DM n° 17 : Polynômes

Ce devoir est à m'envoyer scanné au format pdf, par mail, avec les consignes suivantes à respecter scupuleusement (y compris les majuscules et les espacements). Le respect de ces consignes facilite grandement la gestion des fichiers. Merci d'avance !

- sujet du mail : DM17 MPSI4
- nom du fichier : dm17-nom.pdf (par exemple dm17-troesch.pdf si c'est ma copie), sans accent, sans tréma, sans espace.

Vous faites AU CHOIX l'un des deux problèmes suivants. Vous avez le droit de faire les 2 bien entendu !

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 $\boxed{\text{théorème de d'Alembert-Gauss}}$.

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 $\boxed{\mathbb{K}_1 \text{ est un corps.}}$
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, $\boxed{\text{la restriction de } \varphi \text{ à } \mathbb{K} \text{ est injective}}$. 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, $\boxed{\theta \in \mathbb{K}_1 \text{ est une racine de } P}$.

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, $\boxed{\text{il existe un corps } \mathbb{K}_2 \text{ dans lequel } P \text{ est scindé}}$.

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 $\alpha_1 \geqslant \alpha_2 \geqslant \cdots \geqslant \alpha_n$, 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 $\boxed{\alpha_1 \geqslant \alpha_2 \geqslant \cdots \geqslant \alpha_n}$.

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 :
$$\mathrm{MD}(\Sigma_1^{\alpha_1-\alpha_2}\cdots\Sigma_{n-1}^{\alpha_{n-1}-\alpha_n}\Sigma_n^{\alpha_n}) = \prod_{i=1}^{n}X_i^{(\alpha_i-\alpha_{i+1})+\cdots+(\alpha_n-\alpha_{n+1})} = \prod_{i=1}^{n}X_i^{\alpha_i}.$$
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 $a_{N_1,1}=\min\limits_m(a_{m,1})$. 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'$\boxed{\text{existence d'une racine réelle de } P}$.
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, $\boxed{P\notin\mathbb{R}[X].}$

   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 $\boxed{Q\in\mathbb{R}[X]}$.

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 $\boxed{Q \text{ est irréductible sur } \mathbb{R}.}$
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 $\boxed{\text{tout polynôme non constant de } \mathbb{C}[X] \text{ admet une racine dans } \mathbb{C}}$.

Correction du problème 2 – (Théorème de l'élément primitif)

Partie I – Extensions de degré fini.

1. Soit $K \subset L$ et $L \subset M$ deux extensions de degré fini. Soit $(a_1, \dots, a_n)$ une base du K-ev L et $(b_1, \dots, b_m)$ une base du L-ev M. Soit alors $x \in M$. On a donc l'existence de scalaires $\lambda_1, \dots, \lambda_m$ dans le corps L tels que
$$x = \sum_{k=1}^{m} \lambda_k b_k.$$
Or, les coefficients λ_k sont dans L, dont une K-base est $(a_1, \dots, a_n)$. Ainsi, il existe pour tout $k \in [\![1, m]\!]$, il existe une famille $(\mu_{1,k}, \cdots, \mu_{n,k}$ telle que
$$\lambda_k = \sum_{\ell=1}^{n} \mu_{\ell,k} a_\ell.$$
On en déduit que :
$$x = \sum_{\ell=1}^{n} \sum_{k=1}^{m} \mu_{\ell,k} a_\ell b_k.$$
La famille $(a_\ell b_k)_{(\ell,k) \in [\![1,n]\!] \times [\![1,m]\!]}$ est donc une famille génératrice du K-ev L.
Par ailleurs étant donnés des scalaires $\lambda_{i,j} \in K$ tels que
$$\sum_{i=1}^{n} \sum_{j=1}^{m} \lambda_{i,j} a_i b_j = 0,$$
on peut écrire,
$$\sum_{j=1}^{m} \left(\sum_{i=1}^{n} \lambda_{i,j} a_i \right) b_j = 0.$$
Ainsi, la somme interne étant un élément de L, par liberté sur L de la famille (b_j), on obtient, pour tout $j \in [\![1, m]\!]$,
$$\sum_{j=1}^{m} \left(\sum_{i=1}^{n} \lambda_{i,j} a_i \right) = 0.$$
La liberté de la famille (a_i) sur K amène alors :
$$\forall (i,j) \in [\![1, n]\!] \times [\![1, m]\!], \quad \lambda_{i,j} = 0$$
Ainsi, la famille $(a_i b_j)$ est une famille libre.
Il s'agit donc d'une base de M sur K. Son cardinal est nm. On en déduit que
$$\dim_K M = \dim_K L \times \dim_L M \qquad \text{soit:} \qquad \boxed{[M : K] = [M : L] \times [L : K]}.$$

2. Soit $\alpha \in L$. La famille $(\alpha^n)_{n \in \mathbb{N}}$ ne peut pas être libre, car le cardinal d'une famille libre est inférieur à la dimension de l'espace. Ainsi, il existe une famille $(\lambda_n)_{n \in \mathbb{N}}$ de scalaires presque tous nuls, mais non tous nuls tels que $\sum\limits_{n=0}^{+\infty} \lambda_n \alpha^n = 0$. Les λ_i étant presque tous nuls, $P = \sum\limits_{n=0}^{+\infty} \lambda_n X^n$ est un polynôme, non nul, et tel que $P(\alpha) = 0$. Ainsi, α est algébrique sur K.
Par conséquent, $\boxed{\text{si } K \subset L \text{ est de degré fini, alors elle est algébrique.}}$

3. Soit $K \subset L$ une extension de degré fini. D'après la question précédente, elle est algébrique. Ainsi, étant donné $\alpha \in L$, il existe $P \in K[X]$ non nul tel que $P(\alpha) = 0$. Considérons $I = \{P \in K[X], P(\alpha) = 0\}$. L'ensemble I est clairement stable par différence et contient 0, c'est donc un sous-groupe additif de $K[X]$. Par ailleurs, si $P(\alpha) = 0$, alors pour tout $Q \in K[X]$, $PQ(\alpha) = 0$. Par conséquent, I est stable par multiplication par un élément de $K[X]$. Ainsi, I est un idéal non nul de $K[X]$. Comme $K[X]$ est principal, on en déduit qu'il existe $P_\alpha \neq 0$, qu'on peut choisir unitaire, tel que $I = (P_\alpha)$
Si P_α n'est pas irréductible, il existe une factorisation $P_\alpha = QR$ par des polynômes non constants. On a alors $Q(\alpha)R(\alpha) = 0$, d'où $Q(\alpha) = 0$ ou $R(\alpha) = 0$, par intégrité. Ainsi, Q ou R est un élément de I, donc divisible

par P_α. Cela contredit le fait que ces deux polynômes sont non nuls (car non constants) et de degré strictement inférieur à celui de P_α.

Ainsi, P_α est irréductible.

Par ailleurs, soit P un autre polynôme unitaire (distinct de P_α) de I. Montrons que $P \neq P_\alpha$. Cela provient du fait que P_α divise P. Si $\deg P = \deg P_\alpha$, on a l'existence d'une constante λ tel que $P = \lambda P_\alpha$. Les deux polynômes étant unitaires, $\lambda = 1$, ce qui contredit $P \neq P_\alpha$. On en déduit que $\deg P > \deg P_\alpha$, et la divisibilité par P_α nous donne l'existence d'une décomposition non triviale $P = P_\alpha Q$. Ainsi, P n'est pas irréductible.

Il existe donc un $\boxed{\text{unique polynôme irréductible unitaire } P_\alpha \text{ tel que } P_\alpha(\alpha) = 0.}$

Partie II – Adjonction d'un ou plusieurs éléments à un corps

1. Soit $M = \bigcap_{i\in I} M_i$. On a $M \subset L$. Par ailleurs, 1_L est dans chaque M_i, donc M est non vide. De plus, si x et y sont dans M, pour tout $i \in I$, $x, y \in M_i$, et M_i étant un sous-corps de L, $x - y \in M_i$, et si de plus y est inversible, $xy^{-1} \in M_i$. Ces inclusions étant vraies pour tout $i \in I$, $x - y \in M$ et si y est inversible $xy^{-1} \in M$.

   On en déduit que $\boxed{M \text{ est un sous-corps de } L.}$
2. On considère $\mathcal{M}$ l'ensemble des sous-corps M de K tels que $K \cup E \subset M$. L'ensemble $\mathcal{M}$ est non vide, puisque $L \in \mathcal{M}$. On définit
$$M_0 = \bigcap_{M\in\mathcal{M}} M.$$
   Il s'agit d'un sous-corps de L d'après la question précédente. Ce corps contient $K \cup E$, car c'est le cas de chaque M de l'intersection. Par ailleurs, pour tout corps M_1 contenant K et E, M_1 est l'un des termes de l'intersection, donc $M_0 \subset M_1$. Ainsi, M_1 est bien le plus petit sous-corps de L contenant $K \cup E$.

   D'où $\boxed{\text{l'existence de } K(E).}$
3.
   - On a $E \subset K(E) \subset K(E)(F)$, $F \subset K(E)(F)$ et $K \subset K(E) \subset K(E)(F)$. Ainsi, $K \cup E \cup F \subset K(E)(F)$. Comme de plus, par définition, $K(E)(F)$ est un corps, $K(E \cup F) \subset K(E)(F)$, par propriété de minimalité de $K(E \cup F)$.
   - On a $K \subset K(E \cup F)$ et $E \subset K(E \cup F)$, et $K(E \cup F)$ est un corps. Donc, par minimalité de $K(E)$, $K(E) \subset K(E \cup F)$. De plus, $F \subset K(E \cup F)$, donc par minimalité de $K(E)(F)$, $K(E)(F) \subset K(E \cup F)$.
   - Les deux inclusions amènent l'égalité $\boxed{K(E \cup F) = K(E)(F).}$
4. Considérons $K = \mathbb{R}$, $L = \mathbb{C}$, $\alpha = 1$ (ou n'importe quel réel), et $\beta = \mathrm{i}$. On a alors $K(\alpha) = \mathbb{R}$ et $K(\beta) = \mathbb{C}$. Or, les corps $\mathbb{R}$ et $\mathbb{C}$ ne sont pas isomorphes. En effet, soit $\varphi : \mathbb{R} \to \mathbb{C}$ un morphisme de corps. Supposons que φ soit un isomorphisme. Par surjectivité, il existe $x \in \mathbb{R}$ tel que $\varphi(x) = \mathrm{i}$. On a alors $\varphi(x^2) = \varphi(x)^2 = \mathrm{i}^2 = -1$. Or, $\varphi(-1) = -\varphi(1) = -1$, donc, par injectivité, $x^2 = -1$, ce qui est impossible puisque $x \in \mathbb{R}$.

   Ainsi, en général, $\boxed{\text{on n'a pas } K(\alpha) = K(\beta)}$.
5. Soit $x \in K[X]/(P)$ non nul, et Q un représentant de x dans P. Le polynôme Q n'est alors par divisible par P (puisque x est non nul). Le polynôme P étant irréductible, Q est premier avec P (sinon, le PGCD, non constant et différent de P par non divisibilité, diviserait P, ce qui contredirait son irréductibilité).

   Il existe donc, d'après le théorème de Bézout, deux polynômes U et V tels que $UP + VQ = 1$. En passant au quotient, et en notant y la classe de V dans $K[X]/(P)$, on obtient $xy = \overline{1}$. Ainsi, x est inversible.

   Par conséquent, $\boxed{\text{l'anneau } K[X]/(P) \text{ est un corps.}}$
6.
   - Soit $Q = 1$ le polynôme constant égal à 1. On a alors $Q(\alpha) = 1$. Donc $\varphi(1) = 1$.
   - Soit Q_1, Q_2 deux polynômes. On a
$$\varphi(Q_1 + Q_2) = (Q_1 + Q_2)(\alpha) = Q_1(\alpha) + Q_2(\alpha) = \varphi(Q_1) + \varphi(Q_2),$$
     et de même $\varphi(Q_1Q_2) = \varphi(Q_1)\varphi(Q_2)$.
   - Ainsi, $\boxed{\varphi \text{ est un morphisme d'anneaux.}}$
   - En adaptant l'argument de la question I-3, les polynômes annulant α forment un idéal non nul (il contient P_α), engendré par un polynôme irréductible unitaire P_α qui est l'unique polynôme irréductible unitaire annulant α. Ce polynôme irréductible unitaire est alors le polynôme irréductible P divisé par son coefficient

dominant (par unicité). On en déduit qu'il existe $\lambda \in K$ tel que $P = \lambda P_\alpha$. Ainsi, P et P_α engendrent le même idéal, donc $\boxed{\mathrm{Ker}(\varphi) = (P)}$.

7. En quotientant $K[X]$ par le noyau de φ, l'application φ passe au quotient et définit un morphisme d'anneau injectif de $K[X]/(P) \to L$ (donc un morphisme de corps), Son image est donc un sous-corps de L. Montrons que cette image (qui est aussi $\mathrm{Im}(\varphi)$) est $K(\alpha)$.

   En effet, on a, pour tout polynôme constant $Q = x \in K$, $\varphi(x) = x$ donc $x \in \mathrm{Im}(\varphi)$, donc $K \subset \mathrm{Im}(\varphi)$. De plus, $\varphi(X) = \alpha$, donc $\alpha \in \mathrm{Im}(\varphi)$. Comme $\mathrm{Im}(\varphi)$ est un corps, par minimalité, on a donc $K(\alpha) \subset \mathrm{Im}(\varphi)$.

   Réciproquement, par stabilité par produit et somme, puisque $\alpha \in K(\alpha)$, et $K \subset K(\alpha)$, toute combinaison linéaire de puissances de α à coefficients dans K est encore dans $K(\alpha)$, donc $\mathrm{Im}(\varphi) \subset K(\alpha)$.

   On a donc $\mathrm{Im}(\varphi) = K(\alpha)$, et l'injectivité étant acquise, on a un $\boxed{\text{isomorphisme de corps entre } K[X]/(P) \text{ et } K(\alpha).}$

8. Soit α et β deux racines d'un polynôme irréductible P. La question précédente montre que $K(\alpha)$ et $K(\beta)$ sont tous deux isomorphes au même corps $\mathbb{K}[X]/(P)$, donc $\boxed{K(\alpha) \simeq K(\beta)}$.

   On remarquera que l'isomorphisme de la question précédente est un isomorphisme d'espace vectoriel sur K, donc en particulier, $K(\alpha)$ et $K(\beta)$ auront même dimension sur K. On se servira de cette remarque par la suite.

9. Considérons $P = X^3 - 2 \in \mathbb{Q}[X]$. Ses racines dans $\mathbb{C}$ sont $\sqrt[3]{2}$, $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$. Or, si P n'est pas irréductible, il se factorise en un produit non trivial de polynômes irréductibles de $\mathbb{Q}[X]$, dont l'un au moins aura un degré égal à 1. Ce polynôme s'écrira donc sous la forme $X - \alpha$ (à une constante multiplicative près), avec α rationnel. Le rationnel α est alors une racine de P. Mais $\sqrt[3]{2}$ est irrationnel, donc P n'a pas de racine rationnelle, d'où une contradiction.

   On en déduit que Q est irréductible.

   Clairement $Q(\sqrt[3]{2}) \neq Q(j\sqrt[3]{2})$, puisque le premier corps est inclus dans $\mathbb{R}$ et pas le second. Donc en général $\boxed{\text{on n'a pas } K(\alpha) = K(\beta)}$ pour α et β deux racines d'un même polynôme irréductible P.

Partie III – Corps de décomposition d'un polynôme

1. D'après II-5, i est bien une application entre deux corps. On a trivialement, par définition de la structure quotient $\varphi(1) = \overline{1} = 1_{K[X]/(P)}$, $\varphi(\lambda\mu) = \overline{\lambda\mu} = \overline{\lambda}\,\overline{\mu} = \varphi(\lambda)\varphi(\mu)$ et de même $\varphi(\lambda + \mu) = \varphi(\lambda) + \varphi(\mu)$.

   Ainsi, $\boxed{\varphi \text{ est un morphisme de corps.}}$

2. Soit $\alpha = \overline{X}$ la classe de X dans $K[X]/(P)$. En notant $P = \sum\limits_{k=0}^{d} \lambda_k X^k$, on a

$$P(\alpha) = \sum_{k=0}^{d} \lambda_k \alpha^k = \sum_{k=0}^{d} \overline{\lambda_k X}^k,$$

   puisqu'on a identifié λ_k et $\overline{\lambda_k}$ via le morphisme i. On a donc :

$$P(\alpha) = \overline{\sum_{k=0}^{k} \lambda_k X^k} = \overline{P} = 0_{K[X]/(P)}.$$

   Ainsi, α est racine de P, donc $\boxed{P \text{ admet une racine dans } K[X]/(P).}$

3. Soit $P \in K[X]$. Soit P_0 un facteur irréductible de P. Il existe d'après la question précédente une extension L de K telle que P_0 admette une racine dans L. Comme P_0 divise P, P admet cette même racine dans L.

   Ainsi, $\boxed{\text{il existe une extension } L \text{ de } K \text{ telle que } P \text{ admette une racine dans } L.}$

   Autrement dit, il existe un corps de rupture de P.

4. On montre par récurrence sur $n \in \mathbb{N}^*$ que pour tout corps K, et tout polynôme P de degré n dans $K[X]$, il existe une extension $K \subset L$ de K telle que P soit scindé sur L. Remarquez que je quantifie sur le corps dans la propriété de récurrence.

   Pour $n = 1$, la propriété est évidente, un polynôme de degré 1 s'écrivant $P = \lambda(X - \alpha)$, avec λ, α dans K.

   Soit $n \in \mathbb{N}^*$ tel que la propriété soit vérifiée pour les polynômes de degré n (sur un corps quelconque). On considère K un corps et P un polynôme de degré $n + 1$ dans $K[X]$. D'après la question précédente, il existe une extension $K \subset M$ telle que P ait une racine α dans M. On peut alors factoriser $P = (X-\alpha)Q$, où Q est un polynôme de $M[X]$ de degré n. On peut appliquer l'hypothèse de récurrence sur $Q \in M[X]$ (on voit ici la nécessité d'étendre l'hypothèse de récurrence à tout corps, puisqu'on l'utilise pour un corps distinct du corps initial K). Ainsi, il existe une extension L de M telle que Q soit scindé sur L. Le corps L est aussi une extension de K, et P est alors scindé sur L.

D'après le principe de récurrence, pour tout corps K, pour tout polynôme P de $K[X]$, il existe une extension L de K telle que $\boxed{P \text{ soit scindé sur } L.}$

5. • Puisque λ est un morphisme de corps,

$$\overline{\lambda}(1_K) = \lambda(1_K) = 1_{K'}$$

(vu comme élément de $K'[X]$: il s'agit du polynôme constant)

• Soit $P = \sum\limits_{k=0}^{+\infty} a_k X^k$ et $Q = \sum\limits_{k=0}^{+\infty} b_k X^k$, les a_k et les b_k étant presque tous nuls. Puisque $\lambda(0) = 0$, les $\lambda(a_k)$ et $\lambda(b_k)$ sont aussi presque tous nuls, ce qui permet de justifier que $\widehat{\lambda}$ est bien défini. On a de plus :

$$\widehat{\lambda}(P+Q) = \sum_{k=0}^{+\infty} \lambda(a_k+b_k)X^k = \sum_{k=0}^{+\infty} (\lambda(a_k)+\lambda(b_k))X^k = \widehat{\lambda}(P) + \widehat{\lambda}(Q),$$

ainsi que :

$$\widehat{\lambda}(PQ) = \sum_{k=0}^{+\infty} \lambda\left(\sum_{\ell=0}^{k} a_\ell b_{k-\ell}\right) X^k = \sum_{k=0}^{+\infty} \left(\sum_{\ell=0}^{k} \lambda(a_\ell)\lambda(b_{k-\ell})\right) X^k = \widehat{\lambda}(P)\widehat{\lambda}(Q).$$

• Ainsi, $\widehat{\lambda}$ est un morphisme d'anneau.

• Tout $\sum\limits_{k=0}^{+\infty} b_k X^k \in K'[X]$ est l'image par φ de $\sum\limits_{k=0}^{+\infty} a_k X^k \in K[X]$, où pour tout k, $a_k = \lambda^{-1}(b_k)$ (existe par bijectivité). Donc $\widehat{\lambda}$ est surjective.

• Soit $P = \sum\limits_{k=0}^{+\infty} a_k X^k \in \operatorname{Ker}(\widehat{\lambda})$. On a donc $\sum\limits_{k=0}^{+\infty} \lambda(a_k)X^k = 0$, donc les coefficients de ce polynôme sont tous nuls. Ainsi, pour tout $k \in \mathbb{N}$, $\lambda(a_k) = 0$, et λ étant un isomorphisme d'anneaux, $a_k = 0$. On en déduit que $P = 0$. Ainsi, $\operatorname{Ker}(\widehat{\lambda}) = \{0\}$, donc $\widehat{\lambda}$ est injective.

On en déduit que $\boxed{\widehat{\lambda} \text{ est un isomorphisme d'anneaux.}}$

6. Soit P un polynôme de $K[X]$ tel que P_λ ne soit pas irréductible. Notons φ l'isomorphisme réciproque de $\widehat{\lambda}$. Comme $\widehat{\lambda}$ respecte les degrés, il en est de même de φ. Soit une décomposition $P_\lambda = QR$, en polynômes de degrés strictement positifs. On a alors

$$P = \varphi(P_\lambda) = \varphi(QR) = \varphi(Q)\varphi(R).$$

D'après la propriété ci-dessus de conservation du degré par φ, il s'agit d'une décomposition de P assurant que P n'est pas irréductible.

Ainsi, par contraposée, $\boxed{\text{si } P \text{ est irréductible, } P_\lambda \text{ l'est aussi.}}$

L'application $\widehat{\lambda}$ définit, par composition avec la projection $\pi : K'[X] \to K'[X]/(P_\lambda)$, un morphisme d'anneaux μ de $K[X]$ dans $K'[X]/(P_\lambda)$, surjectif en tant que composée de 2 surjections. Soit $Q \in \operatorname{Ker}(\mu)$. On a donc $\overline{Q_\lambda} = 0$, soit $P_\lambda \mid Q_\lambda$. Comme $\widehat{\lambda}$ est un isomorphisme d'anneaux, la factorisation traduisant cette divisibilité se traduit en une factorisation dans $K[X]$, donc $P \mid Q$. Ainsi, $\operatorname{Ker}(\mu) \subset (P)$, la réciproque étant immédiate. Par conséquent, $\operatorname{Ker}(\mu) = (P)$, et on peut donc passer μ au quotient, définissant un morphisme injectif d'anneaux de $K[X]/(P)$ dans $K'[X]/(P_\lambda)$, la surjectivité étant aussi préservée par passage au quotient. Ainsi, il s'agit d'un isomorphisme d'anneaux, et comme ces quotients sont les corps, il s'agit d'un isomorphisme de corps.

On a bien montré que $\boxed{K[X]/(P) \text{ et } K'[X]/(P') \text{ sont isomorphes.}}$

Il n'est pas dur de constater qu'une base du K-ev $K[X]/(P)$ sera envoyée sur une base du K'-ev $K'[X]/(P')$ par cette isomorphisme. Ainsi, les deux extensions de K et K' respectivement ainsi définies ont même degré. Nous nous servirons plus tard de cette remarque.

7. Montrons par récurrence sur $\deg P$ que pour tout corps K, tout isomorphisme $\lambda : K \to K'$, pour tout $P \in K[X]$ non nul, toute extension $K \subset L$ et toute extension $K' \subset L'$ telles que P soit scindé dans L et P_λ soit scindé dans L', en notant $\alpha_1, \cdots, \alpha_r$ les racines distinctes de P dans L et $\beta_1, \ldots, \beta_s$ les racines distinctes de P_λ dans L', le sous-corps $K(\alpha_1, \ldots, \alpha_r)$ de L et le sous-corps $K'(\beta_1, \ldots, \beta_s)$ de L' sont isomorphes.
   - Si P est constant non nul, les ensembles de racine sont vides donc $K(\mathrm{Rac}(P)) = K(\varnothing) = K \simeq K' = K'(\varnothing) = K'(\mathrm{rac}(P'))$, d'où le résultat.
   - Soit $n \in \mathbb{N}$. Supposons la propriété vraie pour tous corps et tout polynôme de degré n tel que dans la propriété de récurrence. Soit K, K', L, L' et P de degré $n+1$ vérifiant les hypothèses de la propriété. Soit $P = QR$, où Q est irréductible (éventuellement, R est constant si P est lui-même irréductible). Une telle décomposition existe du fait que P n'est pas constant. On a alors $P_\lambda = Q_\lambda R_\lambda$, et Q_λ est irréductible. Soit α_1 dans L une racine de Q et β_1 une racine de Q_λ dans L' (existant par hypothèse). On complète en $\alpha_1, \ldots, \alpha_r$ les racines de P et $\beta_1, \ldots, \beta_s$ les racines de P_λ.

     D'après II-7, $K(\alpha_1)$ est isomorphe à $K[X]/(P)$, et $K'(\beta_1)$ est isomorphe à $K'[X]/(P_\lambda)$. D'après III-6, $K[X]/(P)$ et $K'[X]/(P_\lambda)$ sont isomorphes. On en déduit, par composition, que $K(\alpha_1)$ et $K(\beta_1)$ sont isomorphes. Par ailleurs, la description explicite des isomorphismes que l'on compose ainsi (isomorphismes construits dans lesdites questions) montre que l'on peut trouver un isomorphisme $\mu = K(\alpha_1) \to K'(\beta_1)$ coïncidant avec λ sur K et tel que $\mu(\alpha_1) = \beta_1$.

     On peut factoriser P dans $K(\alpha_1)$ sous la forme $P = (X - \alpha_1)Q$. Appliquant la question 5 à μ, coïncidant avec λ sur K, on obtient
     $$P_\lambda = P_\mu = \widehat{\mu}(X - \alpha_1)Q_\mu = (X - \beta_1)Q_\mu.$$
     Les racines de Q sont alors $\alpha_2, \ldots, \alpha_r$ auquel on doit éventuellement ajouter α_1 (si elle était racine multiple de P), et les racines de Q_μ sont de même $\beta_2, \ldots, \beta_s$, auquel on ajoute éventuellement β_1. Par conséquent, le corps de décomposition de Q est $K(\alpha_1)(\alpha_2, \ldots, \alpha_s)$ (la discussion sur α_1 disparaît du fait que α_1 est de toute manière déjà élément du corps de base considéré), et le corps de décomposition de Q' est $K'(\beta_1)(\beta_2, \ldots, \alpha_r)$. On peut appliquer l'hypothèse de récurrence, du fait que Q est de degré n et que $K(\alpha_1)$ et $K(\alpha_2)$ sont isomorphes. Ainsi
     $$K(\alpha_1)(\alpha_2, \ldots, \alpha_r) \simeq K'(\beta_1)(\beta_2, \ldots, \beta_s).$$
     On déduit alors de la question II-3 que $\boxed{K(\alpha_1, \ldots, \alpha_r) \simeq K'(\beta_1, \ldots, \beta_s)}$
   - D'après le principe de récurrence, cette propriété est donc vraie pour tout polynôme.

   La remarque de la question précédente s'adapte ici aussi : les deux extensions obtenues auront même degré.
8. On applique la question précédente à l'isomorphisme $\mathrm{id} : K \to K$, $K \subset L$ et $K \subset L'$ deux extensions telles que L et L' soient des corps de décomposition du polynôme P. On a alors $L = K(\mathrm{Rac}_L(P))$ et $L' = K(\mathrm{Rac}_{L'}(P))$, d'après la remarque suivant III-4. La question III-7 nous donne alors $L \simeq L'$.

   Ainsi, $\boxed{\text{deux corps de décomposition d'un polynôme } P \text{ sont isomorphes.}}$
9. Soit $K \subset L$ une extension de corps.
   - Supposons que L soit le corps de décomposition d'un polynôme P de $K[X]$.

     Pour commencer, $K \subset L$ est de degré fini, car en notant $\alpha_1, \ldots, \alpha_k$ les racines de P,
     $$K \subset K(\alpha_1) \subset K(\alpha_1)(\alpha_2) \subset \cdots \subset K(\alpha_1, \ldots, \alpha_{k-1})(\alpha_k) = K(\alpha_1, \cdots \alpha_k),$$
     chacune de ces extensions étant de degré fini, car isomorphe à un $L[X]/(Q)$ d'après la partie 1, une telle extension étant de degré fini, puisqu'engendrée par des représentants de $1, X, \cdots, X^{d-1}$, où d est le degré de Q. En effet, pour toute classe, on pourra toujours trouver un représentant de degré strictement plus petit que d en considérant le reste de la division euclidienne d'un représentant quelconque par Q). Ainsi, $\boxed{K \subset L \text{ est de degré fini d'après I-1.}}$

     En notant $\alpha_1, \ldots, \alpha_k$ les racines de P dans L, on a donc $L = K(\alpha_1, \ldots, \alpha_k)$. Soit Q un polynôme irréductible ayant une racine β dans L. On considère M une extension de L, corps de décomposition du polynôme PQ (qui peut être vu comme polynôme à coefficients dans L, ce qui assure $L \subset M$). Soit γ une autre racine de Q. Les racines de P étant les α_i, et par description du corps de décomposition lorsqu'on dispose d'un corps dans lequel P est scindé, puisque
     $$L(\beta) = K(\alpha_1, \ldots, \alpha_k, \beta) = K(\beta)(\alpha_1, \ldots, \alpha_k),$$

$L(\beta)$ est corps de décomposition de P sur $K(\beta)$. De même, $L(\gamma)$ est corps de décomposition de P sur $K(\gamma)$. Or, on a vu dans la question 7 que puisque β et γ sont racines d'un même polynôme irréductible, il existe un isomorphisme d'anneaux $\mu : K(\beta) \to K(\gamma)$ coïncidant avec l'identité sur K et tel que $\mu(\beta) = \gamma$. On a alors $P_\mu = P$, puisque P est à coefficients dans γ. Or, la question 7 affirme que le corps de décomposition de P sur $K(\beta)$ est isomorphe au corps de décomposition de P_μ (donc de P) sur $K(\gamma)$. Comme toutes les extensions considérés sont de degré fini, on peut donc écrire

$$[L(\beta) : K(\beta)] = [L(\gamma) : K(\gamma)]$$

D'après I-8 (et la remarque qui suit sa résolution), on a également

$$[K(\beta) : K] = [K(\alpha) : K].$$

La question I-1, amène alors :

$$[L(\beta) : K] = [L(\beta) : K(\beta)][K(\beta) : K] = [L(\alpha) : K(\alpha)] : [K(\alpha) : K] = [L(\alpha) : K].$$

Une nouvelle application de I-1 amène :

$$[L(\beta) : L][L : K] = [L(\gamma) : L][L : K].$$

En simplifiant par $[L : K] \neq 0$, il vient $[L(\beta) : L] = [L(\gamma) : L]$. Or, $\beta \in L$ par hypothèse, donc

$$[L(\gamma) : L] = [L(\beta) : L] = 1.$$

On en déduit que $L(\gamma) = L$, donc $\boxed{\gamma \in L}$. Ainsi, toute racine de Q est dans L, donc $\boxed{Q \text{ est scindé dans } L.}$

- Réciproquement, supposons que $K \subset L$ est une extension de degré fini telle que tout polynôme irréductible de $K[X]$ ayant une racine dans L soit scindé dans L. Comme L est de dimension finie sur K, il existe $(\alpha_1, \dots, \alpha_n)$ une base de L sur K. On a alors de façon immédiate $L = K(\alpha_1, \dots, \alpha_n)$. Les éléments $\alpha_1, \dots, \alpha_n$ sont algébriques puisque l'extension est de degré fini. Soit $P_1, \dots, P_k$ dans $K[X]$ les polynômes irréductibles de $\alpha_1, \dots, \alpha_n$. Comme $P_1, \dots, P_n$ sont irréductibles et admettent une racine dans L, par hypothèse, ils sont scindés dans L. On considère $P = P_1 \cdots P_n$. Puisque P est scindé dans L, il existe un corps de décomposition M de P tel que $M \subset L$. Plus précisément, $K(\mathrm{Rac}(P)) \subset L$. Par ailleurs, puisque $\{\alpha_1, \dots, \alpha_n\} \subset \mathrm{Rac}(P)$, on a aussi :

$$L = K(\alpha_1, \dots, \alpha_n) \subset K(\mathrm{rac}(P));$$

Ainsi, $L = K(\mathrm{rac}(P))$, et $\boxed{L \text{ est donc corps de décomposition de } P.}$

Partie IV – Extensions séparables

1. Soit $P \in K[X]$ non constant, et L un corps de décomposition de P.
   (a) Soit $\alpha \in L$. On suppose que $X - \alpha$ divise P et P' dans $L[X]$, et on écrit $P = (X - \alpha)Q$, où $Q \in L[X]$. On a alors
   $$P' = Q + (X - \alpha)Q'.$$
   Comme $X - \alpha$ divise P' et $(X - \alpha)Q'$, on en déduit que $\boxed{X - \alpha \text{ divise } Q.}$

   (b)
   - Supposons que P est inséparable. Le polynôme P admet donc une racine double dans L. On peut donc factoriser dans L sous la forme $P = (X - \alpha)^2 R$. On a alors $P' = (X - \alpha)((X - \alpha)R' + 2XR)$. Ainsi, $X - \alpha$ divise à la fois P et P', donc $P \wedge P' \neq 1$.
   - Réciproquement, si $P \wedge P' \neq 1$, P et P' étant scindés sur L, ils admettent une racine commune α. Ils sont donc tous deux divisibles par $X - \alpha$. D'après la question précédente, en reprenant les notations de cette question, on peut factoriser Q sous la forme $Q = (X - \alpha)R$, donc $P = (X - \alpha)^2 R$. On en déduit que α est racine au moins double de P dans L, donc P est inséparable.

   Ainsi, $\boxed{P \text{ est inséparable si et seulement si } P \wedge P' \neq 1.}$

   Remarquez qu'on a utilisé le PGCD dans $L[X]$ alors que le PGCD considéré est en fait dans $K[X]$. Ce n'est pas, gênant, puisque le PGCD est invariant pas extension de corps (pour un polynôme à coefficients dans

K, l'algorithme d'Euclide s'écrit de la même façon que l'on se place dans $K[X]$ ou dans $L[X]$, L étant une extension de K).

Remarquez également qu'on ne peut pas se servir directement de la caractérisation de la multiplicité par les dérivées donnée dans le cours, cette caractérisation ayant été établie pour un corps de caractéristique nulle.

2. Soit K un corps de caractéristique nulle, et P un polynôme irréductible. En particulier, P est non constant. Donc $P' \neq 0$, et $\deg P' < \deg P$. On a alors nécessairement $P \wedge P' = 1$, sinon, il existerait Q non constant, de degré inférieur ou égal à $\deg P'$, donc strictement inférieur à $\deg P$, divisant simultanément P et P'. Cela contredirait l'irréductibilité de P. Ainsi, d'après la question précédente, P est séparable.

   Ainsi, en caractéristique nulle, $\boxed{\text{tout polynôme irréductible est séparable.}}$

   Soit K un corps de caractéristique $p \neq 0$, et P un polynôme irréductible. Si $P' \neq 0$ le raisonnement précédent reste valide, et donc P est séparable. Si $P' = 0$, alors $P \wedge P' = P$ (ou plutôt l'unique polynôme unitaire colinéaire à P), donc $P \wedge P' \neq 1$, un polynôme irréductible n'étant pas constant. Donc P est inséparable d'après la question précédente.

   Ainsi, en caractéristique non nulle, $\boxed{\text{un polynôme irréductible est séparable si et seulement si } P' \neq 0.}$

3. Soit p un nombre premier impair. On donne ici un exemple de polynôme irréductible non séparable pour un corps K de caractéristique p.

   (a) Il suffit de considérer $K = \mathbb{F}_p(X)$ le corps des fractions de $\mathbb{F}_p$. L'élément $t = X$ de K n'est pas algébrique sur $\mathbb{F}_p$, car par définition même des polynômes formels (qui sont aussi des fractions rationnelles via l'identification classique), pour tout $P \in \mathbb{F}_p(X)$ non nul, $P(t) = P(X) = P \neq 0$!

   Ainsi, $\mathbb{F}_p$ admet une $\boxed{\text{extension } K \text{ dans laquelle il existe un élément transcendant } t.}$

   (b) Soit L un corps de décomposition de $P = X^p - t$. Soit α une racine de P dans L. On a donc $\alpha^p = t$. D'après la formule du binôme,
$$(X-\alpha)^p = \sum_{k=0}^{p} \binom{p}{k} (-\alpha)^k X^{p-k}.$$
   Or, p est premier, donc $\binom{p}{k}$ est divisible par p pour tout $k \in [\![1, p-1]\!]$. Comme K est de caractéristique p, on en déduit que
$$(X-\alpha)^p = X^p + (-\alpha)^P.$$
   Or, p est impair et $\alpha^p = t$, donc $\boxed{(X-\alpha)^p = X^p - t.}$

   (c) Supposons que P n'est pas irréductible. Il existe donc dans $K[X]$ un diviseur Q de $K[X]$, non constant et de degré strictement inférieur à celui de P. Il s'agit aussi d'un diviseur dans $L[X]$. D'après la question précédente, il existe donc $q \in [\![1, p-1]\!]$ tel que $Q = (X-\alpha)^q$.

   On peut raisonner sur la somme des racines, égale à un coefficient de Q, donc élément de K (puisque $Q \in K[X]$) : les racines étant en nombre q et toutes égales à α, on obtient $q\alpha \in K$. Comme $q \in [\![1, p-1]\!]$ et p est premier, q est premier avec p donc est inversible modulo p d'après le théorème de Bezout (donc inversible dans $\mathbb{F}_p \subset K$). On en déduit que $\boxed{\alpha \in K.}$

   (d) On suppose que P n'est pas irréductible. D'après la question précédente, $\alpha \in K = \mathbb{F}_p(t)$. Or, l'application $\varphi : F_p(X) \mapsto K$ qui à une fraction rationnelle F associe $F(t)$ est clairement bien définie, car si $F = \frac{P}{Q}$, $P(t)$ et $Q(t)$ sont à valeurs dans K par stabilité, et $Q(t)$ est non nul, puisque t n'est pas algébrique. Il est assez immédiat de vérifier que φ est un morphisme de corps, donc son image est un sous-corps de K contenant $\mathbb{F}_p$ (image des fractions rationnelles constantes) et t (image de X). Par minimalité de $K = \mathbb{F}_p(t)$, on a donc $K = \mathrm{Im}(\varphi)$.

   En particulier, puisque $\alpha \in K$, on peut donc écrire $\alpha = F(t)$ pour une certaine fraction rationnelle $F \in \mathbb{F}_p[X]$. L'équation $\alpha^p = t$ se réécrit alors $F(t)^p - t = 0$. En écrivant $F = \frac{P}{Q}$, avec P et Q premiers entre eux, il vient
$$P(t)^p - tQ(t)^p = 0.$$
   Comme t n'est pas algébrique, cette relation n'est possible que si $P^p - XQ^p$ est le polynôme nul. Or, $\deg(P^p) \equiv 0 \ [p]$ et $\deg(XQ^p) \equiv 1 \ [p]$, d'où une contradiction.

   Ainsi, $\boxed{P \text{ est irréductible, et inséparable}}$, puisqu'il n'a qu'un racine de mulitplicité p.

4. Soit $K \subset L \subset M$ deux extensions de corps.
   (a) Soit $\alpha \in M$, algébrique sur K. Il existe donc un polynôme $P \in K[X]$ tel que $P(\alpha) = 0$. Comme $K \subset L$, on a aussi $P \in L[X]$, donc $\boxed{\alpha \text{ est algébrique sur } L}$.
   (b) Soit $P_\alpha \in K[X]$ le polynôme irréductible de α sur K et $Q_\alpha \in L[X]$ le polynôme irréductible de α sur L. En particulier, on a aussi $P_\alpha \in L[X]$, donc P_α est un polynôme annulateur de α dans $L[X]$. Or, par un argument similaire à I-3, l'ensemble des polynômes annulateurs de α dans $L[X]$ est (Q_a). On en déduit que $P_\alpha \in (Q_\alpha)$, donc $\boxed{Q_\alpha \text{ divise } P_\alpha.}$
   (c) Supposons que $K \subset M$ est séparable.
      - Puisque $L \subset M$, pour tout $\alpha \in L$, la séparibilité de l'extension $K \subset M$ assure que α est algébrique sur K et que P_α le polynôme minimal de α sur K (c'est le même qu'on se place globalement dans L ou dans M) est séparable. Donc $\boxed{K \subset L \text{ est séparable}}$.
      - Soit $\alpha \in M$. Puisque $K \subset M$ est séparable, α est algébrique sur K donc sur L d'après 4(a). Soit $Q_\alpha \in L[X]$ son polynôme irréductible sur L et P_α sont polynôme irréductible sur K. D'après 4(b), Q_α divise P_α. Or, P_α n'ayant que des racines simples dans un corps de décomposition, il en est de même de ses diviseurs, donc que Q_α. Ainsi, α est séparable. On en déduit que $\boxed{L \subset M \text{ est séparable}}$.

Partie V – Théorème de l'élément primitif

1. Soit $K \subset L$ une extension de degré fini, telle que K soit de cardinal infini.
   (a) On suppose qu'il existe α et β tels que $L = K(\alpha, \beta)$. Comme $K \subset L$ est de degré fini, α et β sont algébriques sur K, d'après I-2. Il existe donc des polynômes irréductibles P_α et P_β de α et β sur K.

      Soit $\alpha, \alpha_2, \cdots, \alpha_r$ et $\beta, \beta_2, \ldots, \beta_s$ respectivement les racines distinctes de P_α et de P_β dans un corps M de décomposition du produit $P_\alpha P_\beta$.

      Puisque $K \subset L$ est séparable, les β_j, $j \in [\![2, s]\!]$, sont deux à deux distincts, et distincts de β. Ainsi, $\beta_j - \beta \neq 0$ pour tout $j \in [\![2, s]\!]$. L'équation $\alpha_i + t\beta_j = \alpha + t\beta$ équivaut donc à $t = \frac{\alpha - \alpha_j}{\beta_j - \beta}$.

      Il suffit donc de choisir $t \in K^*$ distinct des $\frac{\alpha - \alpha_j}{\beta_j - \beta}$, $i \in [\![2, r]\!]$, $j \in [\![2, s]\!]$, ce qui est possible puisque ces valeurs sont en nombre fini (au plus $(r-1)(s-1)$) alors que K^* est infini par hypothèse.

      Il est donc possible de choisir $t \in K^*$ tel que pour tout $(i, j) \in [\![2, r]\!] \times [\![2, s]\!]$, $\boxed{\alpha_i + t\beta_j \neq \alpha + t\beta}$.
   (b) On se donne un tel t, et on pose $\theta = \alpha + t\beta$. Soit $H \in K(\theta)[X]$ le polynôme à coefficients dans $K(\theta)$ défini par $H(X) = P_\alpha(\theta - tX)$. On se place dans un corps de décomposition de HP_β. Dans un tel corps, les deux polynômes H et P_β sont scindés. Leur pgcd est donc obtenu en considérant leurs racines communes et en conservant leur multiplicité minimale dans ces deux polynômes. Les racines communes sont nécessairement des racines de P_β, donc β ou les β_j, $j \in [\![2, s]\!]$. Or, pour tout $j \in [\![2, s]\!]$,
      $$H(\beta_j) = P_\alpha(\alpha + t\beta - t\beta_j).$$
      Or, d'après le choix de t, $\alpha + t\beta - t\beta_j$ n'est égal à aucun α_j. Il ne peut pas être égal à α non plus, sinon au aurait $\beta = \beta_j$, ce qui n'ets pas de cas, P_β étant séparable. On en déduit que $\alpha + t\beta - t\beta_j$ n'est pas une racine de P_α donc β_j n'est pas racine de H.

      En revanche,
      $$H(\beta) = P_\alpha(\alpha + t\beta - t\beta) = P(\alpha) = 0.$$
      Ainsi, la seule racine commune de H et P_β est β, et cette racine ne peut pas être multiple, puisque par hypothèse, P_β est séparable.

      Ainsi, $\boxed{H \wedge P_\beta = X - \beta}$.
   (c) Puisque $H \in K(\theta)[X]$ et $P_\beta \in K(\theta)[X]$, on a aussi $H \wedge P_\beta \in K(\theta)[X]$, et donc $\boxed{\beta \in K(\theta).}$

      On a de plus $\alpha = \theta - t\beta$, donc on a aussi $/a \in K(\theta)$. Ainsi, par minimalité de $K(\alpha, \beta)$ comme corps contenant K, α et β, on en déduit que $K(\alpha, \beta) \subset K(\theta)$.

      Réciproquement, puisque clairement $\theta \in K(\alpha, \beta)$ le même argument donne $K(\theta) \subset K(\alpha, \beta)$.

      Les deux inclusions donnent $\boxed{K(\theta) = K(\alpha, \beta) = L.}$

(d) Montrons par récurrence sur $n \in \mathbb{N}$ que si $L = K(\alpha_1, \dots, \alpha_n)$ et si $K \subset L$ est séparable de degré fini, alors il existe $\theta \in L$ tel que $L = K(\theta)$.

Si $n = 0$, il n'y a rien a démontrer (il suffit de prendre $\theta = 1$). Si $n = 1$, le résultat est trivial. Le cas $n = 2$ est celui qu'on a démontré dans la question précédente.

Soit $n \geqslant 2$ tel que le résultat soit vrai pour toute extension séparable de degré fini $K \subset K(\alpha_1, \dots, \alpha_n)$. Soit $K \subset L$ une extension séparable de degré fini, telle qu'il existe $\alpha_1, \dots, \alpha_{n+1}$ tels que $L = K(\alpha_1, \dots, \alpha_{n+1})$.

On a donc $L = K(\alpha_1, \dots, \alpha_n)(\alpha_{n+1})$. Par hypothèse de récurrence, il existe $\lambda \in L$ tel que $K(\alpha_1, \dots, \alpha_n) = K(\lambda)$. On a alors :

$$L = K(\lambda)(\alpha_{n+1}) = K(\lambda, \alpha_{n+1}),$$

et en appliquant la question 1c, il existe $\theta \in L$ tel que $L = K(\theta)$.

D'après le principe de récurrence, pour toute extension séparable de degré fini du type $K \subset L = K(\alpha_1, \dots, \alpha_n)$, il existe θ tel que $\boxed{L = K(\theta)}$.

(e) Il reste à montrer que si $K \subset L$ est une extension déparable de degré fini, on peut trouver une famille finie $(\alpha_1, \dots, \alpha_n)$ d'éléments de L tels que $L = K(\alpha_1, \dots, \alpha_n)$.

Il suffit pour cela de considérer une K-base $(\alpha_1, \dots, \alpha_n)$ de L. En effet,

$$K(\alpha_1, \dots, \alpha_n) \subset L = \mathrm{Vect}(\alpha_1, \dots, \alpha_n) \subset K(\alpha_1, \dots, \alpha_n),$$

d'où l'égalité voulue.

On applique la question précédente pour conclure : pour toute extension séparable $K \subset L$ de degré fini, il existe $\theta \in L$ tel que $\boxed{L = K(\theta)}$ (on dit que l'extension est simple).

2. Soit $\alpha = \sqrt{2}$ et $\beta = \sqrt{3}$. Puisque $\sqrt{2}$ et $\sqrt{3}$ sont irrationnels, leurs polynômes irréductibles sont au moins de degré 2. On en déduit que $P_\alpha = X^2 - 2$ et $P_\beta = X^2 - 3$. Le corps de décomposition de $P_\alpha P_\beta$ est inclus dans $\mathbb{R}$, et dans ce corps, P_α a deux racines $\sqrt{2}$ et $-\sqrt{2}$, tandis que P_β en a également deux, $\sqrt{3}$ et $-\sqrt{3}$. On a donc, avec les notations précédentes, $r = s = 2$, $\alpha_2 = -\sqrt{2}$ et $\beta_2 = -\sqrt{3}$. En suivant l'argument des questions 1(a) et 1(b), on choisit t distinct de $\frac{\alpha - \alpha_2}{\beta_2 - \beta} = -\frac{\sqrt{2}}{\sqrt{3}}$. Par exemple $t = 1$ convient. La question 1(c) donne alors :

$$\boxed{\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}).}$$

Comme on le voit, on a beaucoup d'autres possibilités pour définir θ.

3. C'est une question classique, qu'on a déjà traitée dans un DM. On ne fait qu'en esquisser l'argument. On renvoie au DM en question pour plus de détails.

Le premier argument est un résultat classique sur l'exposant d'un groupe abélien. Ce résultat affirme que si G est un groupe abélien d'ordre fini, et si $\omega(G)$ désigne le ppcm de l'ordre de tous les éléments de G, il existe un élément x de G d'ordre ω. Cela se montre en commençant par montrer que si x et y sont d'ordres n et m premiers entre eux, alors xy est d'ordre nm. Une façon de terminer (qui n'est pas celle du DM) est de dire que si p^α est un facteur de la décomposition primaire de $\omega(G)$, il existe un élément dont l'ordre est divisible par p^α. Une de ses puissances est alors d'ordre p^α. Ainsi, si $p_1^{\alpha_1} \dots p_n^{\alpha_n}$ est la décomposition primaire de $\omega(G)$, il existe des éléments $x_1, \dots, x_n$ d'ordres respectifs $p_1^{\alpha_1}, \dots, p_n^{\alpha_n}$. En effectuant une récurrence à partir du cas d'un produit de deux termes, on obtient alors que $x_1 \dots x_n$ est d'ordre $\omega(G)$

On applique ce résultat au groupe abélien $(L^*, \times)$. On note $\omega = \omega(L^*)$. Soit $P = X^\omega - 1$. Par définition de ω, pour tout $x \in K^*$, l'ordre de x divise ω, donc $x^\omega = 1$, donc x est racine de P. Ainsi, $X^\omega - 1$ admet tout élément de L^* comme racine de P. Soit $n = |L^*|$. Le polynôme P ayant n racines distinctes, il est de degré au moins n, donc $\omega \geqslant n$.

Par ailleurs, l'ordre de tout élément x de L^* divise n d'après le théorème de Lagrange, donc ω divise n, donc $\omega \leqslant n$.

On en déduit que $\omega = n$. D'après le premier argument, il existe donc $\theta \in L^*$ d'ordre n. Ainsi, $\langle \theta \rangle = L^*$, donc $\boxed{L^* \text{ est cyclique.}}$

4. Soit $K \subset L$ une extension séparable de degré fini. tel que K soit un corps fini. En fait, l'hypothèse de séparabilité est ici inutile. L étant un K-ev de dimension finie, la donnée d'une base de cardinal n permet d'obtenir un

système de coordonnée définissant une bijection de K^n sur L. Ainsi, $|L| = |K|^n$, donc L est un corps fini. On peut donc appliquer le résultat de la question précédente : L^* est un groupe cyclique. Soit θ tel que $\langle\theta\rangle = L^*$. On a alors clairement $\boxed{K(\theta) = L.}$

Question subsidiaire (hors barême)

- Si K est de caractéristique nulle, tout polynôme irréductible est séparable (IV-2). Donc toute extension algébrique est séparable, donc $\boxed{K \text{ est parfait}}$.
- Si K est de caractéristique $p \neq 0$ et $K = \{a^p, a \in K\}$. Soit $K \subset L$ une extension algébrique et $\alpha \in L$. Soit $P = P_\alpha$ le polynôme irréductible de α.
  Si $P' \wedge P \neq 1$, comme P est irréductible, on a nécessairement $P' \wedge P = P$, donc P divise P', ce qui n'est possible que si $P' = 0$. Soit $P = \sum\limits_{k=0}^{d} a_k X^k$. On a
  $$P' = \sum_{k=1}^{d} k a_k X^{k-1}.$$
  On a $P' = 0$ si et seulement si $ka_k = 0$ pour tout $k \in [\![0, d]\!]$. Puisque k est inversible dans $\mathbb{F}_p$ (donc dans K) si et seulement si k n'est pas divisible pas p (et si k est divisible par p, $ka_k = 0$), on en déduit que $P' = 0$ si et seulement si pour tout k non divisible par p, $a_k = 0$.
  Ainsi, $P' \wedge P \neq 1$ si et seulement si P n'est constitué que de monômes de degré divisible par p.
  D'après IV-1(b), P est donc inséparable si et seulement P s'écrit sous la forme
  $$P = \sum_{k=0}^{m} b_k X^{kp},$$
  donc si et seulement s'il existe un polynôme Q tel que $P = Q(X^p)$.
  On en déduit que Q est polynôme annulateur de a^p.
  Or, considérons l'application $\varphi : K \to K$ définie par $\varphi(x) = x^p$ est alors surjective. De plus, puisque $\binom{p}{k} = 0$ lorsque $k \in [\![1, p-1]\!]$, la formule du binôme permet d'établir que $\varphi(x + y) = \varphi(x) + \varphi(y)$. Enfin de façon évidente, $\varphi(xy) = \varphi(x)\varphi(y)$ et $\varphi(1) = 1$. Ainsi, φ est un morphisme de corps (appelé morphisme de Forbenius), donc en particulier injectif.
  On en déduit que φ est un isomorphisme de corps. Avec les notations de la partie III, et P_φ est irréductible. De plus, φ se prolonge en un morphisme $\tilde{\varphi}$ défini de la même façon de L dans L (on perd en revanche la surjectivité). On a alors
  $$P_\varphi(\alpha^p) = \tilde{\varphi}(P(\alpha)) = \tilde{\varphi}(0) = 0.$$
  Ainsi, P_φ est le polynôme irréductible de α^p, et il est de même degré que P. Cela contredit le fait que Q de degré strictement plus petit que P annule α.
  Ainsi, le polynôme irréductible de tout $\alpha \in K$ est séparable donc $K \subset L$ est séparable. Ceci étant vrai pour toute extension algébrique, $\boxed{K \text{ est parfait.}}$
- Réciproquement, si K est parfait de caractéristique non nulle p, le morphisme de Frobenius ci-dessus peut toujours être défini, et est injectif, comme tout morphisme de corps. Il s'agit de montrer sa surjectivité. Si ce n'est pas le cas, il existe un élément α qui n'est pas dans l'image de φ, c'est-à-dire tel que pour tout $\beta \in K$, $\beta^n \neq \beta$. Considérons un tel α, et adaptons l'argument de IV-3, en considérant $P = X^p - \alpha$. Ce polynôme n'admet pas de racine dans K, vu le choix de α. Dans un corps de décomposition L, il admet par le même argument qu'en IV-3, une racine unique θ. Cette racine n'est pas élément de K, son polynôme irréductible est donc de degré au moins 2, et divise P. Ainsi, il admet une unique racine θ, d'ordre de multiplicité au moins 2. Ainsi, P_θ est inséparable dans $K(\theta)$. Par ailleurs, θ étant algébrique, $K(\theta)$ est de dimension finie (voir III-9). Ainsi, l'extension $K \subset K(\theta)$ est de dimension finie, donc algébrique, et elle n'est pas séparable, puisque le polynôme irréductible de θ n'est pas séparable. Cela contredit le fait que K est parfait.
  Ainsi, si K est parfait de caractéristique non nulle, $\boxed{\text{le morphisme de Frobenius est un isomorphisme}}$.