Corps de rupture et corps de décomposition : correction

Exercice 1.
A chaque fois on notera R un corps de rupture et D un corps de décomposition du polynôme en question.

1. X^2+7 a pour racines $i\sqrt{7}$ et $-i\sqrt{7}$, qui ne sont pas dans $\mathbf{Q}$. Comme il est de degré 2 il est irréductible sur $\mathbf{Q}$. On a donc par exemple $R=\mathbf{Q}(i\sqrt{7})$ qui est de degré 2 sur $\mathbf{Q}$ et on remarque que X^2+7 a toutes ses racines dans R d'où $D=R$.
2. Racines : $2^{1/3}, j2^{1/3}, j^2 2^{1/3}$, de degré 3 donc irréductible sur $\mathbf{Q}$, on a donc $R=\mathbf{Q}(2^{1/3})$ qui est de degré 3 sur $\mathbf{Q}$.

   Un sous-corps de $\mathbf{C}$ qui est un corps de décompostion de X^3-2 contient nécessairement $2^{1/3}$ et $2^{1/3}j$ donc $2^{1/3}$ et j. Il contient donc $\mathbf{Q}(2^{1/3}, j)$. Par ailleurs X^3-2 est scindé sur ce corps, c'est donc un corps de décomposition.

   On peut remarquer que $\mathbf{Q}(2^{1/3}, j)$ est une extension stricte de $\mathbf{Q}(2^{1/3})$ qui est de degré 3 sur $\mathbf{Q}$ (puisque $\mathbf{Q}(2^{1/3})$ est un sous-corps de $\mathbf{R}$ qui ne contient pas j), engendrée par j, dont X^2+X+1 est un polynôme annulateur. On en déduit que $[\mathbf{Q}(2^{1/3}, j) : \mathbf{Q}(2^{1/3})] = 2$ et donc que $[\mathbf{Q}(2^{1/3}, j) : \mathbf{Q}] = 6$.
3. Même argumentation que précédement : $R=\mathbf{Q}(11^{1/3})$ de degré 3 sur $\mathbf{Q}$, $D=\mathbf{Q}(11^{1/3}, j)$ de degré 6.
4. Les racines complexes de X^4+1 sont $\alpha = e^{i\pi/4}$, $\overline{\alpha}$, α^3 et $\overline{\alpha^3}$. Comme elles sont toutes complexes, X^4+1 n'admet pas de facteur de degré 1 sur $\mathbf{Q}$.

   D'autre part la décomposition en facteurs irréductibles unitaires de X^4+1 sur $\mathbf{R}$ est $(X^2-\sqrt{2}X+1)(X^2+\sqrt{2}X+1)$. Aucun de ces facteurs n'est à coefficients rationnels, X^4+1 n'admet donc pas de facteurs de degré 2 sur $\mathbf{Q}$. Il est donc irréductible sur $\mathbf{Q}$.

   On en déduit qu'un corps de rupture, par exemple $\mathbf{Q}(\alpha)$, est de degré 4. On remarque que les autres racines sont toutes des puissances de α, et $\mathbf{Q}(\alpha)$ est donc également un corps de décomposition.
5. $X^4-1=(X-1)(X+1)(X^2+1)$ n'est pas irréductible sur $\mathbf{Q}$. Des corps de rutpure de ses facteurs respectifs sont $\mathbf{Q}$ et $\mathbf{Q}(i)$, de degré 1 et 2 respectivement. $\mathbf{Q}(i)$ est un corps de décomposition.
6. X^4+2 est irréductible sur $\mathbf{Q}$ (Eisenstein, p=2). Ses racines complexes sont $2^{1/4}\alpha$, $2^{1/4}\alpha^{-1}$, $2^{1/4}\alpha^3$ et $2^{1/4}\alpha^{-3}$. Un corps de rupture est par exemple $\mathbf{Q}(2^{1/4}\alpha)$ de degré 4.

   Un sous-corps de $\mathbf{C}$ corps de décomposition de X^4+2 contiendra $\sqrt{2} = -2^{1/4}\alpha \cdot 2^{1/4}\alpha^3$ et $i=\alpha^2=(2^{1/4}\alpha)^2/\sqrt{2}$, il contiendra donc $\alpha=(1+i)/\sqrt{2}$ et finalement $2^{1/4}$. On remarque que X^4+2 est scindé dans $\mathbf{Q}(2^{1/4}, \alpha)$, c'est donc un corps de décomposition de X^4+2.

   On peut calculer son degré séparément. Le polynôme minimal de $2^{1/4}$ sur $\mathbf{Q}$ est X^4-2 (irréductible par Eisenstein), $\mathbf{Q}(2^{1/4})$ est donc de degré 4 sur $\mathbf{Q}$. C'est un sous-corps de $\mathbf{R}$, il ne contient donc pas α, et $\mathbf{Q}(2^{1/4}, \alpha)$ est une extension stricte de $\mathbf{Q}(2^{1/4})$ engendrée par α. On remarque que $X^2-\sqrt{2}X+1$ est un polynôme annulateur de degré 2 de α à coefficients dans $\mathbf{Q}(2^{1/4})$, c'est donc le polynôme minimal de α sur $\mathbf{Q}(2^{1/4})$. On a donc $[\mathbf{Q}(2^{1/4}, \alpha) : \mathbf{Q}(2^{1/4})] = 2$ et $[\mathbf{Q}(2^{1/4}, \alpha) : \mathbf{Q}] = 8$.
7. On raisonne comme précédement et on trouve $R=\mathbf{Q}(2^{1/4})$ de degré 4 et $D=R=\mathbf{Q}(2^{1/4}, i)$ de degré 8 sur $\mathbf{Q}$.

8. $X^4 - 5X^2 + 6 = (X^2 - 2)(X^2 - 3)$. Corps de rupture $\mathbf{Q}(\sqrt{2})$ ou $\mathbf{Q}(\sqrt{3})$. Corps de décomposition $\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\sqrt{2} + \sqrt{3})$ de degré 6 (cf TD1).
9. $X^p - 1 = (X-1)\Phi_{p-1}$. $\mathbf{Q}$ est donc un corps de rupture. Les racines de $X^p - 1$ sont les ζ_p^k, le polynôme Φ_{p-1} est irréductible sur $\mathbf{Q}$ (cf TD 1) de degré $p-1$. On en déduit qu'un corps de rupture est $\mathbf{Q}(\zeta_p)$ qui est de degré $p-1$ sur $\mathbf{Q}$.

Exercice 2.

1. Faux si le polynôme n'est pas irréductible (chaque facteur irréductible donne un corps de rupture de degré égal au degré du facteur), vrai sinon (tous les corps de rupture sont alors isomorphes à $K[X]/<P(X)>$ et donc isomorphes entre eux).
2. Faux : une extension de corps admet en général beaucoup d'automorphismes. $\mathbf{C}$ est par exemple un corps de rupture de X^2+1 sur $\mathbf{R}$ et admet deux automorphismes : id et la conjugaison, qui (respectivement)fixe et échange les racines de X^2+1.

   Par-contre deux corps de rupture sont isomorphes à un unique "isomorphisme d'extension monogène" près (c'est-à-dire un isomorphisme qui préserve le corps de base et envoie élément générateur sur élément générateur).
3. Vrai (cf. cours).
4. Faux, même contre-exemple que pour les corps de rupture.
5. Faux, cf. contre-exemples exo 1.
6. $deg(P)$! (par récurrence).

Exercice 3.

1. Soit $P \in K[X]$ un polynôme unitaire de degré 2. On peut l'écrire $P = X^2 - p_1 X + p_2$ avec p_1, $p_2 \in K$. Si le corps est de caractéristique 2, alors pour tout $x \in K$ $P(x) = (x - p_1 x + p_2)^2$ et P est donc scindé sur K.

   Sinon, en posant $a = p_1/2$ et $b = p_1^2/4 - p_2$ (ce qui est licite lorsque K n'est pas de caractéristique 2), on a bien $P = (X-a)^2 - b$. P est alors soit scindé sur K, soit tout corps de rupture est de degré 2 et est également corps de décomposition.
2. Soit $\widetilde{\alpha} \in L \setminus K$. La famille $(1, \widetilde{\alpha})$ est donc une famille K-libre de L. C'en est donc une base. On peut ainsi écrire $\widetilde{\alpha}^2 = \mu\widetilde{\alpha} + \lambda$ pour un certain couple $(\lambda, \mu) \in K^2$. Le polynôme minimal de $\widetilde{\alpha}$ est alors $\mu_{\widetilde{\alpha}}(X) = X^2 - \mu X - \lambda$ (ce polynôme est en effet annulateur, et il est clairement de degré minimal pour cette propriété). D'après la question précédente, il existe a et b dans K tels que $\mu_{\widetilde{\alpha}}(X) = (X-a)^2 - b$. Soit $\alpha = \widetilde{\alpha} - a$. On a évidemment $K(\alpha) = K(\widetilde{\alpha}) = L$, et $\alpha^2 = (\widetilde{\alpha} - a)^2 = b \in K$.
3. Soit $\beta \in L$ tel que $L = K(\beta)$ et $\beta^2 \in K$. On peut alors écrire $\beta = \lambda\alpha + \mu$, pour $(\lambda, \mu) \in K^2$. On obtient alors $\beta^2 = (\lambda^2\alpha^2 + \mu)^2 + 2\lambda\mu\alpha$. L'hypothèse $\beta^2 \in K$ entraîne donc que $\lambda = 0$ ou que $\mu = 0$. Mais le premier cas est impossible car il entraînerait $\beta \in K$; on a donc $\mu = 0$, c'est-à-dire que $\beta/\alpha \in K$.

Exercice 4.

1. Dans $\mathbf{F}_2[X]$, le polynôme $X^4 + X + 1$ est irréductible : en effet, il n'a pas de racine et ne peut pas s'écrire comme produit de deux irréductibles de degré 2 (il n'y a qu'un seul irréductible de degré 2, X^2+X+1, et $X^4+X+1 \neq (X^2+X+1)^2 = X^4+X^2+1$). Le polynôme unitaire X^4+X+1 est donc irréductible dans $\mathbf{Q}[X]$.

   Si l'on ne pense pas à cette astuce, il est toujours possible de s'en sortir avec moins de subtilité : une éventuelle racine rationnelle a/b de $X^4 + X + 1$ aurait un dénominateur b divisant

le coefficient dominant et un numérateur a divisant le coefficient constant. Ces deux coefficients étant égaux à 1, il n'y a qu'à vérifier que ± 1 n'est pas racine de X^4+X+1 (ce qui est immédiat) pour s'assurer qu'il n'a pas de racine rationnelle. Pour obtenir l'irréductibilité, il ne reste donc plus qu'à exclure une factorisation

$$X^4+X+1=(X^2+aX+b)(X^2+cX+d)$$

en deux polynômes du second degré à coefficients entiers (en effet, le lemme de Gauß implique qu'un polynôme entier unitaire est réductible sur $\mathbf{Q}$ si et seulement s'il l'est sur $\mathbf{Z}$). En développant et en identifiant les coefficients, on obtient le système

$$a+c=0, \qquad b+ac+d=0, \qquad ad+bc=1, \qquad bd=1,$$

qui n'a pas de solution sur $\mathbf{Z}$ (la première équation entraîne $c=-a$, la dernière entraîne $b=d=\pm 1$, donc la deuxième équation devient $a^2=\pm 2$, ce qui est impossible pour $a\in\mathbf{Q}$).

2. Par hypothèse, il existe une suite d'extensions $\mathbf{Q}=K_0\subseteq K_1\subseteq\cdots\subseteq K_m$ avec $x\in K_m$ et $[K_{i+1}:K_i]=2$. On peut supposer que $x\notin K_{m-1}$. Alors le polynôme minimal de x sur K_{m-1} est de degré 2, et divise P dans $K_{m-1}[X]$.

3. Soit $P=(X^2+aX+b)(X^2+cX+d)$ la décomposition de la question précédente. En développant et en identifiant les coefficients, on a donc

$$\begin{cases} a+c &= 0\\ b+ac+d &= 0\\ ad+bc &= 1\\ bd &= 1. \end{cases} \Leftrightarrow a\neq 0 \text{ et } \begin{cases} c &= -a\\ b+d &= a^2\\ d-b &= 1/a\\ bd &= 1. \end{cases}$$

Les deuxième et troisième équations entraînent $2d=a^2+1/a$ et $2b=a^2-1/a$. La quatrième équation s'écrit donc $4=(a^2+1/a)(a^2-1/a)$ ou encore $a^4-a^{-2}=4$. Le coefficient a est donc bien racine de $Q(X)=X^6-4X^2-1$.

4. Par construction, $Q\in\mathbf{Q}[X]$ a une racine a constructible, dont le degré $\deg\mu_a$ est de ce fait une puissance de 2 inférieure à 6.

   On vérifie facilement que Q n'a pas de racine entière. Puisqu'il est unitaire, cela entraîne qu'il n'a pas de racine dans $\mathbf{Q}$. Le degré de l'algébrique a est donc 2 ou 4.

   Que ce degré vaille 2 ou 4, on a trouvé une décomposition $Q=Q_2Q_4$ de Q en produit de deux polynômes unitaires, l'un de degré 2 et l'autre de degré 4. Puisque Q n'a pas de racine, Q_2 est irréductible.

   Comme on a en outre $Q(X)=Q(-X)=Q_2(-X)Q_4(-X)$, Q_2 doit diviser $Q_2(-X)$ ou $Q_4(-X)$.
   - Si Q_2 divise $Q_2(-X)$, alors $Q_2=Q_2(-X)$, et ceci impose que Q_2 soit de la forme X^2+n ($n\in\mathbf{Q}$).
   - Sinon, Q_2 divise $Q_4(-X)$, donc $Q_2(X)$ et $Q_2(-X)$ divisent $Q_4(X)$. On peut alors écrire $Q=Q_2(X)Q_2(-X)\tilde{Q}(X)$, ce qui entraîne $\tilde{Q}(X)=\tilde{Q}(-X)$, et donc $\tilde{Q}(X)=X^2+n$ ($n\in\mathbf{Q}$).

   Dans les deux cas, on a donc une factorisation sur $\mathbf{Q}$ de la forme $Q=(X^2+n)R$. Comme Q est unitaire, on a affaire à une factorisation en polynômes unitaires dans $\mathbf{Q}[X]$. D'après le lemme de Gauß, les deux facteurs sont bien dans $\mathbf{Z}[X]$. En particulier, $n\in\mathbf{Z}$.

5. Soit α une racine carrée (complexe) de n. Alors α est racine de Q ; donc $n=\alpha^2$ est racine de X^3-4X-1, qui n'a pas de racine entière, d'où une contradiction. Donc x n'est pas constructible.

Exercice 5. Pour cet exercice, nous n'avons pas corrigé tous les cas envisagés par l'énoncé, mais seulement détaillé certains d'entre eux. Nous encourageons les lecteurs à traiter intégralement un autre cas, en s'inspirant de ce qui suit.

1. Un polynôme de degré 2 ou 3 est irréductible si et seulement s'il n'a pas de racine. Sur $\mathbf{F}_2$, il faut et il suffit donc que le coefficient constant soit égal à 1 (0 n'est pas racine) et que le nombre de coefficients égaux à 1 soit impair (1 n'est pas racine). Ainsi, les polynômes de degré 2 ou 3 irréductibles sont

$$X^2+X+1, \qquad X^3+X+1 \qquad \text{et} \qquad X^3+X^2+1.$$

En degré 4, il faut aussi empêcher que le polynôme soit le produit de deux irréductibles de degré 2. Sur $\mathbf{F}_2$, cela n'exclut que $(X^2+X+1)=X^4+X^2+1$. Les polynômes irréductibles de degré 4 sont donc

$$X^4+X^3+X^2+X+1, \qquad X^4+X+1 \qquad \text{et} \qquad X^4+X^3+1.$$

2. D'après ce qui précède, $\mathbf{F}_8=\mathbf{F}_2[X]/(X^3+X+1)$ est une extension de degré 3 de $\mathbf{F}_2$. Si on note ω la classe de X, on a donc

$$\mathbf{F}_8=\{0,1,\omega,\omega+1,\omega^2,\omega^2+1,\omega^2+\omega,\omega^2+\omega+1\}$$

et ω vérifie $\omega^3=\omega+1$. On aurait pu faire l'autre choix et construire $\mathbf{F}_8'=\mathbf{F}_2[X]/(X^3+X^2+1)=\mathbf{F}_2[\alpha]$, avec $\alpha^3=\alpha^2+1$ mais on obtient ainsi un corps isomorphe. En effet,

$$(\omega+1)^3=\omega^3+\omega^2+\omega+1=\omega^2=(\omega+1)^2+1.$$

Puisque $\omega+1\notin\mathbf{F}_2=\{0,1\}$, son polynôme minimal sur $\mathbf{F}_2$ est bien X^3+X^2+1 et l'application

$$\begin{aligned}\text{év}_{\omega+1}:\mathbf{F}_2[X] &\to \mathbf{F}_8\\ P &\mapsto P(\omega+1)\end{aligned}$$

induit bien un isomorphisme $\varphi:\mathbf{F}_8'=\mathbf{F}_2[X]/(X^3+X^2+1)\to\mathbf{F}_8$ envoyant α sur $\omega+1$. On peut facilement calculer toutes les valeurs de φ :

$x\in\mathbf{F}_8'\mapsto\psi(x)\in\mathbf{F}_8$	$x\in\mathbf{F}_8'\mapsto\psi(x)\in\mathbf{F}_8$	$x\in\mathbf{F}_8'\mapsto\psi(x)\in\mathbf{F}_8$	$x\in\mathbf{F}_8'\mapsto\psi(x)\in\mathbf{F}_8$
$0\mapsto 0$	$\alpha\mapsto\omega+1$	$\alpha^2\mapsto\omega^2+1$	$\alpha^2+\alpha\mapsto\omega^2+\omega$
$1\mapsto 1$	$\alpha+1\mapsto\omega$	$\alpha^2+1\mapsto\omega^2$	$\alpha^2+\alpha+1\mapsto\omega^2+\omega+1.$

3. L'élément ω engendre $\mathbf{F}_8^\times$ (comme $\mathbf{F}_8^\times$ est un groupe d'ordre 7, tout élément de $\mathbf{F}_8^\times$ est un générateur).

$$\omega^0=1,\ \omega^1=\omega,\ \omega^2=\omega^2,\ \omega^3=\omega+1,\ \omega^4=\omega^2+\omega,\ \omega^5=\omega^2+\omega+1,\ \omega^6=\omega^2+1.$$

4. $\mathbf{F}_8/\mathbf{F}_2$ est une extension de degré 3 donc tous les éléments de $\mathbf{F}_8$ sont algébriques, d'un degré divisant 3, c'est-à-dire 1 ou 3. Il suffit donc, pour chaque élément de $\mathbf{F}_8\setminus\mathbf{F}_2$ de déterminer lequel des deux polynômes irréductibles de degré 3 l'annule.

   Ainsi, 0 a pour polynôme minimal X, 1 a $X-1$; ω, ω^2 et $\omega^2+\omega$ ont X^3+X+1 et $\omega+1$, ω^2+1 et $\omega^2+\omega+1$ ont X^3+X+1.

5. Prenons $\mathbf{F}_{16}=\mathbf{F}_2[X]/(X^4+X+1)$ et appelons β la classe de X. On obtient que β est un générateur de $\mathbf{F}_{16}^\times$ (cette fois-ci, rien ne garantissait que ce soit le cas, puisqu'il y a des éléments de $\mathbf{F}_{16}^\times$, groupe cyclique d'ordre 15, qui ne l'engendrent pas, mais on est rassuré dès que l'on constate que β^3 et β^5 sont différents de 1) :

$$\begin{aligned}&\beta^0=1,\beta^1=\beta,\beta^2,\beta^3,\beta^4=\beta+1,\beta^5=\beta^2+\beta,\beta^6=\beta^3+\beta^2,\beta^7=\beta^3+\beta+1,\\ &\beta^8=\beta^2+1,\beta^9=\beta^3+\beta,\beta^{10}=\beta^2+\beta+1,\beta^{11}=\beta^3+\beta^2+\beta,\beta^{12}=\beta^3+\beta^2+\beta+1,\\ &\beta^{13}=\beta^3+\beta^2+1,\beta^{14}=\beta^3+1.\end{aligned}$$

Maintenant, les éléments de $\mathbf{F}_{16}$ sont algébriques sur $\mathbf{F}_2$, de degré divisant 4. Il faut les répartir parmi les quatre polynômes minimaux possibles (le polynôme irréductible de degré 2 et les trois polynômes irréductibles de degré 4). Une remarque aide : comme $(X-1)(X^2+X+1) = X^3-1$ et $(X-1)(X^4+X^3+X^2+X+1) = X^5-1$ (évidemment, les $-$ sont aussi des $+$, mais il est plus facile de se souvenir de ces formules-ci), les éléments de $\mathbf{F}_{16}$ dont le polynôme minimal est X^2+X+1 (resp. $X^4+X^3+X^2+X+1$) sont les racines troisièmes (resp. cinquièmes) de l'unité différentes de 1, c'est-à-dire β^5 et β^{10} (resp. β^3, β^6, β^9 et β^{12}). Pour le reste des calculs (c'est-à-dire pour répartir les huit éléments restants entre les deux polynômes irréductibles X^4+X+1 et X^4+X^3+1) la table des puissances de β permet de mener les calculs relativement rapidement. Par exemple, $(\beta^3+\beta^2+\beta)^4+(\beta^3+\beta^2+\beta)^3+1 = (\beta^{11})^4+(\beta^{11})^3+1 = \beta^{44}+\beta^{33}+1 = \beta^{14}+\beta^3+1 = 0$. On obtient ainsi les résultats suivants.
– Le polynôme minimal de 0 est X ;
– Le polynôme minimal de 1 est $X-1$;
– Le polynôme minimal de $\beta^2+\beta$ et $\beta^2+\beta+1$ est X^2+X+1 ;
– Le polynôme minimal de β^3, $\beta^3+\beta^2$, $\beta^3+\beta$ et $\beta^3+\beta^2+\beta+1$ est $X^4+X^3+X^2+X+1$;
– Le polynôme minimal de β, $\beta+1$, β^2 et β^2+1 est X^4+X+1 ;
– Le polynôme minimal de β^3+1, $\beta^3+\beta+1$, $\beta^3+\beta^2+1$ et $\beta^3+\beta^2+\beta$ est X^4+X^3+1.
En particulier, on obtient ainsi des éléments de polynôme minimal X^4+X^3+1 et $X^4+X^3+X^2+X+1$, ce qui permet de trouver des morphismes de corps

$$\varphi' = \text{év}_{\beta^3+1} : \mathbf{F}'_{16} = \mathbf{F}_2[X]/(X^4+X^3+1) \to \mathbf{F}_{16}, \qquad \varphi'' = \text{év}_{\beta^3} : \mathbf{F}''_{16} = \mathbf{F}_2[X]/(X^4+X^3+X^2+X+1) \to \mathbf{F}_{16}$$

qui sont des isomorphismes par égalité des cardinaux (ou des $\mathbf{F}_2$-dimensions).
On remarque que l'on obtient de la même façon un morphisme de corps

$$\iota = \text{év}_{\beta^2+\beta} : \mathbf{F}_4 = \mathbf{F}_2[X]/(X^2+X+1) \to \mathbf{F}_{16}$$

dont l'image est $\{0, 1, \beta^2+\beta, \beta^2+\beta+1\}$.

Exercice 6.

1. Évidemment, cette question fait penser à l'existence et à l'unicité à isomorphisme près de la clôture algébrique. On va d'ailleurs utiliser ce fait pour notre preuve. Plus précisément, si Ω est une clôture algébrique de K, on définit l'ensemble L_Ω des éléments $x \in \Omega$ pour lesquels il existe une suite de corps
$$K_0 = K \subseteq K_1 \subseteq \cdots \subseteq K_n$$
tels que K_i/K_{i-1} soit une extension de degré 2 et $x \in K_n$.
On va alors montrer :
– que L_Ω est quadratiquement clos ;
– que si $K \subseteq L' \subseteq \Omega$ est une extension intermédiaire telle que L' soit quadratiquement clos, alors $L' \supseteq L_\Omega$;
– que si L' est une clôture quadratique de K, alors l'extension L'/K est algébrique.
Les deux premiers points montrent que L_Ω est une clôture quadratique de K et même que c'est la seule clôture quadratique de K incluse dans Ω.
Les deux derniers points montrent l'unicité à isomorphisme près. En effet, si L'/K est une clôture quadratique, on peut choisir une clôture algébrique Ω' de L'. Puisque l'extension L'/K est algébrique, il en est de même de Ω'/L', et Ω' est une clôture algébrique de K. D'après le deuxième point, on a donc $L' = L(\Omega')$. Toutes les clôtures quadratiques de K sont donc de la forme L_Ω pour une clôture algébrique Ω de K. Or, on voit directement à l'aide de la définition que si $\varphi : \Omega \to \Omega'$ est un isomorphisme K-linéaire entre deux clôtures algébriques, celui-ci vérifie $\varphi(L_\Omega) = L(\Omega')$: deux clôtures quadratiques de K sont donc bien isomorphes.
Démontrons donc successivement ces trois points.

– Montrons que L_Ω est quadratiquement clos. Soit donc $\mathrm{P} \in \mathrm{L}_\Omega[\mathrm{X}]$ un polynôme de degré 2, que l'on peut supposer unitaire. Écrivons $\mathrm{P} = \mathrm{X}^2 + b\mathrm{X} + c$. Les coefficients b et c appartiennent à L_Ω donc on peut trouver des tours d'extensions quadratiques

$$\mathrm{K} = \mathrm{K}_0 \subseteq \mathrm{K}'_1 \subseteq \mathrm{K}'_2 \subseteq \cdots \subseteq \mathrm{K}_{n'} \ni b$$
$$\mathrm{K} = \mathrm{K}_0 \subseteq \mathrm{K}''_1 \subseteq \mathrm{K}''_2 \subseteq \cdots \subseteq \mathrm{K}_{n''} \ni c.$$

Comme $\mathrm{K}'_{i+1}/\mathrm{K}'_i$ est quadratique, un simple argument de degré montre que pour tout $\beta_{i+1} \in \mathrm{K}'_{i+1} \setminus \mathrm{K}'_i$, on a $\mathrm{K}'_{i+1} = \mathrm{K}'_i\left[\beta_{i+1}\right]$. L'argument étant le même pour la deuxième suite, on peut trouver des éléments $\beta_1, \ldots, \beta_{n'}$ et $\gamma_1, \ldots, \gamma_{n''}$ dans L_Ω tels que $\mathrm{K}'_i = \mathrm{K}[\beta_1, \ldots, \beta_i]$ et $\mathrm{K}''_j = \mathrm{K}[\gamma_1, \ldots, \gamma_j]$. La tour d'extensions

$$\begin{aligned}\mathrm{K} \subseteq \mathrm{K}_1 = \mathrm{K}[\beta_1] \subseteq \mathrm{K}_2 = \mathrm{K}[\beta_1, \beta_2] \subseteq \cdots \subseteq \mathrm{K}_{n'} = \mathrm{K}[\beta_1, \ldots, \beta_{n'}] \\ \subseteq \mathrm{K}_{n'+1} = \mathrm{K}[\beta_1, \ldots, \beta_{n'}, \gamma_1] \subseteq \cdots \subseteq \mathrm{K}_{n'+n''} = \mathrm{K}[\beta_1, \ldots, \beta_{n'}, \gamma_1, \ldots, \gamma_{n''}]\end{aligned}$$

vérifie manifestement $\forall i \in [\![1, n' + n'']\!], [\mathrm{K}_i : \mathrm{K}_{i-1}] \in \{1, 2\}$. En outre, $\mathrm{K}_{n'+n''}$ contient les éléments b et c.
Le corps $\mathrm{K}_{n'+n''}$ est donc le dernier étage d'une tour d'extensions quadratiques et contient les coefficients de P. Ainsi, P a ses racines soit dans $\mathrm{K}_{n'+n''}$ soit dans une extension quadratique de $\mathrm{K}_{n'+n''}$. Dans tous les cas, P a ses racines dans L_Ω, ce qui achève la preuve.

– Démontrons maintenant le second point : soit $\mathrm{K} \subseteq \mathrm{L}' \subseteq \Omega$ une extension intermédiaire quadratiquement close. Soit $x \in \mathrm{L}_\Omega$. Par construction, on peut trouver une tour d'extensions quadratiques

$$\mathrm{K}_0 = \mathrm{K} \subseteq \mathrm{K}_1 \subseteq \cdots \subseteq \mathrm{K}_n$$

telles que $x \in \mathrm{K}_n$. Montrons par récurrence que $\mathrm{K}_i \subseteq \mathrm{L}'$: l'initialisation est claire, L' étant par définition une extension de K_0. Si maintenant $\mathrm{K}_i \subseteq \mathrm{L}'$, soit $y \in \mathrm{K}_{i+1}$. Par hypothèse, y est algébrique sur K_i, de degré 1 ou 2. Si $y \in \mathrm{K}_i$, il appartient également à L'. S'il est de degré 2 sur K_i, il admet un polynôme minimal $\mu_y \in \mathrm{K}_i[\mathrm{X}]$. Puisque L' est quadratiquement clos, μ_y admet une racine dans L' ; comme le degré de μ_y est 2, cela entraîne que μ_y est scindé sur L', et donc que toutes ses racines appartiennent à L'. On a donc $y \in \mathrm{L}'$, ce qui clôt la récurrence. Ainsi, on a en particulier montré que $x \in \mathrm{L}'$, et on a donc bien $\mathrm{L}' \supseteq \mathrm{L}_\Omega$.

– Soit L' une clôture quadratique de K. On pose

$$\mathrm{M} = \left\{ x \in \mathrm{L}' \,\middle|\, x \text{ soit algébrique sur } \mathrm{K} \right\}.$$

D'après le cours, M est un sous-corps de L' (contenant K). Montrons qu'il est quadratiquement clos. Soit donc $\mathrm{P} \in \mathrm{M}[\mathrm{X}]$ un polynôme de degré 2. Puisque L' est quadratiquement clos, il existe une racine $\alpha \in \mathrm{L}'$ de P. Cet élément $\alpha \in \mathrm{L}$ est donc algébrique sur M. Or, comme M/K est par définition une extension algébrique, le fait que α soit algébrique sur M entraîne qu'il est algébrique sur K. On a donc $\alpha \in \mathrm{M}$, ce qui prouve que M est quadratiquement clos. Par définition de la clôture quadratique, cela entraîne que $\mathrm{M} = \mathrm{L}'$, et donc que L'/K est bien une extension algébrique.

2. Vu la description précédente, le corps des nombres constructibles est une clôture quadratique de **Q**. **C** est une clôture quadratique de **R** : algébriquement clos, il est évidemment quadratiquement clos, et tout sous-corps de **C** quadratiquement clos contenant **R** soit également contenir une racine de $\mathrm{X}^2 + 1$, donc être égal à **C** lui-même. Quant à **C**, de même que tout corps algébriquement clos (ou même uniquement quadratiquement clos), il est égal à sa propre clôture quadratique.

3. Soit $\mathrm{P} \in \mathbf{F}_q[\mathrm{X}]$ un polynôme de degré 2. S'il a une racine dans $\mathbf{F}_q$, il en a évidemment une dans $\mathbf{F}_{q^2}$. Si ce n'est pas le cas, il a tautologiquement une racine dans le sous-corps $\mathbf{F}_q[\alpha]$ de

sa clôture algébrique, où α est une des racines de P. Mais, comme $\mathbf{F}_q$ n'a, à isomorphisme près, qu'une unique extension de degré 2, à savoir $\mathbf{F}_{q^2}$, on a bien $\alpha \in \mathbf{F}_{q^2}$. Cela démontre directement que l'union croissante

$$\mathrm{L} = \bigcup_{n \geq 0} \mathbf{F}_{q^{2^n}}$$

forme un corps quadratiquement clos.

Comme en outre chaque élément $x \in \mathbf{F}_{q^{2^n}}$ vit au dernier étage d'une tour

$$\mathbf{F}_q \subseteq \mathbf{F}_{q^2} \subseteq \mathbf{F}_{q^4} \subseteq \cdots \subseteq \mathbf{F}_{q^{2^n}}$$

d'extensions quadratiques, il doit appartenir à tout sous-corps de L quadratiquement clos. L s'identifie donc bien à la clôture quadratique de $\mathbf{F}_q$.

En revanche, cette clôture quadratique L ne contient par construction que des éléments dont le degré sur $\mathbf{F}_q$ est une puissance de 2. Comme toute clôture algébrique $\overline{\mathbf{F}}_q$ de $\mathbf{F}_q$ soit contenir des éléments de degré 3 sur $\mathbf{F}_q$ (car $\mathbf{F}_q$ possède une extension de degré 3, à savoir $\mathbf{F}_{q^3}/\mathbf{F}_q$), L ne peut pas être algébriquement clos.