

DM n° 17 : Polynômes

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

Problème 1 – Théorème de d'Alembert-Gauss

Nous donnons dans ce problème deux preuves du théorème de d'Alembert-Gauss, l'une essentiellement analytique, l'autre essentiellement algébrique (mais reposant sur une propriété analytique simple : l'analyse semble incontournable dans ce théorème).

Partie I – Démonstration analytique

Soit $P = \sum_{k=0}^n a_k X^k$ un polynôme de $\mathbb{C}[X]$, qu'on suppose unitaire (sans perte de généralité), et non constant. Montrer le théorème de d'Alembert Gauss revient à montrer l'existence d'une racine de P .

- Montrer que $|P(z)| \rightarrow +\infty$ lorsque $|z| \rightarrow +\infty$ ($z \in \mathbb{C}$).

On peut donc considérer $M > 0$ tel que pour tout $z \in \mathbb{C}$, $|z| \geq M \implies |P(z)| > |P(0)|$.

- Justifier que le sous-ensemble $\overline{B}(0, M)$ de \mathbb{C} est compact (c'est-à-dire qu'il vérifie la propriété de Bolzano-Weierstrass).
- Justifier que $|P|$ admet un minimum sur $\overline{B}(0, M)$.

Notre but est de montrer que $P(z_0) = 0$. Pour cela, on raisonne par l'absurde en supposant que ce n'est pas le cas.

On note $z_0 \in \overline{B}(0, M)$ un point en lequel $|P|$ atteint son minimum sur cet ensemble. et on fait un changement de variable permettant de centrer le minimum : on considère Q le polynôme $Q(X) = P(z_0 + X)$, et on pose (b_k) ses coefficients :

$$Q(X) = \sum_{k=0}^n b_k X^k.$$

On note $\ell = \inf\{k \in \mathbb{N}^ \mid b_k \neq 0\}$. Ainsi,*

$$Q(X) = b_0 + \sum_{k=\ell}^n b_k X^k.$$

Enfin, on pose c une racine ℓ -ième de $-\frac{b_0}{b_\ell}$.

- Justifier que $b_0 \neq 0$
- On pose f la fonction définie sur \mathbb{R} par $f(t) = \left| \frac{Q(te)}{b_0} \right|$. Montrer qu'il existe $\eta > 0$ tel que pour tout $t \in]0, \eta[$, $|f(t)| < 1$.
- En déduire une contradiction et conclure.

Partie II – Corps de décomposition d'un polynôme

Soit \mathbb{K} un corps, et P un polynôme de $\mathbb{K}[X]$. On veut montrer l'existence d'un corps \mathbb{K}' contenant \mathbb{K} tel que P soit scindé dans $\mathbb{K}'[X]$. Si \mathbb{K}' est minimal pour cette propriété, on dit que \mathbb{K}' est un corps de décomposition de \mathbb{K} .

Soit Q un facteur irréductible (dans $\mathbb{K}[X]$) de P . On note (Q) l'idéal principal de $\mathbb{K}[X]$ engendré par Q , et on note $\mathbb{K}_1 = \mathbb{K}[X]/(Q)$ le quotient de $\mathbb{K}[X]$ par l'idéal (Q) (cela se comprend au sens d'un quotient de groupe).

1. Justifier que les lois $+$ et \times de $\mathbb{K}[X]$ passent au quotient et que les lois quotients définissent sur \mathbb{K}_1 une structure de corps.
2. Soit $\varphi : \mathbb{K}[X] \rightarrow \mathbb{K}_1$ la projection canonique. Montrer que φ est un morphisme d'anneau, et que sa restriction à \mathbb{K} est injective.
Ainsi, on peut identifier \mathbb{K} à son image $\Phi(\mathbb{K}) \subset \mathbb{K}_1$. Via cette identification, on peut considérer que $\mathbb{K} \subset \mathbb{K}_1$.
3. En considérant $\theta = \varphi(X)$, montrer que P , vu comme polynôme de $\mathbb{K}_1[X]$, admet une racine dans \mathbb{K}_1 .
4. En raisonnant par récurrence, montrer l'existence d'un corps \mathbb{K}_2 contenant \mathbb{K} dans lequel P est scindé.
5. Montrer l'existence d'un sous-corps minimal de \mathbb{K}_2 contenant \mathbb{K} , dans lequel P est scindé.

Partie III – Polynômes symétriques

Soit $\mathbb{K}[X_1, \dots, X_n]$ l'anneau des polynômes à n indéterminées à coefficients dans \mathbb{K} , qui peut se définir récursivement par

$$\mathbb{K}[X_1, \dots, X_n] = \mathbb{K}[X_1, \dots, X_{n-1}][X_n].$$

Les éléments de $\mathbb{K}[X_1, \dots, X_n]$ s'écrivent de façon unique comme combinaison linéaire de monômes $X_1^{\alpha_1} \dots X_n^{\alpha_n}$.

Soit $P \in \mathbb{K}[X_1, \dots, X_n]$. On dit que P est symétrique si pour tout $\sigma \in \mathfrak{S}_n$, on a :

$$P(X_1, \dots, X_n) = P(X_{\sigma(1)}, \dots, X_{\sigma(n)}).$$

On définit les polynômes symétriques élémentaires :

$$\Sigma_k = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} X_{i_1} X_{i_2} \dots X_{i_k}.$$

Le but de cette partie est de montrer que l'ensemble S des polynômes symétriques de $\mathbb{K}[X_1, \dots, X_n]$ est le sous-anneau de $\mathbb{K}[X_1, \dots, X_n]$ engendré par les polynômes symétriques élémentaires.

1. Montrer que S est un sous-anneau de $\mathbb{K}[X_1, \dots, X_n]$.
2. Pour $P \in \mathbb{K}[X_1, \dots, X_n]$, on note $\text{MD}(P)$ le monôme directeur de P , égal au monôme $aX_1^{\alpha_1} \dots X_n^{\alpha_n}$ de la décomposition de P pour lequel $(\alpha_1, \dots, \alpha_n)$ est maximal pour l'ordre lexicographique.

Montrer que si P est un polynôme symétrique, alors

$$\text{MD}(P) = aX_1^{\alpha_1} \dots X_n^{\alpha_n} \implies \alpha_1 \geq \dots \geq \alpha_n.$$

3. Montrer que pour tout $P, Q \in \mathbb{K}[X_1, \dots, X_n]$, $\text{MD}(PQ) = \text{MD}(P)\text{MD}(Q)$.
4. Soit $\alpha_1 \geq \dots \geq \alpha_n$ des entiers naturels. Montrer que

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

5. En raisonnant par récurrence sur $(\alpha_1, \dots, \alpha_n)$ le n -uplet des exposants du monôme directeur de P , montrer que tout polynôme symétrique s'écrit comme combinaison linéaire de produits de polynômes symétriques élémentaires, et conclure. On pourra considérer l'ordre lexicographique sur les n -uplets $(\alpha_1, \dots, \alpha_n)$, et on justifiera la validité de la « récurrence » ainsi faite sur l'ordre lexicographique.

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

On montre dans cette partie qu'un polynôme de degré impair strictement supérieur à 1 n'est pas irréductible. On rappelle que pour tout corps \mathbb{K} , l'anneau $\mathbb{K}[X]$ est principal, et on admettra que cela implique que $\mathbb{K}[X]$ est factoriel, donc que tout polynôme de $\mathbb{K}[X]$ se décompose de façon unique (à inversibles près, et à l'ordre près des facteurs) comme produit de polynômes irréductibles.

- Soit $P \in \mathbb{R}[X]$ de degré impair. Montrer que P admet une racine réelle.

On considère $P \in \mathbb{C}[X]$ de degré impair $n = 2p + 1 > 1$.

$$\text{Si } P = \sum_{k=0}^n a_k X^k, \text{ on note } \bar{P} = \sum_{k=0}^n \bar{a}_k X^k.$$

On suppose que P est unitaire et irréductible, et on pose $Q = P\bar{P}$.

- Justifier que $P \notin \mathbb{R}[X]$ et $Q \in \mathbb{R}[X]$.
- Montrer que Q est irréductible dans $\mathbb{R}[X]$

Soit \mathbb{K} un corps de décomposition de Q sur \mathbb{C} , et $\alpha_1, \dots, \alpha_{2n}$ les racines de Q (non nécessairement distinctes) dans \mathbb{K} . On définit le polynôme R par :

$$R = \prod_{1 \leq i < j \leq 2n} (X - (\alpha_i + \alpha_j)).$$

- En remarquant que les coefficients de R sont symétriques en les α_i , montrer que $R \in \mathbb{R}[X]$.

- Montrer que R admet une racine r dans \mathbb{R} . On définit :

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

Montrer que $S = T$. En déduire l'existence de $U \in \mathbb{R}[X]$ tel que $S(X) = U(X^2)$

- En déduire l'existence d'une racine α de P et conclure.

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

- Soit P un polynôme de $\mathbb{C}[X]$, et $\alpha_1, \dots, \alpha_n$ ses racines (non nécessairement distinctes) dans un corps de décomposition \mathbb{K} de P . On considère comme ci-dessus

$$R = \prod_{1 \leq i < j \leq n} (X - (\alpha_i + \alpha_j)).$$

Justifier que $R \in \mathbb{C}[X]$, et qu'il existe un polynôme irréductible Q divisant R et dont la valuation 2-adique du degré est strictement inférieure à la valuation 2-adique de degré de P .

- Montrer le théorème de d'Alembert-Gauss par récurrence sur la valuation 2-adique du degré de P , en adaptant la preuve de la partie IV.

Problème 2 – (Théorème de l'élément primitif)

Le but de ce problème est d'étudier des propriétés des extensions de corps. Une extension d'un corps K est la donnée d'un corps L et d'un morphisme de corps $K \rightarrow L$. D'après le cours, ce morphisme est nécessairement injectif, donc son image est un sous-corps de L , isomorphe à K . Quitte à identifier K et son image, si $K \rightarrow L$ est une extension du corps K , on peut toujours considérer que K est un sous-corps de L . Dans le problème, cette identification sera faite systématiquement, et à chaque fois qu'on construira une extension de corps $K \rightarrow L$, on considérera K comme un sous-corps de L ; en particulier, les éléments de K seront considérés comme des éléments de L aussi.

Nous commençons par montrer, étant donné un polynôme P de $K[X]$, l'existence d'une extension L de K minimale, unique à isomorphisme près, telle que P soit scindé sur L . Une telle extension L est appelée corps de décomposition de P .

Le but ultime du problème est de montrer le théorème de l'élément primitif, affirmant que sous certaines hypothèses, une extension L de K est engendrée par un unique élément, dans le sens où il existe α dans L tel que $L = K(\alpha)$, $K(\alpha)$ étant le plus petit sous-corps de L contenant tous les éléments de K et α .

Partie I – Extensions de degré fini.

Soit $K \subset L$ une extension du corps K . On dit qu'un élément α du corps L est algébrique sur K s'il existe un polynôme $P \neq 0$ à coefficients dans K ($P \in K[X]$) tel que $P(\alpha) = 0$. On dit que l'extension $K \subset L$ est algébrique si tout élément α de L est algébrique sur K .

On rappelle que L est muni d'une structure de K -espace vectoriel. Si L est de dimension finie sur K , on dira que l'extension $K \subset L$ est de degré fini $\dim_K(L)$. Cette dimension sera notée $[L : K]$ (degré de L sur K)

1. Montrer que si $K \subset L$ et $L \subset M$ sont deux extensions de degré fini, alors $K \subset M$ est aussi de degré fini, et $[M : K] = [M : L] \times [L : K]$
Indication : considérer la famille $(a_i b_j)$, où (a_i) est une base de L sur K et (b_j) une base de M sur L .
2. Montrer que si l'extension $K \subset L$ est de degré fini, alors elle est algébrique.
3. Soit $K \subset L$ une extension de degré fini. Montrer que pour tout $\alpha \in L$, il existe un unique polynôme unitaire irréductible $P_\alpha \in K[X]$ tel que α soit racine de P_α . Le polynôme P_α est appelé polynôme minimal de α , ou polynôme irréductible de α sur K .

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

Dans cette partie, on considère K un corps, et $K \rightarrow L$ une extension de K . Suivant les conventions données dans l'introduction, on considère que $K \subset L$. On définit, pour toute partie E de L , $K(E)$ le plus petit sous-corps de L tel que $K \cup E \subset K(E)$, si un tel corps existe. Pour alléger les notations, on notera par la suite, pour $\alpha \in L$, $K(\alpha)$ au lieu de $K(\{\alpha\})$ le plus petit sous-corps de L contenant K et α , et de même $K(\alpha_1, \dots, \alpha_n)$ au lieu de $K(\{\alpha_1, \dots, \alpha_n\})$.

1. Soit $(M_i)_{i \in I}$ une famille non vide de sous-corps de L . Montrer que $\bigcap_{i \in I} M_i$ est un sous-corps de L .
2. Soit $E \subset L$. Justifier l'existence de $K(E)$.
3. Montrer que si E et F sont deux parties de L , $K(E \cup F) = K(E)(F)$ (le plus petit sous-corps de L contenant $K(E)$ et F).

En particulier, si $\alpha_1, \dots, \alpha_n$ sont des éléments de L , on a donc $K(\alpha_1, \dots, \alpha_n) = K(\alpha_1, \dots, \alpha_{n-1})(\alpha_n)$.

4. A-t-on en général $K(\alpha) \simeq K(\beta)$, pour $\alpha, \beta \in L$ quelconques ? (on pourra chercher un contre-exemple avec des corps bien connus).
5. Soit P un polynôme irréductible sur K . On note (P) l'idéal principal engendré par P dans $K[X]$. On rappelle qu'on peut munir le quotient $K[X]/(P)$ d'une structure d'anneau.
Montrer que $K[X]/(P)$ est un corps.
6. Soit $\alpha \in L$ une racine de P . Soit $\varphi : K[X] \rightarrow L$ définie par $\varphi(Q) = Q(\alpha)$. Montrer que φ est un morphisme d'anneaux et justifier que son noyau est (P) .
7. En déduire qu'il existe un isomorphisme de corps entre $K[X]/(P)$ et $K(\alpha)$ (on dira que les deux corps sont isomorphes ; de façon générale, on notera $K \simeq K'$ pour dire que les deux corps K et K' sont isomorphes)
8. Soit α et β deux racines dans L d'un même polynôme irréductible sur K . Montrer que $K(\alpha)$ et $K(\beta)$ sont isomorphes.
9. Dans les hypothèses de la question précédente, a-t-on en général $K(\alpha) = K(\beta)$? On pourra considérer le polynôme $X^3 - 2$ de $\mathbb{Q}[X]$, après avoir justifié qu'il est irréductible sur \mathbb{Q} .

Partie III – Corps de décomposition d'un polynôme

Dans la partie précédente, on a considéré une extension minimale $K(\alpha)$ de K dans laquelle un polynôme irréductible P admet une racine α . Cette construction a été possible du fait de la donnée préalable d'un corps L dans lequel P admet une racine. Nous aimerais maintenant nous affranchir de cette donnée initiale. Pour cela, nous partons de l'observation que la question 7 donne une description de $K(\alpha)$ indépendante de L .

1. Soit P un polynôme irréductible. Montrer que l'application $i : K \rightarrow K[X]/(P)$ associant à λ la classe du polynôme constant λ est un morphisme de corps, permettant donc de considérer K comme un sous-corps de $K[X]/(P)$.
2. En considérant α la classe du polynôme X dans $K[X]/(P)$, montrer que le polynôme P admet une racine dans l'extension $K[X]/(P)$ de K .

*Si $K \subset L$ est une extension de K telle que le polynôme (irréductible ou non) $P \in K[X]$ admette une racine dans L , on dit que L est un corps de rupture de P . On vient de démontrer que pour tout polynôme **irréductible** P , il existe une extension $K \subset L$ telle que L soit un corps de rupture du polynôme P .*

3. Justifier que pour tout $P \in K[X]$ (irréductible ou non), il existe une extension $K \subset L$ de P telle que L soit un corps de rupture de P .
4. En raisonnant par récurrence sur $\deg P$, montrer que pour tout $P \in K[X]$, il existe une extension $K \subset L$ de K telle que P soit scindé sur L .

Notant alors $\alpha_1, \dots, \alpha_r$ les racines distinctes de P , le sous-corps $M = K(\alpha_1, \dots, \alpha_r)$ de L est alors une extension de K dans laquelle P est scindé, et est clairement minimale pour cette propriété dans le sens où pour toute extension $K \subset M' \subset M$ telle que P soit scindé sur M' , on a $M = M'$. Une telle extension M , sur laquelle P est scindé, et minimale pour cette propriété, est appelée corps de décomposition de P . Le but de la fin de cette partie est de justifier l'unicité (à isomorphisme près) de deux corps de décomposition d'un polynôme P .

Soit $\lambda : K \rightarrow K'$ un isomorphisme entre deux corps K et K' . On définit $\widehat{\lambda} : K[X] \rightarrow K'[X]$ par $\widehat{\lambda}(P) = P_\lambda$, où, pour $P = \sum_{k=0}^d a_k X^k$, P_λ est défini par $P_\lambda = \sum_{k=0}^d \lambda(a_k) X^k$.

5. Montrer que $\widehat{\lambda}$ est un isomorphisme d'anneaux.
6. Montrer que si $P \in K[X]$ est irréductible, il en est de même de P_λ , et que les corps $K[X]/(P)$ et $K'[X]/(P_\lambda)$ sont isomorphes.
- *7. En raisonnant par récurrence sur $\deg P$, montrer que pour tout polynôme $P \neq 0$ (sur n'importe quel corps K), pour tout isomorphisme $\lambda : K \rightarrow K'$, pour 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 $\alpha_1, \dots, \alpha_r$ les racines distinctes de P dans L et β_1, \dots, β_s les racines distinctes de P_λ dans L' , le sous-corps $K(\alpha_1, \dots, \alpha_r)$ de L et le sous-corps $K'(\beta_1, \dots, \beta_s)$ de L' sont isomorphes.

Indication : on pourra commencer par comparer $K(\alpha_1)$ et $K'(\beta_1)$, en supposant que α_1 et β_1 sont racines de facteurs irréductibles Q et R de P et P_λ respectivement, se correspondant via λ (c'est-à-dire tels que $R = Q_\lambda$).

8. En déduire que deux corps de décomposition de P sont isomorphes.

**9. [Cette question n'est pas utile pour la suite]

Soit $K \subset L$ une extension de corps. Montrer que L est le corps de décomposition d'un polynôme P de $K[X]$ si et seulement si L est de degré fini, et si tout polynôme irréductible P de $K[X]$ ayant une racine dans L est scindé dans L .

Indications :

- Pour le sens direct, si L est corps de rupture de P , et si Q est un polynôme irréductible ayant une racine dans L , considérer une extension $L \subset M$ telle que M soit corps de décomposition du polynôme PQ ,
- pour la réciproque, écrire $L = K(\alpha_1, \dots, \alpha_n)$ et considérer un corps de décomposition M du produit des polynômes minimaux des α_i . Notant β et γ deux racines de Q dans M , comparer $[L(\beta) : K(\beta)]$ et $[L(\gamma) : K(\gamma)]$ puis $[L(\beta) : L]$ et $[L(\gamma) : L]$.

Partie IV – Extensions séparables

Un polynôme irréductible $P \in K[X]$ est dit séparable lorsque ses racines dans un corps de décomposition de P sont deux à deux distinctes. Il est dit inséparable sinon.

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 $Q \in L[X]$. Montrer que $X - \alpha$ divise Q .
 - (b) En déduire que P est inséparable si et seulement si $P \wedge P' \neq 1$ (on prendra garde au fait que la caractéristique de K est quelconque).

Ainsi, en contraposant, un polynôme non constant P est séparable si et seulement si $P \wedge P' = 1$. On remarquera que cette caractérisation ne dépend pas de L (ou même plus généralement d'une extension dans laquelle P est scindé).

2. Montrer que si K est de caractéristique nulle, tout polynôme irréductible P est séparable. Montrer que si K est de caractéristique finie, un polynôme irréductible P 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) Justifier qu'il existe une extension $\mathbb{F}_p \subset K$ et un élément t de K tel que t ne soit pas algébrique sur \mathbb{F}_p (on pourra considérer $K = \mathbb{F}_p(X)$)
 - (b) Soit $P = X^p - t \in K[X]$, et α une racine de P dans un corps de décomposition L de P . Montrer que $P = (X - \alpha)^p$.
 - *(c) Montrer que si P n'est pas irréductible sur K , $\alpha \in K$.
 - *(d) Montrer que P est un polynôme irréductible inséparable.

Indication : montrer que l'appartenance de α à K entre en contradiction avec la transcendance de t ; on pourra pour cela justifier l'existence de $F \in \mathbb{F}_p(X)$ tel que $\alpha = F(t)$.

Soit $K \subset L$ une extension de corps. On dit qu'un élément α de L est séparable sur K s'il est algébrique et si son polynôme irréductible (ou minimal) P_α est séparable sur K . On dit que l'extension $K \subset L$ est séparable si tout élément de α est séparable sur K .

4. Soit $K \subset L \subset M$ deux extensions de corps.

- (a) Soit $\alpha \in M$, algébrique sur K . Justifier que α 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 . Montrer que Q_α divise P_α dans $L[X]$.
- (c) Montrer que si $K \subset M$ est séparable, alors $K \subset L$ et $L \subset M$ sont séparables.

Partie V – Théorème de l'élément primitif

On montre dans cette partie le théorème de l'élément primitif. Ce théorème affirme que si $K \subset L$ est une extension séparable de degré fini, alors il existe $\theta \in L$ tel que $L = K(\theta)$ (on dit que l'extension est simple).

On se donne donc dans cette partie une extension $K \subset L$ séparable de degré fini. On note $n = \dim_K(L) = [L : K]$.

1. On suppose dans un premier temps que K est de cardinal infini.

- (a) On traite pour commencer le cas où il existe deux éléments α et β tels que $L = K(\alpha, \beta)$. Après avoir justifié l'existence de polynômes irréductibles P_α et P_β de $K[X]$ annulant respectivement α et β , et en notant $\alpha, \alpha_2, \dots, \alpha_r$ et $\beta, \beta_2, \dots, \beta_s$ respectivement les racines distinctes de P_α et de P_β dans un corps M de décomposition du produit $P_\alpha P_\beta$, montrer qu'il existe $t \in K^*$ tel que pour tout $(i, j) \in \llbracket 2, r \rrbracket \times \llbracket 2, s \rrbracket$, $\alpha_i + t\beta_j \neq \alpha + t\beta$.
- (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 $H(X) = P_\alpha(\theta - tX)$. Montrer que $H \wedge P_\beta = X - \beta$
Indication : calculer ce PGCD dans $M[X]$ en déterminant les racines communes et leurs multiplicités.
- (c) En déduire que $\beta \in K(\theta)$, puis que $K(\theta) = K(\alpha, \beta) = L$.
- (d) Montrer par récurrence sur n que si $L = K(\alpha_1, \dots, \alpha_n)$, il existe $\theta \in L$ tel que $L = K(\theta)$
- (e) Terminer la preuve du théorème de l'élément primitif pour K infini.

2. Trouver θ tel que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\theta)$.

- *3. Soit L un corps fini. Montrer que (L^*, \times) est un groupe cyclique.

4. En déduire le théorème de l'élément primitif lorsque K est un corps fini.

**Question subsidiaire (hors barême)

Un corps K est dit parfait si toute extension algébrique de K est séparable. Montrer que K est un corps parfait si et seulement si la caractéristique de K est nulle, ou si la caractéristique de K est égale à $p \neq 0$ et $K = \{a^p, a \in K\}$.