Intégralité : correction

Exercice 1.

1. C'est une des versions du lemme de Gauß. Donnons-en une preuve à la main. Supposons que P soit irréductible dans $\mathbf{Z}[X]$ mais réductible dans $\mathbf{Q}[X]$. On peut donc trouver $\Delta \in \mathbf{Z}\setminus\{0\}$ et $P_1, P_2 \in \mathbf{Z}[X]$ non constants tels que $\Delta P = P_1 P_2$. Quitte à diviser, on peut supposer que le contenu de P_i soit premier avec Δ. Soit alors p un facteur premier de Δ. On obtient dans $\mathbf{F}_p[X]$
$$\overline{P}_1 \overline{P}_2 = \overline{0}.$$
Mais l'anneau $\mathbf{F}_p[X]$ est intègre ! L'un des P_i soit donc vérifier $\overline{P}_i = 0$, c'est-à-dire que p divise le contenu de P_i, ce qui constitue une contradiction.

2. Le polynôme $2X$ est réductible dans $\mathbf{Z}[X]$ mais irréductible dans $\mathbf{Q}[X]$.
Soit maintenant P irréductible dans $\mathbf{Q}[X]$ de contenu 1. Soit $P = P_1 P_2$ une factorisation non triviale dans $\mathbf{Z}[X]$. *Non triviale* signifie que les P_i ne sont ni nuls, ni des éléments de $\mathbf{Z}[X]^\times = \{\pm 1\}$. La factorisation est encore valable dans $\mathbf{Q}[X]$, mais elle doit y devenir triviale. Un des P_i soit donc vérifier $P_i \in \mathbf{Q}[X]^\times \cap \mathbf{Z}[X] = \mathbf{Z}\setminus\{0\}$. Puisque aucun des P_i n'est égal à ± 1 par ce qui précède, on doit avoir $P_i = n$, un entier non nul et non inversible. En particulier, n divise le contenu de P, ce qui est une contradiction.

3. Soit $P = P_1 P_2$ une factorisation dans $\mathbf{Z}[X]$. (Comme P est unitaire, les conditions d'irréductibilité dans $\mathbf{Z}[X]$ et $\mathbf{Q}[X]$ sont équivalentes.) En observant les coefficients dominants, on voit que les P_i sont unitaires au signe près. Modulo p, on obtient
$$\overline{P} = \overline{P}_1 \overline{P}_2,$$
avec $\deg \overline{P} = \deg P$ et $\forall i, \deg \overline{P}_i = \deg P_i$. Par irréductibilité dans $\mathbf{F}_p[X]$, l'un des $\overline{P}_i$ doit être élément de $\mathbf{F}_p[X]^\times = \mathbf{F}_p^\times$. En particulier, $\deg \overline{P}_i = 1$. D'après ce qui précède, cela implique $P_i = \pm 1$ et l'irréductibilité de P dans $\mathbf{Z}[X]$.

4. Sur $\mathbf{C}$, on a
$$\begin{aligned} X^4 + 1 &= (X^2 + i)(X^2 - i) \\ &= \left(X - e^{i\pi/4}\right)\left(X + e^{i\pi/4}\right)\left(X - e^{3i\pi/4}\right)\left(X - e^{3i\pi/4}\right) \end{aligned}$$
Le cours entraîne alors que $P = \Phi_8$ est irréductible dans $\mathbf{Z}[X]$ (et $\mathbf{Q}[X]$).
On va montrer que $\overline{\Phi}_8 \in \mathbf{F}_p[X]$ est réductible en montrant qu'il a une racine dans tous les $\mathbf{F}_{p^2}$ (et en utilisant le critère de l'exercice 6 du TD 1). Remarquons déjà qu'en caractéristique 2, $X^4 + 1 = (X+1)^4$ a toujours 1 comme racine quadruple.
Lemme. Soit K un corps de caractéristique différente de 2. Alors $X^4 + 1 \in K[X]$ a une racine si et seulement si K a une racine primitive huitième de l'unité, c'est-à-dire si $K^\times$ a un élément d'ordre 8.
Preuve.
$$\begin{aligned} \xi \in K^\times \text{ est d'ordre } 8 &\Leftrightarrow (\xi^4) \neq 1 \text{ et } (\xi^4)^2 = 1 \\ &\Leftrightarrow \xi^4 = -1 \\ &\Leftrightarrow \xi \text{ est une racine de } X^4 + 1. \end{aligned}$$

On a utilisé l'hypothèse sur la caractéristique pour la deuxième équivalence.
Puisque le groupe $\mathbf{F}_q^\times$ est cyclique, et qu'un groupe cyclique d'ordre n contient des éléments de tout ordre divisant n (si d divise n et que ζ est un générateur, $\zeta^{n/d}$ fait l'affaire), le polynôme X^4+1 a une racine dans $\mathbf{F}_q$ si et seulement si $q-1$ est un multiple de 8.
En tout cas, c'est le cas si $q=p^2$, p nombre premier impair. En effet, dans ce cas, les deux facteurs de $p^2-1=(p+1)(p-1)$ sont tous deux pairs et, comme leur différence vaut 2, l'un des deux doit être un multiple de 4.

Exercice 2.

1. C'est une propriété générale des groupes abéliens finis : *Un groupe abélien fini* G *dont les sous-groupes*
$$G_{[n]}=\left\{g\in G\,\middle|\, ng=0\right\}$$
vérifient $\forall n\in\mathbf{N}^*, |G_{[n]}|\leq n$ *est cyclique.* Une preuve rapide vient du théorème de classification des groupes abéliens finis. On sait en effet qu'il existe une suite $d_1,d_2,\dots,d_r$ d'entiers tels que d_i divise d_{i+1} et
$$G\simeq \mathbf{Z}/d_1\mathbf{Z}\oplus\cdots\oplus\mathbf{Z}/d_r\mathbf{Z}.$$
Si r était strictement supérieur à 1, on trouverait ainsi un sous-groupe isomorphe à $(\mathbf{Z}/d_1\mathbf{Z})^2$ dans G, ce qui impliquerait $\left|G_{[d_1]}\right|\geq d_1^2$, une contradiction. On a donc $r=1$ et le groupe G est cyclique.
2. Le polynôme
$$P(X)=\prod_{x\in K}(X-x)\in K[X],$$
de degré $|K|$, convient.
3. On sait que
$$\omega=-\frac{1}{2}+\frac{\sqrt{3}}{2}i.$$
On vérifie alors immédiatement que $\mathbf{Q}(\omega)=\mathbf{Q}(\sqrt{3}i)$, donc $d=-3$ convient.
4. Le polynôme $P=X^8+X^7+\cdots+X+1$ vérifie
$$P=\frac{X^9-1}{X-1}=\Phi_9\Phi_3.$$
Puisque, d'après le cours (ou l'exercice 3 du TD 2), Φ_3 et Φ_9 sont irréductibles, il s'agit bien de la décomposition de P en éléments irréductibles. Toujours d'après cet exercice, on a les expressions
$$\Phi_3(X)=X^2+X+1,\qquad \Phi_9(X)=X^6+X^3+1.$$

Exercice 3.

1. On vérifie directement que le corps de fractions de $\mathbf{Z}[\sqrt{5}]$ est $\mathbf{Q}(\sqrt{5})$.
Or, l'élément $\dfrac{1+\sqrt{5}}{2}\in\mathbf{Q}(\sqrt{5})$ est entier sur $\mathbf{Z}[\sqrt{5}]$ (ou même sur $\mathbf{Z}$, ce qui est d'ailleurs équivalent car $\mathbf{Z}[\sqrt{5}]$ est entier sur $\mathbf{Z}$), son polynôme minimal étant X^2-X-1.
Or, $\mathbf{Z}[\sqrt{5}]=\left\{a+b\sqrt{5}\,\middle|\, a,b\in\mathbf{Z}\right\}$. On vérifie en effet facilement que cet ensemble est un anneau, et il est alors clair que c'est le plus petit contenant $\sqrt{5}$. Comme $\dfrac{1+\sqrt{5}}{2}$ n'est pas dans cet anneau, $\mathbf{Z}[\sqrt{5}]$ n'est pas intégralement clos.

2. Supposons que A soit un corps. Soit $x \in B \setminus \{0\}$. Ce dernier est par hypothèse entier sur A, c'est-à-dire algébrique sur A (car A est un corps !) On a donc

$$A[x] = A(x) \subseteq B,$$

et x a bien un inverse dans B.

Réciproquement, supposons que B soit un corps et soit $x \in A$ non nul. Puisque B est un corps, x a un inverse $x^{-1} \in B$, et il s'agit de montrer que ce dernier est en fait dans A. Comme B est entier sur A, on peut trouver un entier n et des coefficients $a_i \in A$ tels que

$$(x^{-1})^n + a_{n-1}(x^{-1})^{n-1} + \cdots + a_1 x^{-1} + a_0 = 0.$$

En multipliant par x^{n-1}, on obtient donc

$$\begin{aligned} x^{-1} &= -\left(a_{n-1} + a_{n-2}x + \cdots + a_1 x^{n-2} + a_0 x^{n-1}\right) \\ &\in A[x] \subseteq A, \end{aligned}$$

et A est bien un corps.

3. $\mathfrak{p}$ est l'intersection de deux sous-groupes de $(B,+)$ donc il en est également un. Soit maintenant $p \in \mathfrak{p}$ et $a \in A$. Comme $a \in A$ et $p \in \mathfrak{p} \subseteq A$, le produit ap appartient bien à A. Comme $a \in A \subseteq B$ et $p \in \mathfrak{p} \subseteq \mathfrak{q}$ et que $\mathfrak{q}$ est un idéal de B, on a bien $ap \in \mathfrak{q}$. On a donc bien $ap \in \mathfrak{p}$ et $\mathfrak{p}$ est un idéal de A.

Pour démontrer le critère de maximalité, on va voir que l'anneau $B/\mathfrak{q}$ contient un anneau isomorphe à $A/\mathfrak{p}$ et qu'il est même entier sur cet anneau. La question précédente affirmera alors que $A/\mathfrak{p}$ est un corps si et seulement si $B/\mathfrak{q}$ en est également un, ce qui est bien équivalent au résultat que l'on cherche à démontrer.

Soit

$$\begin{aligned} \varphi : A &\to B/\mathfrak{q} \\ a &\mapsto [a]_{\mathfrak{q}}. \end{aligned}$$

Comme d'habitude, on note $[x]_I$ la classe de x modulo I. Cette application, qui est la composée de l'inclusion $A \to B$ et de la surjection canonique $B \to B/\mathfrak{q}$, est un morphisme d'anneaux. Son noyau est clairement

$$\ker \varphi = \left\{ a \in A \,\middle|\, [a]_{\mathfrak{q}} = 0 \right\} = A \cap \mathfrak{q} = \mathfrak{p}.$$

Le théorème de factorisation montre alors que φ induit un morphisme injectif

$$\overline{\varphi} : A/\mathfrak{p} \to B/\mathfrak{q}.$$

En outre, si $\beta \in B/\mathfrak{q}$, on peut trouver $b \in B$ tel que $\beta = [b]_{\mathfrak{q}}$ et, comme B est entier sur A, des éléments $a_i \in A$ tels que

$$b^n + a_{n_1} b^{n-1} + \cdots + a_1 b + a_0 = 0.$$

Modulo q, on obtient donc

$$\begin{aligned} [b]_{\mathfrak{q}}^n + [a_{n-1}]_{\mathfrak{q}}[b]_{\mathfrak{q}}^{n-1} + \cdots + [a_1]_{\mathfrak{q}}[b]_{\mathfrak{q}} + [a_0]_{\mathfrak{q}} = 0 \\ \text{c'est-à-dire } \beta^n + \varphi(a_{n-1})\beta^{n-1} + \cdots + \varphi(a_1)\beta + \varphi(a_0) = 0, \end{aligned}$$

ce qui montre bien que $B/\mathfrak{q}$ est entier sur $\varphi(A) = \overline{\varphi}(A/\mathfrak{p})$ et conclut la preuve.

Exercice 4.

1. Si le polynôme minimal P est à coefficients dans A_K, $K[s]$ est entier sur A_K, lui-même entier sur A. Mais cela implique que $K[s]$ est entier sur A.
   Réciproquement, si s est entier, il existe un polynôme unitaire $Q \in A[X]$ tel que $Q(s) = 0$. Celui-ci est alors un multiple de P. Toutes les racines de Q dans une clôture algébrique sont entières sur A. Il en va donc de même des racines de P qui en forment un sous-ensemble. D'après les relations coefficients-racine, les coefficients de P s'expriment comme des polynômes à coefficients entiers évalués en les racines de P. Ainsi, les coefficients de P eux-mêmes sont entiers sur K, ce qui implique $P \in A_K[X]$.
   Si A est intégralement clos, $A = A_K$ et le critère est encore plus simple.
2. Les facteurs irréductibles dans K d'un polynôme sont les polynômes minimaux sur K de ses racines dans une clôture algébrique $\overline{K}$. Si $f \in A[X]$ est unitaire, lesdites racines sont toutes entières sur A et le résultat provient directement de (la deuxième partie) de la question précédente.

Exercice 5.

1. Le corps $\mathbf{F}_{16}$ est isomorphe à $\mathbf{F}_2[X]/(P)$, où $P \in \mathbf{F}_2[X]$ est un polynôme irréductible de degré 4. Ceux-ci ont été déterminés à l'exercice 9 du TD 1. On a donc
$$\mathbf{F}_{16} = \mathbf{F}_2[X]/(X^4+X+1) = \mathbf{F}_2[X]/(X^4+X^3+1) = \mathbf{F}_2[X]/(X^4+X^3+X^2+X+1).$$
   On va choisir la première construction et noter $\beta \in \mathbf{F}_{16}$ l'image de X dans le quotient.
2. On va réutiliser les calculs faits dans le corrigé de l'exercice 9 du TD 1. On y avait notamment établi que β était bien un générateur de $\mathbf{F}_{16}^\times$. Ce groupe étant un groupe cyclique d'ordre 15, les autres générateurs sont exactement les β^k, où k décrit $(\mathbf{Z}/15\mathbf{Z})^\times$. En particulier, $\omega = \beta^7$ est un générateur de $\mathbf{F}_{16}^\times$ dont on avait vérifié que le polynôme minimal était X^4+X^3+1.
   Notons que cela implique que si on avait choisi la deuxième construction de $\mathbf{F}_{16}$ et que l'on avait noté ω l'image de X, notre élément ω aurait également été un générateur du groupe cyclique.
   En revanche, si on avait choisi la troisième construction et noté ζ l'image de X, il n'en aurait pas été de même : en effet, racine de $X^4+X^3+X^2+X+1$, ζ vérifie $\zeta^5 = 1$ et est donc d'ordre 5 (et certainement pas générateur) dans $\mathbf{F}_{16}$.
3. Les calculs déjà évoqués montrent que les racines de X^4+X^3+1 dans $\mathbf{F}_{16}$ sont
$$\begin{aligned} \beta^3+1 &= \beta^{14} = \omega^2, \\ \beta^3+\beta+1 &= \beta^7 = \omega, \\ \beta^3+\beta^2+1 &= \beta^{13} = \beta^{28} = \omega^4, \\ \text{et } \beta^3+\beta^2+\beta &= \beta^{11} = \beta^{56} = \omega^8. \end{aligned}$$
   Pour montrer que ces éléments constituent une base, il suffit de les comparer à la base $(1, \beta, \beta^2, \beta^3)$:
$$\det_{\mathbf{F}_2}(\omega^2, \omega, \omega^4, \omega^8) = \begin{vmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{vmatrix} \underset{L_4 \leftarrow L_4+L_1}{=} \begin{vmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{vmatrix} = 1.$$
   On a donc trouvé une $\mathbf{F}_2$-base de l'extension $\mathbf{F}_{16}$ constituée de toutes les racines d'un polynôme irréductible $P \in \mathbf{F}_2[X]$ dont $\mathbf{F}_{16}$ est un corps de décomposition. Une telle base est dite *normale,* et le *théorème de la base normale* affirme qu'il en existe toujours pour une extension normale et séparable.

4. Dans un groupe cyclique d'ordre 15 (noté multiplicativement), le morphisme $x \mapsto x^5$ a pour image les éléments d'ordre 3 et les images réciproques d'un point sont vides ou de la forme $\left\{\zeta z_0 \,\middle|\, \zeta^5 = 1\right\}$. Ici, l'équation n'a donc aucune solution sauf si a est une des racines troisièmes de l'unité (explicitement, 1, $\beta^5 = \beta^2+\beta$ et $\beta^{10} = \beta^2+\beta+1$). Toujours en utilisant nos calculs, on obtient les ensembles de solutions
   - $a = 1$:
   $$\mathscr{S} = \left\{\zeta \,\middle|\, \zeta^5 = 1\right\} = \left\{1, \beta^3, \beta^6, \beta^9, \beta^{12}\right\} = \left\{1, \beta^3, \beta^3+\beta^2, \beta^3+\beta, \beta^3+\beta^2+\beta+1\right\}.$$
   - $a = \beta^5$:
   $$\mathscr{S} = \left\{\beta\zeta \,\middle|\, \zeta^5 = 1\right\} = \left\{\beta, \beta^4, \beta^7, \beta^{10}, \beta^{13}\right\} = \left\{\beta, \beta+1, \beta^3+\beta+1, \beta^2+\beta+1, \beta^3+\beta^2+1\right\}.$$
   - $a = \beta^{10}$
   $$\mathscr{S} = \left\{\beta^2\zeta \,\middle|\, \zeta^5 = 1\right\} = \left\{\beta^2, \beta^5, \beta^8, \beta^{11}, \beta^{14}\right\} = \left\{\beta^2, \beta^2+\beta, \beta^2+1, \beta^3+\beta^2+\beta, \beta^3+1\right\}.$$
   - $a \notin \{1, \beta^5, \beta^{10}\}$:
   $$\mathscr{S} = \varnothing.$$
   On voit que la table des puissances d'un générateur facilite véritablement ce genre de calculs.

Exercice 6. Le morphisme d'anneaux

$$\begin{aligned} \text{év}_{T^2,T^3} : \mathbf{C}[X,Y] &\to \mathbf{C}[T] \\ P &\mapsto P(T^2, T^3) \end{aligned}$$

vérifie clairement

$$\ker \text{év}_{T^2,T^3} \supseteq (Y^2 - X^3).$$

Montrons l'inclusion réciproque. Soit donc $P \in \mathbf{C}[X,Y]$ tel que $P(T^2,T^3) = 0$. Vu comme polynôme en Y à coefficients dans $\mathbf{C}[X]$, le polynôme $Y^2 - X^3$ est unitaire et de degré 2. On peut donc écrire la division euclidienne (cf. TD 0, exercice 4)

$$P = Q(X,Y)(Y^2 - X^3) + R(X,Y),$$

où $R(X,Y)$ est un polynôme en Y, à coefficients dans $\mathbf{C}[X]$, de degré ≤ 1. On peut donc écrire

$$R = R_1(X)Y + R_0, \qquad R_i \in \mathbf{C}[X].$$

En particulier, puisque P et $Y^2 - X^3$ appartiennent à $\ker \text{év}_{T^2,T^3}$, on a

$$R(T^2,T^3) = R_1(T^2)T^3 + R_0(T^2) = 0.$$

Mais le $\mathbf{C}$-espace vectoriel $\mathbf{C}[T]$ possède une décomposition en somme directe

$$\mathbf{C}[T] = \mathbf{C}[T]_{\text{pair}} \oplus \mathbf{C}[T]_{\text{impair}},$$

où

$$\mathbf{C}[T]_{\text{pair}} = \text{Vect}_{\mathbf{C}}(1, T^2, T^4, \ldots) \qquad \text{et} \qquad \mathbf{C}[T]_{\text{impair}} = \text{Vect}_{\mathbf{C}}(T, T^3, T^5, \ldots).$$

Comme $R_1(T^2)T^3 \in \mathbf{C}[T]_{\text{impair}}$ et $R_0(T^2) \in \mathbf{C}[T]_{\text{pair}}$, on a donc $R_1(T^2)T^3 = R_0(T^2) = 0$, ce qui entraîne $R = R_0 = R_1 = 0$ et $P \in Y^2 - X^3$. On a donc bien $\ker \text{év}_{T^2,T^3} = (Y^2 - X^3)$ et le morphisme $\text{év}_{T^2,T^3}$ induit un morphisme injectif

$$\varphi : A = \mathbf{C}[X,Y]/(Y^2 - X^3) \to \mathbf{C}[T].$$

En particulier, A est (isomorphe à) un sous-anneau de $\mathbf{C}[T]$ donc il est intègre.
L'image de φ est clairement égale à $\mathbf{C}[T^2,T^3] \subseteq \mathbf{C}[T]$, le plus petit sous-anneau de $\mathbf{C}[T]$ contenant à la fois T^2 et T^3. Comme tout entier ≥ 2 s'écrit $2u+3v$ pour des entiers $u, v \in \mathbf{N}$, on a

$$\mathbf{C}[T^2,T^3] = \text{Vect}_{\mathbf{C}}\left(T^i, i \neq 1\right).$$

Comme φ induit un isomorphisme entre A et $\mathbf{C}[T^2,T^3]$ (en particulier, l'un est intégralement clos si et seulement si l'autre l'est), on travaille dans la suite directement avec l'anneau $\mathbf{C}[T^2,T^3]$.
Puisque $\mathbf{C}[T^2,T^3]$ est inclus dans le corps $\mathbf{C}(T)$, son corps des fractions s'identifie au sous-corps

$$\left\{\frac{P}{Q}\,\middle|\, P \in \mathbf{C}[T^2,T^3], Q \in \mathbf{C}[T^2,T^3] \setminus \{0\}\right\} \subseteq \mathbf{C}(T).$$

Mais ce sous-corps contient à la fois $\mathbf{C}$ et $T = \dfrac{T^2}{T^3}$, donc il est égal à $\mathbf{C}(T)$ tout entier.
Pour conclure l'exercice, il suffit maintenant de montrer que l'ensemble des éléments de $\mathbf{C}(T)$ entiers sur $\mathbf{C}[T^2,T^3]$ est $\mathbf{C}[T]$. Comme $T \in \mathbf{C}[T] \setminus \mathbf{C}[T^2,T^3]$, cela montrera du même coup que $\mathbf{C}[T^2,T^3]$ n'est pas intégralement clos et que sa clôture intégrale est $\mathbf{C}[T]$. Via l'isomorphisme $A = \mathbf{C}[X,Y]/(Y^2 - X^3) \simeq \mathbf{C}[T^2,T^3]$, on aura donc prouvé les résultats voulus sur A.
Déjà, T est racine du polynôme unitaire

$$U^2 - T^2 \in \left(\mathbf{C}[T^2,T^3]\right)[U]$$

donc il est entier sur $\mathbf{C}[T^2,T^3]$. La clôture intégrale de $\mathbf{C}[T^2,T^3]$ contient donc $\mathbf{C}[T]$. Mais cet anneau, principal et donc factoriel, est intégralement clos. Il s'ensuit donc que la clôture intégrale de $\mathbf{C}[T^2,T^3]$ est bien $\mathbf{C}[T]$.

Exercice 7.

1. Clairement, $K = \mathbf{Q}(\sqrt{p},\sqrt{q})$ est le corps de décomposition du polynôme

   $$(X^2 - p)(X^2 - q) \in \mathbf{Q}[X].$$

   En particulier, $K/\mathbf{Q}$ est une extension normale.

2. Un automorphisme de $\mathbf{Q}(\sqrt{p},\sqrt{q})$ est déterminé par les images de $\sqrt{p}$ et $\sqrt{q}$ qui doivent être racines de $X^2 - p$ et de $X^2 - q$, respectivement. On a donc une injection

   $$\begin{array}{ccc} \text{Aut}_{\mathbf{Q}} K & \to & \{\pm\sqrt{p}\} \times \{\pm\sqrt{q}\} \\ \varphi & \mapsto & (\varphi(\sqrt{p}), \varphi(\sqrt{q})). \end{array}$$

   On a vu lors de l'exercice 8 du TD 1 que le polynôme $X^2 - p$ reste irréductible sur $\mathbf{Q}(\sqrt{q})$ et donc que K est le corps de rupture du polynôme irréductible $X^2 - p \in \mathbf{Q}(\sqrt{q})[X]$. À ce titre, il y a deux plongements $K \to \mathbf{C}$ qui prolongent l'inclusion de $\mathbf{Q}(\sqrt{q})$ dans $\mathbf{C}$, donnés par $\sqrt{p} \mapsto \pm\sqrt{p}$.
   Comme l'image de ces plongements est clairement K lui-même (on pourrait invoquer la normalité de l'extension $K/\mathbf{Q}(\sqrt{q})$, mais c'est vraiment évident ici), il existe un automorphisme σ_1 fixant $\mathbf{Q}(\sqrt{q})$ et échangeant $\sqrt{p}$ et $-\sqrt{p}$.
   De même, il existe un automorphisme σ_2 fixant $\mathbf{Q}(\sqrt{p})$ et échangeant $\sqrt{q}$ et $-\sqrt{q}$. La composée $\sigma_3 = \sigma_2 \circ \sigma_1$ est à la fois différente de σ_1 et σ_2 (par exemple, elle fixe $\sqrt{pq}$). On a

donc bien quatre automorphismes différents (et, d'après l'argument plus haut, exactement quatre)

$$\mathrm{Aut}_{\mathbf{Q}}\,\mathrm{K} = \{\mathrm{id}, \sigma_1, \sigma_2, \sigma_3\}.$$

(Par ailleurs, on voit assez directement que $\sigma_i^2 = \mathrm{id}$, donc le groupe est isomorphe à la *Vierergruppe* de Klein $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.)

On voit ici une instance de la correspondance de Galois : $\mathbf{Q}(\sqrt{p}, \sqrt{q})/\mathbf{Q}$ est une extension normale et séparable, et (donc) ses sous-extensions correspondent aux sous-groupes du groupe (de Galois) $\mathrm{Aut}_{\mathbf{Q}}\,\mathbf{Q}(\sqrt{p}, \sqrt{q})$, chaque sous-extension $\mathrm{L}/\mathbf{Q}$ correspondant au sous-groupe des éléments σ tels que $\sigma_{|\mathrm{L}} = \mathrm{id}_{\mathrm{L}}$.