $\mathbb{N}$?

   C'est en fait un principe de descente infinie : étant donné $A \in \mathbb{N}^n$, il n'existe pas de chaîne infinie

$$A_0 = A > A_1 > A_2 > \cdots > A_m > \cdots .$$

   En effet, en supposant le contraire, et en notant pour tout $m \in \mathbb{N}$,

$$A_m = (a_{m,1}, \dots, a_{m,n}),$$

   la propriété fondamentale de $\mathbb{N}$ assure l'existence de N_1 tel que $a_{N_1,1} = \min_m(a_{m,1})$. La décroissance de la suite (A_m) assure qu'alors pour tout $m \geqslant N_1$, $a_{m,1} = a_{N_1,1}$. On peut alors constuire $N_2 > N_1$ tel que

$$a_{N_2,2} = \min_{m>N_1}(a_{m,2}),$$

   et pour les mêmes raisons, pour tout $m \geqslant N_2$, $a_{m,2} = a_{N_2,2}$. On continue de la sorte en construisant $N_3, \dots, N_n$ de façon similaire. On a alors, pour tout $m \geqslant N$,

$$a_{m,1} = a_{N_1,1}, \qquad a_{m,2} = a_{N_2,2}, \qquad \dots \qquad a_{m,n} = a_{N_n,n},$$

   donc la suite (A_n) est strationnaire, ce qui contredit sa stricte décroissance.

   Ainsi, il n'existe pas de chaîne majorée strictement décoissante infinie. Le principe de descente infinie nous assure alors la validité du raisonnement par récurrence ci-dessus.

   Remarquez qu'en revanche, la plupart des éléments admettent une infinité de minorants. N'est-ce pas contradictoire ?

Partie IV – Les polynômes de degré impair > 1 ne sont pas irréductibles dans $\mathbb{C}[X]$

1. Comme P est de degré impair, ses limites en $-\infty$ et $+\infty$ sont infinies de signe opposé. Ainsi, P étant continu, le théorème des valeurs intermédiaires permet de conclure à l'existence d'une racine réelle de P.
2. Comme P est de degré impair strictement plus grand que 1, la question précédente permet d'affirmer que P ne peut pas être à coefficients réels (l'existence d'une racine contredirait l'irréductibilité). Ainsi, $P \notin \mathbb{R}[X]$.

   Pour tout $x \in \mathbb{R}$, on a $Q(x) = P(x)\overline{P(x)} = |P(x)|^2$. Par caractérisation des éléments de $\mathbb{R}[X]$ parmi les éléments de $\mathbb{C}[X]$, on en déduit que $Q \in \mathbb{R}[X]$.
3. Le polynôme P est irréductible dans $\mathbb{C}[X]$, donc aussi $\overline{P}$ (car R divise P si et seulement si $\overline{R}$ divise $\overline{P}$).

   Ainsi, $Q = P\overline{P}$ est la décomposition irréductible dans $\mathbb{C}[X]$ de Q. On en déduit que les seuls diviseurs dans $\mathbb{C}[X]$ de Q sont, à constante multiplicative près, 1, P, $\overline{P}$ et Q.

   Comme P et $\overline{P}$ ne sont pas dans $\mathbb{R}[X]$, les seuls diviseurs de Q dans $\mathbb{R}[X]$ sont, à constante près, 1 et Q, ce qui signifie que Q est irréductible sur $\mathbb{R}$.
4. En développant l'expression de R, et en notant $T = \{(i,j) \in [\![1, 2n]\!]^2,\ i < j\}$, on obtient

$$R = \sum_{I \subset T} X^{|T|-|I|} \prod_{(i,j)\in I} (\alpha_i + \alpha_j) = \sum_{k=0}^{\frac{2n(2n-1)}{2}} X^k \left(\sum_{\substack{I \subset T \\ |I|=k}} \prod_{(i,j)\in I} (\alpha_i + \alpha_j) = k \right)$$

   Or, étant donné σ une permutation de $[\![1, 2n]\!]$, σ induit une bijection $\hat{\sigma}$ sur T, définie par :

$$\hat{\sigma} : (i,j) \mapsto (\sigma(i), \sigma(j)) \qquad \text{ou} \qquad (\sigma(j), \sigma(i)),$$

   suivant que $\sigma(i) < \sigma(j)$ ou l'inverse. Cette application est bien à valeurs dans T, et est une bijection, sa réciproque étant $\hat{\sigma^{-1}}$.

L'application $\hat{\sigma^{-1}}$ induit induit une bijection $\tilde{\sigma}$ de $\mathcal{P}_k(T)$ sur lui-même (application image directe). En effet, elle est bien définie (l'image directe par une bijection conserve le cardinal) et surjective (tout ensemble de cardinal n a une image réciproque de cardinal n aussi, et est l'image de son image réciproque, par surjectivité de $\hat{\sigma^{-1}}$), donc aussi injective par cardinalité.

Ainsi, en notant pour tout (i,j), $\alpha_{(i,j)} = \alpha_i + \alpha_j$, on a :

$$\sum_{\substack{I\subset T\\|I|=k}} \prod_{(i,j)\in I} (\alpha_{\sigma(i)} + \alpha_{\sigma(j)}) = \sum_{\substack{I\subset T\\|I|=k}} \prod_{(i,j)\in I} \alpha_{\hat{\sigma}(i,j)} = \sum_{\substack{I\subset T\\|I|=k}} \prod_{(i,j)\in \tilde{\sigma}(I)} \alpha_{(i,j)} = \sum_{\substack{I\subset T\\|I|=k}} \prod_{(i,j)\in I} (\alpha_{(i,j)},$$

la dernière égalité résultant du fait changement de variable bijectif $I' = \tilde{\sigma}(I)$.

Ainsi, les coefficients de R sont symétriques en les α_i (à coefficients réels), et d'après la partie III, ils peuvent s'exprimer à l'aide des polynômes symétriques élémentaires en les α_i, avec des coefficients réels. Or, les $\Sigma_k(\alpha_1, \cdots, \alpha_{2n})$ s'expriment à l'aide des coefficients réels de Q, d'après les formules de Viète, donc sont tous réels.

On en déduit que les coefficients de R sont réels, donc que $\boxed{R \in \mathbb{R}[X]}$.

5. Le degré de R est

$$\deg(R) = \frac{2n(2n-1)}{2} = n(2n-1).$$

Comme n est impair, on en déduit que R est de degré impair, et dans $\mathbb{R}[X]$.

La question IV-1 amène l'$\boxed{\text{existence d'une racine réelle } r \text{ de } R}$.

Soit alors

$$S = Q\left(X + \frac{r}{2}\right) \qquad \text{et} \qquad T = Q\left(-X + \frac{r}{2}\right).$$

Les polynômes S et T sont à coefficients réels, et le polynôme Q étant irréductible sur $\mathbb{R}$, il en est de même de S et de T (si A divise S, alors $A(X - \frac{r}{2})$ divise Q). Donc soit $S \wedge T = 1$, soit il existe λ tel que $S = \lambda T$. Or, le pgcd de S et T est le même dans $\mathbb{R}$ et dans $\mathbb{C}$; Ainsi, pour montrer que $S \wedge T \neq 1$, il suffit de montrer que S et T admettent une racine complexe commune.

Pour cela, on sait qu'il existe des indices i et j tels que $r = \alpha_i + \alpha_j$. On remarque alors qu'en posant $\alpha = \frac{\alpha_i - \alpha_j}{2}$, on a $\alpha + \frac{r}{2} = \alpha_i$ et $-\alpha + \frac{r}{2}$. Ainsi, puisque α_i et α_j sont racines de Q, α est racine commune de S et T.

On en déduit que $S \wedge T \neq 1$, dont il existe λ tel que $S = \lambda T$. Par ailleurs, les coefficients dominants de S et T diffèrent d'un facteur multiplicatif égal à $(-1)^{\deg(Q)} = (-1)^{2n} = 1$. Ainsi, $\boxed{S = T}$.

Or, il se trouve que $T = S(-X)$, donc S est pair, et ne s'écrit alors qu'avec des monômes de degré pair. Autrement dit, il existe $U \in \mathbb{R}[X]$ tel que $\boxed{S(X) = U(X^2)}$.

6. On a alors $\deg(U) = \frac{1}{2}\deg(S) = \frac{1}{2}\deg(Q) = n$. Comme n est imapair, et U à ceofficients réels, U admet une racine réelle s. Soit alors t une racine carrée (dans $\mathbb{C}$) de s, on a $S(t) = U(s) = 0$, donc $Q(s + \frac{r}{2}) = 0$. Ainsi, Q admet une racine dans $\mathbb{C}$, et par intégrité, soit P soit $\overline{P}$ admet une racine. Or, si v est racine de $\overline{P}$, $\overline{v}$ est racine de P. Dans les deux cas, on a donc obtenu l'existence d'une racine de P, ce qui contredit l'irréductibilité de P (qui avait été supposé de degré > 3).

Par conséquent, $\boxed{\text{les polynômes de } \mathbb{C}[X] \text{ de degré impair} > 3 \text{ ne sont pas irréductibles}}$.

Partie V – Preuve algébrique du théorème de d'Alembert-Gauss

1. - Le raisonnement est le même que plus haut : les coefficients de R sont symétriques en des α_i (et à coefficients réels, donc complexes), donc s'expriment comme combinaisons linéaires à coefficents complexes de produits de fonctions symétriques en des α_i, ces fonctions syémtriques en les α_i s'exrimant elles-même en fonction des coefficients de P, qui sont des complexes. Ainsi, $\boxed{\text{les coefficients de } R \text{ sont complexes}}$.
   Remarquez que ceci n'a rien d'évident, puisqu'on s'est autorisé l'utilisation d'un corps plus gros $\mathbb{K}$ pour décrire R, les racines α_i étant dans $\mathbb{K}$ mais pas nécessairement dans $\mathbb{C}$.
   - Soit $n = 2^k m$ le degré de P, m étant ici impair. Ainsi, k est la valuation 2-adique de n, supposée supérieure ou égal à 1 (le cas $k = 0$ ayant été traité dans la partie précédente). Le degré de R est alors

$$\deg(R) = \frac{2^k m(2^k m - 1)}{2} = 2^{k-1}(2^k m - 1).$$

On en déduit que la valuation 2-adique de R est égale à $k-1$.
Considérons maintenant la décomposition de R en produit de facteurs irréductibles :

$$R = Q_1 \cdots Q_\ell.$$

Si pour tout $i \in [\![1, \ell]\!]$, $\mathrm{val}_2(\deg(Q_i)) \geqslant k$, alors

$$\mathrm{val}_2(R) = \mathrm{val}_2(\deg(Q_1) + \cdots + \deg(Q_i)) \geqslant k.$$

Cela contredit ce qu'on a trouvé ci-dessus. Ainsi, il existe au moins un facteur irréductible Q de R tel que $\boxed{\mathrm{val}_2(Q) < k}$.

2. On montre, par récurrence sur $k \in \mathbb{N}$, que tout polynôme P de degré au moins 2 et tel que $\mathrm{val}_2(\deg(P)) = k$ admet une racine dans $\mathbb{C}$.
   - Le cas $k = 1$ est conséquence de la partie IV. Le cas d'un polynôme de degré 1 est immédiat.
   - Soit $k \in \mathbb{N}^*$, et supposons la propriété vérifiée pour tout polynôme Q tel que $\mathrm{val}_2(\deg(Q)) < k$. Soit P un polynôme tel que $\mathrm{val}_2(P) = k$. Comme pour la question précédente, P admet au moins un facteur irréductible $\tilde{P}$ tel que $\mathrm{val}_2(\tilde{P}) \leqslant k$. Si l'inégalité est stricte, on conclut directement par l'hypothèse de récurrence que $\tilde{P}$ (dont P) admet une racine dans $\mathbb{C}$. Sinon, toute racine de $\tilde{P}$ étant racine de P, on peut remplacer P par $\tilde{P}$ sans perte de généralité. Ainsi, on peut supposer que P est irréductible.
     Soit alors R comme plus haut, et et Q un facteur irréductible de R tel que $\boxed{\mathrm{val}_2(Q) < k}$. On peut appliquer l'hypothèse de récurrence à Q, n'étant pas constant. Ainsi, Q admet une racine r dans $\mathbb{C}$. On considère

$$S = P\left(X + \frac{r}{2}\right) \qquad \text{et} \qquad T = P\left(-X + \frac{r}{2}\right).$$

     Comme P est de degré pair, S et T ont même coefficient dominant. Puisque P est irréductible sur $\mathbb{C}$, S et T le sont aussi, et comme dans la partie IV, on peut trouver une racine commune de S et T dans $\mathbb{K}$, qui empêche que S et T soient premier enter eux (sur $\mathbb{K}$ donc aussi sur $\mathbb{C}$). Étant irréductibles de même coefficient dominant, il vient : $S = T$, d'où la parité de S. On a à nouveau la possibilité d'écrire $S(X) = U(X^2)$, où $\deg(U) = frac12\deg(Q)$. Ainsi,

$$\mathrm{val}_2(\deg(U)) = k - 1.$$

     On peut utiliser une deuxième fois l'hypothèse de récurrence sur U, nous assurant l'existence d'un complexe s tel que $U(s) = 0$. Si t est une racine carré de s, on a alors $S(t) = 0$, ce qui fournit ensuite une racine complexe de P.
   - Ainsi, d'après le principe de récurrence $\boxed{\text{tout polynôme non constant de } \mathbb{C}[X] \text{ admet une racine dans } \mathbb{C}}$.