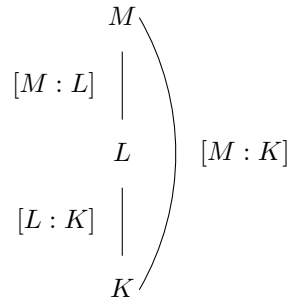
Extensions de corps. Exemples et applications.

Mohamed NASSIRI

Une extension de corps est la donnée d'un morphisme injectif de corps $i : K \to L$, où K et L sont des corps. On la note $K \subset L$. Ainsi, si K est un sous-corps de L, alors L est un K-espace vectoriel. Dans le cadre où $\dim_K L$ est finie, on définit le *degré de l'extension L sur K* par $[L : K] = \dim_K L$. A partir de là, vient le *théorème de la base télescopique*, et son corollaire dit de *la multiplicativité des dégrés* : Soit $K \subset L \subset M$ des corps, si les degrés sont finis, on a

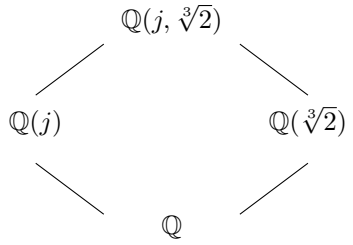
$$[M : K] = [M : L][L : K]$$

On représente souvent les extensions de corps comme le schéma ci-dessous en indiquant accessoirement les degrés des extensions.



Une approche intéressante pour chercher les racines d'un polynôme va être de regarder, pour un polynôme $P \in K[X]$, les extensions du corps K où P admet une racine. De là va émerger la notion de *corps de rupture*. Par exemple, pour $P(X) = X^3 - 2 \in \mathbb{Q}[X]$, on va se placer dans l'extension $\mathbb{Q}(\sqrt[3]{2})$ et constater que P a bien une racine dans cette extenstion (c'est $\sqrt[3]{2}$ ...) Mais manque de bol, il manque des racines ... : $j\sqrt[3]{2}$ et $\overline{j}\sqrt[3]{2} \notin \mathbb{Q}(\sqrt[3]{2})$

Précedemment, on a "cassé" notre polynôme mais pas "totalement décomposé". L'autre idée est de regarder, pour un polynôme $P \in K[X]$, une ou des extensions du corps K où P sera totalement scindé. On parle alors de *corps de décomposition*. Pour notre précédent exemple, le corps de décomposition de $X^3 - 2$ est $\mathbb{Q}(j, \sqrt[3]{2})$. Le schéma ci-contre nous montre comment sont "imbriquer" ces différents corps.



Un autre type de corps va être important : il s'agit de corps où tout polynôme est scindé. De tels corps sont appelés *corps algébriquement clos*. Le plus connu est sans doute $\mathbb{C}$, ce qui constitue l'énoncé du célèbre théorème de D'Alembert-Gauss.

Comme nous l'avons vu, un corps de décomposition est a priori différent d'un corps de rupture comme on a pu le voir par l'exemple précédent. Cependant, pour les corps finis, cette notion coïncide ... On obtient ce résultat en démontrant l'existence et l'unicité des corps finis à partir des corps de décomposition.

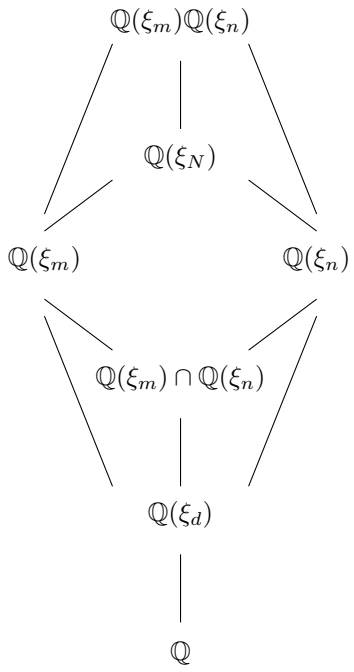
Un cas particulier mérite notre attention : il s'agit de l'étude des polynômes et des corps cyclotomiques. On sait totalement caractériser ces derniers et on comprend même ce qu'il se passe quand on "intersecte" deux corps cyclotomiques. Plus précisement, on a que si le polynôme minimal sur $\mathbb{Q}$ de toute racine primitive n-ième de l'unité est $\Phi_{n,\mathbb{Q}}(X)$. Alors

$$[\mathbb{Q}(\mathbb{U}_n) : \mathbb{Q}] = \varphi(n)$$

et si pour m et n des entiers naturels non nuls, on pose N=ppcm(m,n), d=pgcd(m,n) et pour tout $t \in \mathbb{N}^*$, on désigne par ξ_t une racine primitive t-ième de l'unité. Alors on a

$$\mathbb{Q}(\xi_m)\mathbb{Q}(\xi_n) = \mathbb{Q}(\xi_N)$$
$$\mathbb{Q}(\xi_m) \cap \mathbb{Q}(\xi_n) = \mathbb{Q}(\xi_d)$$

Ce qui simplifie pas mal le diagramme ci-contre ...



Références

[ML3al] Mathématiques L3 Algèbre, Aviva Szpirglas
[GOZ] Théorie de Galois, Ivan Gozard ♠
[PER] Cours d'Algèbre, Daniel Perrin ♠
[OTZ] Exercices d'algèbre, Pascal Ortiz

Développements

Existence et unicité des corps finis
Théorème de Wedderburn

1 Généralités

1.1 Définitions et premières propriétés [PER] p.65-66

Définition 1 *Une extension de corps est la donnée d'un morphisme injectif de corps $i : K \to L$, où K et L sont des corps. Notation : $K \subset L$.* **[ML3al] p.713**

Exemple 2 $\mathbb{Q} \subset \mathbb{R}$ *et* $\mathbb{R} \subset \mathbb{C}$.

Remarque 3 *Si K est un sous-corps de L, alors L est un K-espace vectoriel.*

Définition 4 *Si $\dim_K L$ est finie, on définit le degré de l'extension L sur K par $[L : K] = \dim_K L$.*

Remarque 5 *Si K et L sont des corps finis, on a $|L| = |K|^{[L:K]}$.*

Théorème 6 *Théorème de la base télescopique Soient $K \subset L \subset M$ des corps, $(e_i)_{i\in I}$ une base de L sur K et $(f_j)_{j\in J}$ une base de M sur L. Alors la famille $(e_i f_j)_{(i,j)\in I\times J}$ est une base de M sur K.*

Corollaire 7 *Multiplicativité des dégrés Dans la situation du théorème précédent, si les degrés sont finis, on a*

$$[M : K] = [M : L][L : K]$$

Définition 8 *Soient $K \subset L$ une extension et A une partie de L. On dit que A engendre L sur K et on note L=$K(A)$ si L est le plus petit sous-corps de L contenant K et A.*
Si A est fini avec $A = \{\alpha_1, ..., \alpha_n\}$, on note L=$K(\alpha_1, ..., \alpha_n)$.
L'extension $K \subset L$ est dite monogène s'il existe $\alpha \in L$ tel que $L = K(\alpha)$

Exemple 9 $\mathbb{Q} \subset \mathbb{Q}(i)$ *et* $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$

1.2 Extensions algébriques et transcendantes [GOZ] p.30 → 33

Définition 10 *Soit K un corps, et L une extension de K. Pour $a \in L$, on considère le morphisme de K-algèbres suivant :*

$$ev_a : K[X] \to L$$
$$P(X) \mapsto P(a)$$

- Si ev_a est injective, a est dit algébrique sur K,
- Sinon, a est dit transcendant sur K

Théorème 11 *Si a est transcendant :*
(i) L'application

$$\widetilde{ev_a} : K(X) \to K(a)$$
$$f(X) = \frac{P(X)}{Q(X)} \mapsto f(a) = P(a)Q(a)^{-1}$$

est un ismorphisme de K-algèbres.
(ii) $[K(a) : K] = +\infty$

Remarque 12 *Pour le reste de cette partie, on suppose que a est algébrique.*

Définition 13 *K[X] étant principal,* $\mathrm{Ker}(ev_a)$ *est un idéal principal de K[X] engendré par un unique polynôme* $\pi_{a,K}(X) \in K[X]$ *appelé polynôme minimal de a sur K.*

Proposition 14 *(i) Soit* $P(X) \in K[X]$. *(P est le polynôme minimal de a)* $\Leftrightarrow$ *(P(X) est unitaire, P(a)=0 et pour tout polynôme* $R(X) \in K[X]\backslash\{0\}$ *vérifiant R(a)=0, on a* $\deg(P) \leq \deg(R)$*).*
(ii) Soit $P(X) \in K[X]$. *(P est le polynôme minimal de a)* $\Leftrightarrow$ *(P(X) est unitaire, P(a)=0 et le polynôme P(X) est irréductible dans K[X]).*

Exemple 15 *Soient* $n \in \mathbb{N}^*$ *et* $\alpha = 2^{1/n}$. *On a* $\pi_{\alpha,\mathbb{Q}}(X) = X^n - 2$.

Proposition 16 *En notant* $m = \deg(\pi_{a,K}(X))$, *alors la famille* $(a^i)_{i\in[\![0,m-1]\!]}$ *est une base de K[a] en tant que K-e.v.*

Proposition 17 *(i) K(a)=K[a]*
(ii) Soit L une extension de K. Si $a \in L^*$ *est algébrique sur K, alors* $a^{-1} \in K[a]$
(iii) L'application

$$K(X)/(\pi_{a,K}(X)) \to K(a)$$
$$\overline{P(X)} \mapsto P(a)$$

est un ismorphisme de K-algèbres.

2 Polynômes irréductibles et extension de corps : adjonction de racines

2.1 Corps de rupture [GOZ] p.57→ 59

Définition 18 *Soient K un corps et* $P \in K[X]$ *un polynôme irréductible dans K[X]. On dit que le corps L est un corps de rupture de P si et seulement si L est une extension simple de K engendré par K et une racine, notée* α, *de P.*

Exemple 19 $\mathbb{Q}(\sqrt[3]{2})$ *est un corps de rupture de* $P(X) = X^3 - 2$.

Théorème 20 *Soient K un corps et* $P \in K[X]$ *un polynôme irréductible dans K[X].*
(i) Il existe un corps de rupture de P.
(ii) Si $L = K(\alpha)$ *et* $L' = K(\beta)$ *sont deux corps de rupture de P, alors L et L' sont K-isomorphes*

Corollaire 21 *Soient K un corps et* $P \in K[X]$ *un polynôme de degré* $n \geq 1$. *Il existe une extension algébrique simple L de K dans laquelle P possède (au moins) une racine.*

Proposition 22 *Soit* $P \in K[X]$ *un polynôme de degré* $n \geq 1$. *P(X) est irréductible dans K[X] si et seulement si P(X) n'a pas de racine dans les extensions L de K telles que* $[L : K] \leq n/2$.

Exemple 23 X^4+X+1 *est irréductible sur* $\mathbb{F}_2$ *car il n'a pas de racines dans* $\mathbb{F}_2$, *ni* $\mathbb{F}_4$.

Proposition 24 *Soient* $P \in K[X]$ *un polynôme irréductible de degré* $n \geq 1$ *et L une extension de degré m de K avec pgcd(m,n)=1. Alors P(X) est irréductible dans L[X].*

Exemple 25 $X^3 + X + 1$ *est irréductible sur* $\mathbb{Q}(i)$ *comme sur* $\mathbb{Q}$.

2.2 Corps de décomposition [GOZ] p.59-60

Théorème 26 *Soient K un corps, E une extension de K et* $P \in K[X]$ *un polynôme de degré* $n \geq 1$. *On dit que E est un corps de décomposition de P sur K si et seulement si :*
(i) $\exists a \in E$ *et* $(\alpha_1, ..., \alpha_n) \in E^n$ *tel que, dans E[X],* $P(X) = a(X - \alpha_1)...(X - \alpha_n)$
(ii) $E = K(\alpha_1, ..., \alpha_n)$

Exemple 27 • $\mathbb{C} = \mathbb{R}(i)$ *est le corps de décomposition sur* $\mathbb{R}$ *de* $X^2 + 1$
• $\mathbb{Q}(\sqrt{2})$ *est le corps de décomposition sur* $\mathbb{R}$ *de* $X^2 - 2$

Théorème 28 (admis) *Soient K un corps et* $P \in K[X]$ *un polynôme de degré* $n \geq 1$.
(i) Il existe un corps de décomposition Σ *de P sur K, avec* $[\Sigma : K] \leq n!$
(ii) Si Σ *et* Σ' *sont deux corps de décomposition de P sur K, alors ils sont K-isomorphes*

2.3 Corps algébriquement clos [GOZ] p.62-63

Proposition-Définition 29 *Soit K un corps. Les conditions suivantes sont équivalentes :*
(i) Tout polynôme de degré ≥ 1 *de K[X] est scindé sur K ;*
(ii) Tout polynôme de degré ≥ 1 *de K[X] admet au moins une racine dans K ;*
(iii) Les seuls polynômes irréductibles de K[X] sont

ceux de degré 1 ;
(iv) Toute extension algébrique de K est identique à K lui-même.
On dit alors que K est algébriquement clos.

Exemple 30 *$\mathbb{Q}$ et $\mathbb{R}$ ne sont pas algébriquement clos*

Proposition 31 *Tout corps algébriquement clos est infini.*

Théorème 32 *Théorème de D'Alembert-Gauss :* *$\mathbb{C}$ est algébriquement clos.*

Corollaire 33 • *Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.*
• *Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 qui n'ont pas de racine réelle.*

3 Cyclotomie et extension de corps [GOZ] p.67 → 69

Proposition-Définition 34 *Soit $m \in \mathbb{N}^*$. L'ensemble $\mathbb{U}_m = \{z \in \mathbb{C} \mid z^m = 1\}$ des racines m-ièmes de l'unité dans $\mathbb{C}$.*
$\mathbb{U}_m$ est un groupe cyclique d'ordre m.
On appelle racine primitive m-ièmes de l'unité tout générateur de $\mathbb{U}_m$. On notera $\mathcal{P}_m(\mathbb{C})$ l'ensemble des racines primitives m-ièmes de l'unité.

Proposition 35 *$\mathcal{P}_m(\mathbb{C}) = \{\exp(2ik\pi/m),\ 1 \leq k \leq m,\ \text{pgcd}(k,m) = 1\}$ a pour cardinal $\varphi(m)$.*

Proposition 36 *Soient $m \in \mathbb{N}^*$ et ξ une racine primitive m-ièmes de l'unité dans $\mathbb{C}$. Alors les (autres) racines primitives m-ièmes de l'unité sont les ξ^k, où $1 \leq k \leq m$, $\text{pgcd}(k,m) = 1$.*

Définition 37 *Le sous-corps $\mathbb{Q}(\mathbb{U}_m)$ de $\mathbb{C}$ engendré par les racines m-ièmes de l'unité, qui est $\mathbb{Q}(\xi)$ où ξ une racine primitive m-ièmes de l'unité quelconque, est appelé corps cyclotomique d'indice m.*

Définition 38 *Soit $m \in \mathbb{N}^*$. On appelle m-ième polynôme cyclotomique le polynôme*

$$\Phi_{m,\mathbb{Q}}(X) = \prod_{\xi \in \mathcal{P}_m(\mathbb{C})} (X - \xi)$$

$\Phi_{m,\mathbb{Q}}(X)$ est un polynôme unitaire de degré $\varphi(m)$ et à coefficients dans $\mathbb{C}$.

Proposition 39 *(i)*

$$X^m - 1 = \prod_{d|m} \Phi_{d,\mathbb{Q}}(X)$$

(ii) $\forall n \in \mathbb{N}^*$, $\Phi_{n,\mathbb{Q}}(X) \in \mathbb{Z}[X]$
(iii) $\forall n \in \mathbb{N}^*$, $\Phi_{n,\mathbb{Q}}(X)$ est irréductible dans $\mathbb{Q}[X]$

Corollaire 40 *Soit $n \in \mathbb{N}^*$, le polynôme minimal sur $\mathbb{Q}$ de toute racine primitive n-ième de l'unité est $\Phi_{n,\mathbb{Q}}(X)$. Donc $[\mathbb{Q}(\mathbb{U}_n) : \mathbb{Q}] = \varphi(n)$*

Corollaire 41 *Soit α (resp. β) une racine n-ième (resp. m-ième) de l'unité. Si $\text{pgcd}(n,m) = 1$ alors $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}$.*

Théorème 42 *(Plus généralement) Soient m et n des entiers naturels non nuls. On pose N=ppcm(m,n) et d=pgcd(m,n). Pour tout $t \in \mathbb{N}^*$, on désigne par ξ_t une racine primitive t-ième de l'unité. Alors*
(i) $\mathbb{Q}(\xi_m)\mathbb{Q}(\xi_n) = \mathbb{Q}(\xi_N)$
(ii) $\mathbb{Q}(\xi_m) \cap \mathbb{Q}(\xi_n) = \mathbb{Q}(\xi_d)$
Voir Figure 1.

4 Corps finis [GOZ] p.85→87

Application 43 ♠ *Théorème de Wedderburn* ♠
Tout corps fini est commutatif. **[PER] p.82**

Théorème 44 ♠ *Existence et unicité des corps finis* ♠
Soit p un nombre premier et $n \in \mathbb{N}^*$. On note $q = p^n$.
(1) *Il existe un unique corps fini à q éléments. Il est le corps de décomposition sur $\mathbb{F}_p$ de $X^q - X$. On le note $\mathbb{F}_q$*
(2) *$\mathbb{F}_q = \mathbb{F}_p[X]/(\pi)$, où π est un polynôme irréductible quelconque de degré n sur $\mathbb{F}_p$.*
(3) *Si π est un polynôme irréductible de degré n sur $\mathbb{F}_p$, alors $\pi(x) \mid X^q - X$ dans $\mathbb{F}_p[X]$, donc est scindé sur $\mathbb{F}_q$.*

Remarque 45 *L'assertion (3) se traduit par le fait que, dans les corps finis, le corps de rupture est égal au corps de décomposition.*

Exemple 46 *$\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)$.*
Comme j est racine de $X^2 + X + 1$, on a

$$\mathbb{F}_4 = \mathbb{F}_2(j) = \{0, 1, j, j^2 = 1 + j\}$$

Théorème 47 *Soit p un nombre premier et $n \in \mathbb{N}^*$. On note $q = p^n$.*
Tout corps intermédiaire $\mathbb{F}_q \subseteq K \subseteq \mathbb{F}_{q^n}$ est un corps $\mathbb{F}_{q^d}$ à q^d éléments où d est un diviseur de n et que, pour chaque diviseur d de n, il existe un unique corps intermédiaire de cardinal q^d. **[OTZ] p.141-142**

Illustrations

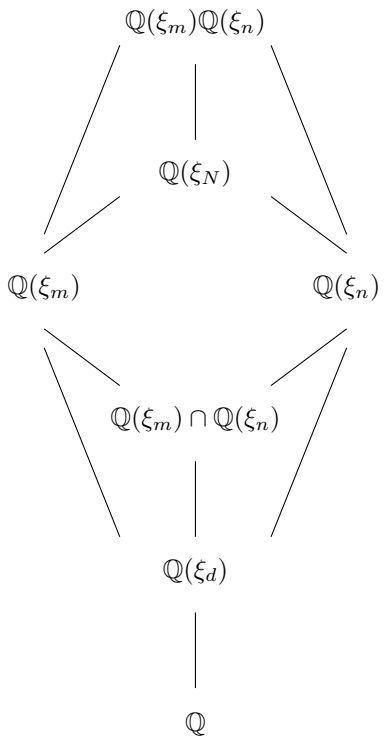


Figure 1

Questions

Exercice : Théorème de la base télescopique
Soient $K \subset L \subset M$ des corps, $(e_i)_{i\in I}$ une base de L sur K et $(f_j)_{j\in J}$ une base de M sur L.
Montrer que la famille $(e_i f_j)_{(i,j)\in I\times J}$ est une base de M sur K.

Solution : Classiquement, nous allons montrer que la famille $(e_i f_j)_{(i,j)\in I\times J}$ est libre et génératrice.

Famille libre : On suppose qu'il existe une famille $(\lambda_{ij})_{(i,j)\in I\times J}$ d'éléments de K telle que

$$\sum_{(i,j)\in I\times J} \lambda_{ij} e_i f_j = 0$$

Par suite,

$$0 = \sum_{(i,j)\in I\times J} \lambda_{ij} e_i f_j = \sum_{j\in J} f_j \underbrace{\left(\sum_{i\in I} \lambda_{ij} e_i\right)}_{\in L}$$

Or, comme $(f_j)_{j\in J}$ une base de M sur L, on en déduit que

$$\forall j \in J,\ \sum_{i\in I} \lambda_{ij} e_i = 0$$

et puis comme $(e_i)_{i\in I}$ une base de L sur K,on en déduit que

$$\forall j \in J,\ \forall i \in I\ \ \lambda_{ij} = 0$$

Famille génératrice : Soit $x \in M$, on peut écrire, puisque $(f_j)_{j\in J}$ une base de M sur L,

$$x = \sum_{j\in J} \mu_j f_j \quad \text{avec } \mu_j \in L$$

Puis, on peut décomposer chaque μ_j dans $(e_i)_{i\in I}$ qui est une base de L sur K (*i.e.*)

$$\forall j \in J,\ \mu_j = \sum_{i\in I} \lambda_{ij} e_i \quad \text{avec } \lambda_{ij} \in K$$

Finalement,

$$x = \sum_{j\in J} \mu_j f_j = \sum_{j\in J} \mu_j \left(\sum_{i\in I} \lambda_{ij} e_i\right) = \sum_{(i,j)\in I\times J} \lambda_{ij} e_i f_j$$

avec $\lambda_{ij} \in K$. D'où le résultat.

Exercice : Soit p un nombre premier et $n \in \mathbb{N}^*$. On note $q = p^n$.
1) Montrer que le corps fini $\mathbb{F}_{q^n}$ admet un unique sous-corps $\mathbb{F}_q$ à q éléments et que $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$.
2) En déduire que tout corps intermédiaire $\mathbb{F}_q \subseteq K \subseteq \mathbb{F}_{q^n}$ est un corps $\mathbb{F}_{q^d}$ à q^d éléments où d est un diviseur de n et que, pour chaque diviseur d de n, il existe un unique corps intermédiaire de cardinal q^d.

Solution : 1) *Unicité :* S'il existe un sous-corps K de $\mathbb{F}_{q^n}$ ayant q éléments, alors le groupe multiplicatif K^* (qui a $q-1$ éléments) vérifie

$$\forall x \in K^*,\ \ x^{q-1} = x \underset{0^{q-1}=0}{\Rightarrow} \forall x \in K,\ \ x^{q-1} = x$$

Par suite, il en résulte que tout $x \in K$ est une racine du polynôme $X^q - X$. Ce polynôme étant de degré q, K est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$. Ainsi, si K existe, alors K est unique (par unicité

du corps de décomposition).

Existence : On sait $\mathbb{F}_{q^n}$ est le corps de décomposition de $X^{q^n} - X$ sur $\mathbb{F}_p$ et $X^q - X \mid X^{q^n} - X$.

Rappel : Pour $a, b \in \mathbb{N}^*$, on a $X^a - 1 \mid X^{ab} - 1$.
Ch'tite démonstration :

$$X^{ab} - 1 = (X^a)^b - 1 = (X^a - 1)(1 + (X^a)^2 + ... + (X^a)^{b-1})$$

D'où le résultat.

□

Donc $\mathbb{F}_{q^n}$ contient un corps de décomposition de $X^q - X$ et un tel corps contient q éléments. D'où l'existence.

Calcul du degré : Soit $m = [\mathbb{F}_{q^n} : \mathbb{F}_q]$. Ce qui se traduit par le fait que $\mathbb{F}_{q^n}$ est un $\mathbb{F}_q$-e.v. de dimension m et donc $|\mathbb{F}_{q^n}| = |\mathbb{F}_q|^m$. Par suite, $q^n = q^m$, d'où $m = n$.

2) Soit $\mathbb{F}_q \subseteq K \subseteq \mathbb{F}_{q^n}$ et soit $d = [K : \mathbb{F}_q]$. Alors $|K| = |\mathbb{F}_q|^d = q^d$ et par multiplicativité des degrés, on a

$$n = [\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : K][K : \mathbb{F}_q]$$

Donc $d \mid n$
Réciproquement, soit d un diviseur de n. Posons $r = q^d$. Alors $\mathbb{F}_{q^n} = \mathbb{F}_{r^m}$ où $m = \frac{n}{d}$ et, d'après ce qui précède, il existe un unique sous-corps $\mathbb{F}_r$ dans $\mathbb{F}_{r^m}$.

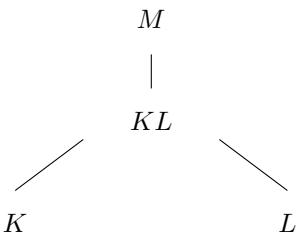
Exercice : Soient m et n des entiers naturels non nuls. On pose N=ppcm(m, n) et d=pgcd(m, n). Pour tout $t \in \mathbb{N}^*$, on désigne par ξ_t une racine primitive t-ième de l'unité. Montrer que
(i) $\mathbb{Q}(\xi_m)\mathbb{Q}(\xi_n) = \mathbb{Q}(\xi_N)$
(ii) $\mathbb{Q}(\xi_m) \cap \mathbb{Q}(\xi_n) = \mathbb{Q}(\xi_d)$

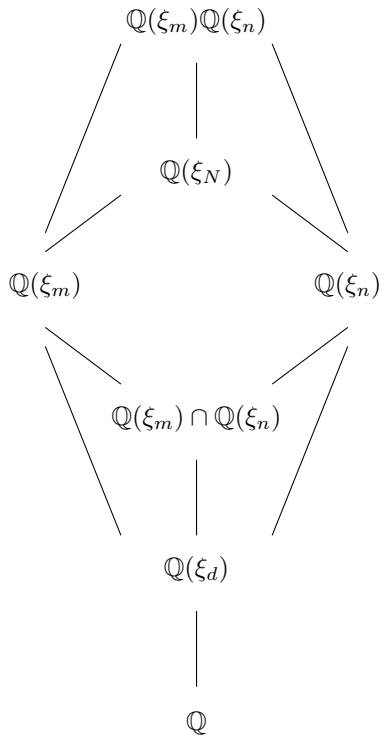
Solution :

Rappel 1 : Soient K et L deux sous-corps d'un corps M. Par définition KL est le plus petit sous corps de M contenant K et L. L'opération

$$(K, L) \to KL$$
$$(k, l) \mapsto kl$$

est commutative et associative et si $K \subseteq L$, alors $KL = L$

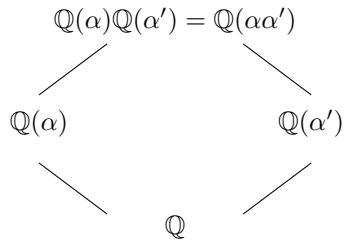




Rappel 2 : Soit α (resp. α') une racine p-ième (resp. q-ième) de l'unité. Si $\text{pgcd}(p,q)=1$ alors $\alpha\alpha'$ est une racine pq-ième de l'unité, et donc on a

$$\mathbb{Q}(\alpha)\mathbb{Q}(\alpha')=\mathbb{Q}(\alpha\alpha')$$

On peut étendre ce résultat par récurrence à plus de deux racines de l'unité.



Ch'tite démonstration : Montrons que si α et α' sont respectivement des racines p-ième et q-ième de l'unité avec $\text{pgcd}(p,q)=1$ alors $\alpha\alpha'$ est une racine pq-ième de l'unité.
Cela provient du résultat plus général suivant (et à connaître !) :

«Soient a et b des éléments d'ordre p et q d'un groupe G. On suppose que a et b commutent et que p et q sont premiers entre eux, alors ab est d'ordre pq.»

Notons n l'ordre de ab. Comme a et b commutent, on a $(ab)^{pq}=a^{pq}b^{pq}=1$, donc n (l'ordre de ab) divise pq.
Inversement, si $(ab)^n=1=a^nb^n$, on a

$$a^{nq}\underbrace{b^{nq}}_{=1}=1 \quad\Rightarrow\quad a^{nq}=1$$

Donc l'ordre de a (qui est q) divise nq mais comme p et q sont premiers entre eux, alors $q \mid n$. On applique le même raisonnement à b et on en déduit que $p \mid n$. Par conséquent, $pq \mid n$. D'où le résultat.

□

Maintenant les rappels faits, revenons à notre exercice.
(i) Ecrivons n, m et N en produit de facteurs premiers distincts :

$$m=p_1^{\alpha_1}...p_k^{\alpha_k}, \qquad n=p_1^{\beta_1}...p_k^{\beta_k}, \qquad N=p_1^{\gamma_1}...p_k^{\gamma_k}$$

où $\alpha_j,\beta_j\geq 0$, $\gamma_j=\max(\alpha_j,\beta_j)\neq 0$ pour tout $j\in\{1,...,k\}$.
D'une part, d'après le Rappel 2, on a

$$\mathbb{Q}(\xi_m)=\mathbb{Q}(\xi_{p_1^{\alpha_1}})...\mathbb{Q}(\xi_{p_k^{\alpha_k}}) \qquad (\dagger)$$
$$\mathbb{Q}(\xi_n)=\mathbb{Q}(\xi_{p_1^{\beta_1}})...\mathbb{Q}(\xi_{p_k^{\beta_k}}) \qquad (\dagger\dagger)$$

D'autre part, pour $a,b\in\mathbb{N}^*$, on a $\mathbb{Q}(\xi_a)\subseteq\mathbb{Q}(\xi_{ab})$. En effet, ξ_a est une racine de $X^{ab}-1=(X^a)^b-1$ et $\mathbb{Q}(\xi_{ab})$ est le corps de décomposition du polynôme $X^{ab}-1$. Avec le Rappel 1, on a donc, pour tout $j\in\{1,...,k\}$

$$\mathbb{Q}(\xi_{p_j^{\alpha_j}})\mathbb{Q}(\xi_{p_j^{\beta_j}})=\mathbb{Q}(\xi_{p_j^{\gamma_j}})$$

Grâce à $(\dagger)$ et $(\dagger\dagger)$, on a donc

$$\begin{aligned}\mathbb{Q}(\xi_m)\mathbb{Q}(\xi_n)&=\mathbb{Q}(\xi_{p_1^{\gamma_1}})...\mathbb{Q}(\xi_{p_k^{\gamma_k}})\\&=[\mathbb{Q}(\xi_{p_1^{\alpha_1}})...\mathbb{Q}(\xi_{p_k^{\alpha_k}})][\mathbb{Q}(\xi_{p_1^{\beta_1}})...\mathbb{Q}(\xi_{p_k^{\beta_k}})]\\&=\mathbb{Q}(\xi_{p_1^{\alpha_1}})\mathbb{Q}(\xi_{p_1^{\beta_1}})...\mathbb{Q}(\xi_{p_k^{\alpha_k}})\mathbb{Q}(\xi_{p_k^{\beta_k}})\\&=\mathbb{Q}(\xi_{p_1^{\gamma_1}})...\mathbb{Q}(\xi_{p_k^{\gamma_k}})\\&=\mathbb{Q}(\xi_{p_1^{\gamma_1}...p_k^{\gamma_k}})=\mathbb{Q}(\xi_N)\end{aligned}$$

(ii) Par commodité, posons $k = \mathbb{Q}(\xi_m) \cap \mathbb{Q}(\xi_n)$. Par définition, $d \mid n$ et $d \mid m$, on a donc $\mathbb{Q}(\xi_d) \subseteq k$. Par ailleurs, on a

$$\underbrace{[\mathbb{Q}(\xi_m) : \mathbb{Q}]}_{\varphi(m)} = [\mathbb{Q}(\xi_m) : \mathbb{Q}(\xi_d)] \underbrace{[\mathbb{Q}(\xi_d) : \mathbb{Q}]}_{\varphi(d)}$$

d'où

$$[\mathbb{Q}(\xi_m) : \mathbb{Q}(\xi_d)] = \frac{\varphi(m)}{\varphi(d)}$$

Puis, par la question précédente, on a

$$[\mathbb{Q}(\xi_n)\mathbb{Q}(\xi_m) : \mathbb{Q}(\xi_m)] = [\mathbb{Q}(\xi_N) : \mathbb{Q}(\xi_m)] = \frac{\varphi(N)}{\varphi(m)}$$
$$[\mathbb{Q}(\xi_n)\mathbb{Q}(\xi_m) : \mathbb{Q}(\xi_n)] = [\mathbb{Q}(\xi_N) : \mathbb{Q}(\xi_n)] = \frac{\varphi(N)}{\varphi(n)}$$

Rappel 3 :

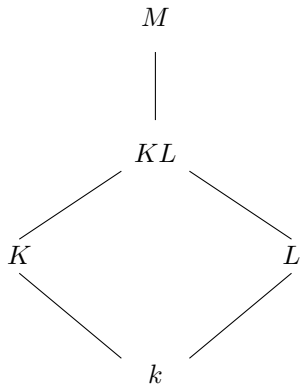
Soit $k \subset M$ une extension, K et L deux corps intermédiaires, KL le sous-corps de M engendré par K et L. Alors on a

$$[KL : L] \leq [K : k]$$

Ch'tite démonstration : Tout élément de KL s'écrit sous la forme

$$x = \sum u_i v_i \quad \text{avec } u_i \in K,\ v_i \in L$$

Ainsi, si $(x_1, ..., x_n)$ est une base de K sur k, alors $(x_1, ..., x_n)$ engendre KL sur L.



□

Par le Rappel 3, on en déduit que

$$[\mathbb{Q}(\xi_n)\mathbb{Q}(\xi_m) : \mathbb{Q}(\xi_n)] \leq [\mathbb{Q}(\xi_m) : k]$$

Par suite,

$$[\mathbb{Q}(\xi_n)\mathbb{Q}(\xi_m) : \mathbb{Q}(\xi_n)] = \frac{\varphi(N)}{\varphi(n)} \leq [\mathbb{Q}(\xi_m) : k] \leq [\mathbb{Q}(\xi_m) : \mathbb{Q}(\xi_d)] \leq \frac{\varphi(m)}{\varphi(d)}$$

Cependant, comme $mn = Nd$, on a donc par multiplicativité de la fonction φ,

$$\varphi(m)\varphi(n) = \varphi(N)\varphi(d)$$

Ainsi, on obtient

$$\frac{\varphi(N)}{\varphi(n)} \leq [\mathbb{Q}(\xi_m) : k] \leq [\mathbb{Q}(\xi_m) : \mathbb{Q}(\xi_d)] \leq \frac{\varphi(m)}{\varphi(d)} \xrightarrow[\varphi(m)\varphi(n)=\varphi(N)\varphi(d)]{} [\mathbb{Q}(\xi_m) : k] = [\mathbb{Q}(\xi_m) : \mathbb{Q}(\xi_d)]$$

Et comme $\mathbb{Q}(\xi_d) \subseteq k \subseteq \mathbb{Q}(\xi_m)$, on a bien $\mathbb{Q}(\xi_d) = k$. D'où le résultat.