TD n°8.

1 Résultant

Exercice 1. Soit K un corps. Soit $A = a_n x^n + \cdots + a_0$ et $B = b_m x^n + \cdots + b_0$ deux polynômes de $K[X]$. On considère l'application linéaire Φ de $K_{m-1}[X] \times K_{n-1}[X]$ dans $K_{n+m-1}[X]$, définie par $\Phi(P,Q) = PA + QB$.

a) Montrer que Φ est injective si et seulement si $\operatorname{pgcd}(A,B) = 1$.

b) Montrer que

$$\operatorname{Res}(A,B) := \det \Phi = \begin{vmatrix} a_n & a_{n-1} & \cdots & & & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & a_n & \cdots & & & & \cdots & a_0 & 0 & 0 \\ \vdots & & \ddots & \ddots & & & & & \ddots & \vdots \\ & & & a_n & \cdots & & & & \cdots & a_0 \\ b_m & b_{m-1} & \cdots & \cdots & b_0 & 0 & \cdots & & \cdots & 0 \\ 0 & b_m & \cdots & & \cdots & b_0 & 0 & \cdots & & 0 \\ \vdots & & \ddots & \ddots & & & \ddots & & & \vdots \\ \vdots & & & \ddots & \ddots & & & \ddots & & \vdots \\ 0 & \cdots & & \cdots & b_m & \cdots & & \cdots & & b_0 \end{vmatrix}$$

c) Calculer $\operatorname{Res}(x^7 - a, x^5 - b)$.

Solution. a) Les solutions de $AP + BQ = 0$ sont exactement $(P,Q) = k(B/D, -A/D)$ où $D = \operatorname{pgcd}(A,B)$. Si $D = 1$, alors la seule solution de $\phi(P,Q) = 0$ est $(P,Q) = (0,0)$. Sinon, il y en a une non nulle : $(B/D, -A/D)$.

b) Prenons comme base de $\mathbb{R}_{m-1}[X] \times \mathbb{R}_{n-1}[X]$: $\big((X^{m-1},0),(X^{m-2},0),\ldots,(1,0),(0,X^{n-1}),\ldots,(0,1)\big)$ et comme base de $\mathbb{R}_{m+n-1}[X]$: $\big(X^{n+m-1},\ldots,1\big)$. On a alors les images respectives de la base de départ : $X^{m-1}A,\ldots,A,X^{n-1}B,\ldots,B$. La matrice de ϕ est donc la transposée de

$$\begin{pmatrix} a_n & a_{n-1} & \cdots & & & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & a_n & \cdots & & & & \cdots & a_0 & 0 & 0 \\ \vdots & & \ddots & \ddots & & & & & \ddots & \vdots \\ & & & a_n & \cdots & & & & \cdots & a_0 \\ b_m & b_{m-1} & \cdots & \cdots & b_0 & 0 & \cdots & & \cdots & 0 \\ 0 & b_m & \cdots & & \cdots & b_0 & 0 & \cdots & & 0 \\ \vdots & & \ddots & \ddots & & & \ddots & & & \vdots \\ \vdots & & & \ddots & \ddots & & & \ddots & & \vdots \\ 0 & \cdots & & \cdots & b_m & \cdots & & \cdots & & b_0 \end{pmatrix}$$

c) Considérons le déterminant $\operatorname{Res}(A,B)$ dans $k(X)$. Remplaçons la dernière colonne C_{n+m} par $C_{n+m} + XC_{n+m-1} + \cdots X^{n+m-1}C_1$. On obtient comme coefficients de la dernière colonne :
$(X^{m-1}A,\ldots,A,X^{n-1}B,\ldots,B)$. Développant ce déterminant par raport à la dernière colonne, on a alors

$$\operatorname{Res}(A,B) = A\sum_{i=1}^{m} M_{i,n+m}X^{n-i} + B\sum_{j=1}^{n} M_{j+m,n+m}X^{m-i} = AP + BQ$$

où les $M_{i,j}$ sont les cofacteurs de la matrice M.

d) On en déduit que $\operatorname{Res}(A,B) = 0$ si et seulement si ϕ n'est pas injective, c'est-à-dire si et seulement si $\deg(A,B) \leq 1$. Dans ce cas ils ont une racine commune, racine de leur pgcd.

e) On trouve $a^5 - b^7$. (matrice blocs).

Exercice 2. Soit $A = a_n \prod_{i=1}^{n}(X - \alpha_i)$ et $B = b_m \prod_{i=1}^{m}(X - \beta_i)$.

a) i) Montrer que $\operatorname{Res}(a,B) = a^m$, $\operatorname{Res}(A,b) = b^n$, $\operatorname{Res}(B,A) = (-1)^{nm}\operatorname{Res}(A,B)$.

ii) Montrer que $\mathrm{Res}((X-\alpha)A, B) = B(a)\,\mathrm{Res}(A, B)$.

iii) En déduire que $\mathrm{Res}(A, B) = a_m^n \prod_{i=1}^m B(\alpha_i) = a_m^n b_n^m \prod_{i=1}^m \prod_{j=1}^n (\alpha_i - \beta_j)$..

b) En déduire que $\mathrm{Disc}(A) = \mathrm{Res}(A, A') = \prod_{i=1}^n A'(\alpha_i) = a_m^{2m-2} \prod_{i<j} (\alpha_i - \alpha_j)^2$.

Solution. a) i) *Montrer que* $\mathrm{Res}(a, B) = a^m$, $\mathrm{Res}(A, b) = b^n$, $\mathrm{Res}(B, A) = (-1)^{nm}\,\mathrm{Res}(A, B)$.
Simple calcul. Pour le dernier, il faut intervertir les m premières lignes avec les n dernières. ceci se fait en appliquant le cycle $(1, \ldots, n+m)$ de signature $(-1)^{n+m-1}$, m fois. La signature est donc $(-1)^{(n+m-1)m} = (-1)^{nm}(-1)^{m^2-m} = (-1)^{nm}$.

ii) *Montrer que* $\mathrm{Res}((X-\alpha)A, B) = B(a)\,\mathrm{Res}(A, B)$.
Posons $C = (X-a)A$. Dans la matrice de $\mathrm{Res}(C, B)$, remplaçons, la dernière colonne C_{n+m+1} par $\sum_{i=0}^{n+m} C_{n+m-i} a^i$. On obtient sur la dernière colonne

$$a^m C(a), \ldots, C(a), a^n B(a), \ldots, B(a) = B(a)(0, \ldots, 0, a^n, a^{n-1}, \ldots, 1).$$

On peut mettre $B(a)$ en facteur dans la dernière colonne. Mais $\mathrm{Res}(C, B)$ est un polynôme de degré m en a (1 a sur les m premières lignes). Donc $\mathrm{Res}(C, B) = B(a)\Delta(a) = B(a)\Delta(0)$. Mais $\Delta(0) = \mathrm{Res}(A, B)$.

iii) *En déduire que* $\mathrm{Res}(A, B) = a_m^n \prod_{i=1}^m B(\alpha_i) = a_m^n b_n^m \prod_{i=1}^m \prod_{j=1}^n (\alpha_i - \beta_j)$..
Déduction immédiate de la question précédente.

b) *En déduire que* $\mathrm{Disc}(A) = \mathrm{Res}(A, A') = \prod_{i=1}^n P'(\alpha_i) = a_n^{2n-1}(-1)^{n(n-1)/2} \prod_{i<j} (\alpha_i - \alpha_j)^2$.
Posons $\mathrm{Disc}(A) = \mathrm{Res}(A, A')$. Supposons $A = a_n \prod_{i=1}^n (X - \alpha_i)$. On a alors

$$A' = a_n \sum_{i=1}^n \prod_{i \neq j} (X - \alpha_j)$$

donc $A'(\alpha_i) = a_n \prod_{i \neq j} (\alpha_i - \alpha_j)$ et

$$\mathrm{Disc}(A) = a_n^{n-1} \prod_{i=1}^n A'(\alpha_i) = a_n^{2n-1} \prod_{i \neq j} (\alpha_i - \alpha_j) = a_n^{2n-1}(-1)^{n(n-1)/2} \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

Exercice 3. Soit $A = a_m \prod_{i=1}^m (X - \alpha_i)$ et $B = b_n \prod_{i=1}^n (X - \beta_i)$.

a) Quelles sont les racines de $r(x) = \mathrm{Res}((A(x-y), B(y))$?

b) Construire des polynômes dont les racines sont les α_i^2, les $B(\alpha_i)$.

c) Construire des polynômes dont les racines sont les $\alpha_i - \beta_j$, les $\alpha_i \beta_j$ et les α_i/β_j (si $B(0) \neq 0$).

Solution. a) *Quelles sont les racines de* $r(x) = \mathrm{Res}((A(x-y), B(y))$ *?*
$r(x) = 0$ lorsque $A(x-y)$ et $B(y)$ ont une racine commune. Les racines de $A(x-y)$ sont les $x - \alpha_i$ et celles de $B(y)$ sont les β_j. On obtient $x = \alpha_i + \beta_j$.

b) *Construire des polynômes dont les racines sont les* α_i^2, *les* $B(\alpha_i)$.
Il suffit de considérer $r(x) = \mathrm{Res}(x - y^2, B(y))$ et $r(x) = \mathrm{Res}(x - B(y), A(y))$.

c) *Construire des polynômes dont les racines sont les* $\alpha_i - \beta_j$, *les* $\alpha_i\beta_j$ *et les* α_i/β_j *(si* $B(0) \neq 0$*).*
On prend $r(x) = \mathrm{Res}(A(x+y), B(y))$, $r(x) = res(y^n A(x/y), B(y))$, $r(x) = \mathrm{Res}(A(xy), B(y))$.

Exercice 4. Soient K un corps de caractéristique 0 et α, β deux éléments algébriques sur K. Soit $\alpha_1 = \alpha, \ldots, \alpha_n$ et $\beta_1 = \beta, \ldots, b_m$ les racines des polynômes minimaux A et B de α et β.

a) Montrer qu'il existe $n \in \mathbb{Z}$ tel que les $\alpha_i + n\beta_j$ soient tous distincts.

b) Trouver un polynôme annulateur C, sans facteur carré, de $\gamma = \alpha + n\beta$.

c) Soit $L = K(\gamma)$. Que vaut $\mathrm{pgcd}(A(\gamma - nX), B(X))$ dans $L[X]$?

d) En déduire que $K(\alpha, \beta) = K(\gamma)$.

e) En déduire que toute extension finie de corps de caractéristique 0 admet un élément primitif.

Solution. a) Si $\alpha_i + t\beta_j = \alpha_k + t\beta_l$, alors, $\beta_j \neq \beta_l$, sinon $\alpha_i = \alpha_k$. Donc $t = \frac{\alpha_i - \alpha_k}{\beta_l - \beta_j}$. Il n'y en a qu'un nombre fini. Tout autre t convient. Une autre méthode : le polynôme $r(x) = \mathrm{Res}(A(x - ty), B(y))$ a pour racines les $\alpha_i + t\beta_j$. $\mathrm{Disc}(r(x))$ est un polynôme en t qui a un nombre fini de racines. Pour $t = n$ assez grand il n'est pas nul et toutes les racines sont distinctes.

b) On prend $C(x) = \mathrm{Res}(A(x - ny), B(y))$, dont les racines sont $\alpha_i + t\beta_j$, toutes distinctes.

c) $D = \mathrm{pgcd}(A(\gamma - nX), B(X))$ a pour racine les racines communes de B et de $A(\gamma - nX)$. D'un côté, ce sont les β_j, de l'autre les x tels que $\gamma - nx = \alpha_i$. On doit donc avoir $\gamma - n\beta_j = \alpha_i$, soit $\gamma = \alpha_i + n\beta_j$. On a donc $x = \beta_1 = \beta$. On a donc $D(X) = X - \beta$

d) On déduit alors que $\beta = -D(0) \in K(\gamma)$. Puis $\alpha = \gamma + D(0)$. D'où $K(\alpha, \beta) \subset K(\gamma)$.

2 Séparabilité

Exercice 5. Soient X et Y deux indéterminées et p un nombre premier. On pose

$$K = \mathbb{F}_p(X^p, Y^p) \quad \text{et} \quad L = \mathbb{F}_p(X, Y).$$

(ı) Montrer que L est une extension finie de K de degré p^2.
(ıı) Montrer qu'il n'existe pas d'élément $\theta \in L$ tel que $L = K(\theta)$.

Solution. (ı) L'élément X est algébrique sur K de degré p. En effet, considérons le polynôme $F = T^p - X^p \in K[T]$. On a $F = (T - X)^p$, de sorte que X est la seule racine de F dans une clôture algébrique de K. Puisque X n'appartient pas à K, l'élément X^p n'est pas une puissance p-ième dans K. D'après l'exercice **??**, F est donc irréductible sur K, et est ainsi le polynôme minimal de X sur K. De même, Y est algébrique sur $K(X)$ de degré p, comme on le constate en considérant le polynôme $T^p - Y^p \in K(X)[T]$ qui est irréductible sur $K(X)$. Compte tenu du fait que l'on a $L = K(X, Y)$, on en déduit le résultat.
(ıı) Supposons qu'il existe $\theta \in L$ tel que $L = K(\theta)$. Il existe des éléments F et G dans $\mathbb{F}_p[X, Y]$ tels que l'on ait

$$\theta = \frac{F(X, Y)}{G(X, Y)}.$$

Puisque L est de caractéristique p, on a

$$\theta^p = \frac{F(X^p, Y^p)}{G(X^p, Y^p)},$$

et donc θ^p appartient à K. On en déduit que le degré de θ sur K est au plus p, ce qui contredit le fait que L/K soit de degré p^2. D'où le résultat.

Exercice 6. Soient K un corps , $F = X^3 - 3X - 1 \in K[X]$ et α une racine de F dans une clôture algébrique de K. Montrer que $K(\alpha)$ est une extension séparable de K.

Solution. Supposons la caractéristique de K différente de 3. Le polynôme dérivé de F, qui est $3(X^2 - 1)$, est premier avec F, ce qui montre que F est séparable dans ce cas et donc que α est séparable sur K. Si la caractéristique de K vaut 3, on a $F = (X - 1)^3$, d'où $\alpha = 1$ puis $K(\alpha) = K$.

Exercice 7. Soient K un corps de caractéristique un nombre premier p et f un polynôme irréductible sur K. Montrer que f n'est pas séparable si et seulement si il existe g dans $K[X]$ tel que $f(X) = g(X^p)$.

Solution. Si f est de la forme $g(X^p)$, le polynôme dérivé de f est nul, donc f est inséparable. Inversement, supposons f inséparable. Posons $f = \sum_{i=0}^{n} a_i X^i$. On a

$$f' = \sum_{i=1}^{n} i a_i X^{i-1}.$$

D'après l'hypothèse faite, on a $f' = 0$, d'où $ia_i = 0$ pour $i = 1, \cdots, n$. Si a_i n'est pas nul, i est donc divisible par p, ce qui entraîne le résultat.

Exercice 8. Soient K un corps de caractéristique un nombre premier p et L une extension finie de K de degré non divisible par p. Montrer que L est séparable sur K.

Solution. Soient α un élément de L et F son polynôme minimal sur K. Il s'agit de montrer que F est séparable. Dans le cas contraire, F étant irréductible, il existe $G \in K[X]$ tel que $F(X) = G(X^p)$ (exercice 7). Il en résulte que le degré de F est multiple de p, par suite p divise le degré de L sur K. D'où une contradiction et le résultat.

Exercice 9. Soient $K = \mathbb{F}_p(X)$ et $P = t^p - X$. Montrer que P n'est pas séparable.

Solution. On a $P' = 0$. P est irréductible dans $k[X]$. En effet, si $P = P_1 \cdot P_2$, alors $P_1(0)P_2(0) = X$, donc $P_1(0) = X$, par exemple. Mais, si α est une racine de P, alors dans $K(\alpha)$, on a $P = t^p - \alpha^p = (t - \alpha)^p$. Donc $P_1 = (t - \alpha)^n$ et $X = \alpha^n = \alpha^p$, donc $p = n$ et $P_1 = P$. P est irréductible dans $k[X]$ donc aussi dans $k(X)$ (lemme de Gauss) et donc non séparable.

3 Extensions galoisiennes

Exercice 10. Soit $n \in \mathbb{N}^*$. Soit $\Phi_n = \prod_{k\in(\mathbb{Z}/n\mathbb{Z})^*}(X - e^{2i\pi k/n}) \in \mathbb{C}[X]$.

a) Montrer que $X^n - 1 = \prod_{d|n} \Phi_d$. En déduire que $\Phi_n \in \mathbb{Z}[X]$.

b) Soit ζ une racine primitive n^{e}de 1 et p un nombre premier premier à n. Soit f et g les polynômes minimaux unitaire sur $\mathbb{Q}$ de ζ et $\zeta' = \zeta^p$. On suppose $f \neq g$.

i) Montrer que $fg|\Phi_n$ et $f|g(X^p)$.

ii) Montrer que l'image de Φ_n dans $\mathbb{F}_p[X]$ a un facteur irréductible ayant multiplicité au moins deux, et en déduire une contradiction.

c) En déduire que Φ_n est un polynôme irréductible.

d) Montrer que $\mathbb{Q}(e^{2i\pi/n})$ est une extension galoisienne de $\mathbb{Q}$ et décrire son groupe de Galois.

e) Soit K une extension finie de $\mathbb{Q}$. Montrer que K ne contient qu'un nombre fini de racines de 1.

Solution. a) Soit μ_∞ le groupe multiplicatif des racines de 1, $\mu^{(n)}$ l'ensemble des éléments de μ_∞ dont l'ordre multiplicatif est n, et μ_n l'ensemble des racines n^{es}de 1 (c'est-à-dire dont l'ordre multiplicatif divise n). Alors $X^n - 1 = \prod_{\zeta\in\mu_n}(X - \zeta)$ et $\Phi_n = \prod_{\zeta\in\mu^{(n)}}(X - \zeta)$. Or μ_n est l'union disjointe des $\mathfrak{m}^{(d)}$ pour d divisant n, donc

$$X^n - 1 = \prod_{\zeta\in\mu_n}(X - \zeta) = \prod_{d|n}\prod_{\zeta\in\mu^{(d)}}(X - \zeta) = \prod_{d|n}\Phi_d.$$

Φ_n est le quotient de $X^n - 1 \in \mathbb{Z}[X]$ par $\prod_{d|n,d\neq n}\Phi_d$, qui par récurrence est un polynôme unitaire de $\mathbb{Z}[X]$, donc la division euclidienne par un polynôme unitaire, nous dit que Φ_n est à coefficient s dans $\mathbb{Z}$.

b) i) Comme $\Phi_n(\zeta) = 0$, $f|\Phi_n$, de même $g|\Phi_n$. Or, en tant que polynômes minimaux, f et g sont irréductibles, donc l'hypothèse $f \neq g$ implique qu'ils sont premiers entre eux. Donc $fg|\Phi_n$.
De même, $g(\zeta^p) = 0$, donc ζ est une racine de $g(X^p)$ donc $f|g(X^p)$.

ii) Soit h un facteur irréductible de $\bar{f}$. Donc $h|\bar{f}|\bar{g}(X^p) = \bar{g}^p$. Comme h est irréductible, $h|g$. Donc $h^2|fg|\Phi_n|X^n - 1$. Donc $h|\gcd(X^n - 1, nX^{n-1}) = 1$ car n est premier à p. Contradiction.

c) Soit k premier à n, et soit $k = \prod_i p_i^{\alpha_i}$. En appliquant b) $\sum_i \alpha_i$ fois, on en déduit que $e^{2i\pi k/n}$ est racine du polynôme minimal f de $e^{2i\pi/n}$. Donc $\Phi_n|f$ et donc Φ_n est bien irréductible.

d) Si x est un conjugué de $\zeta = e^{2i\pi/n}$, alors x est une racine de Φ_n, donc de la forme $e^{2i\pi k/n} = \zeta^k \in \mathbb{Q}(\zeta)$. Donc $\mathbb{Q}(\zeta)$ contient tous les conjugués de ζ donc est une extension normale de $\mathbb{Q}$. Comme on est en caractéristique 0, c'est une extension galoisienne.
Soit $G = \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. D'après la question précédente, les conjugués de ζ sont exactement les ζ^k avec $k \in (\mathbb{Z}/n\mathbb{Z})^\times$. Il existe donc $g_k \in G$ tel que $g(\zeta) = \zeta^k$, unique puisque $\mathbb{Q}(\zeta)$ est engendrée par ζ. Donc $G = \{g_k\}_{k\in(\mathbb{Z}/n\mathbb{Z})^\times}$. Décrivons la loi de groupe de G. On a $g_k g_{k'}(\zeta) = g_k(\zeta^{k'}) = g_k(\zeta)^{k'} = \zeta^{kk'}$. Donc la bijection $(\mathbb{Z}/n\mathbb{Z})^\times \to G$ qui envoie k sur g_k est un isomorphisme de groupe. Donc $G \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.

Exercice 11. Soit a un entier sans facteur carré, différent de $0, 1$ et -1. Soit p un nombre premier. Soit K un corps de décomposition de $X^p - a$ sur $\mathbb{Q}$. Calculer $[K : \mathbb{Q}]$.
Soit $G = \text{Gal}(K/\mathbb{Q})$. Montrer que G a un sous-groupe distingué H isomorphe à $\mathbb{Z}/p\mathbb{Z}$ tel que G/H soit isomorphe à $(\mathbb{Z}/p\mathbb{Z})^*$.

Solution. Le polynôme $X^p - a$ est irréductible d'après le critère d'eisenstein, donc si α est une racine p^{e}de a, $\mathbb{Q}(\alpha)/\mathbb{Q}$ est une extension de degré p.
Soit $\zeta = e^{2i\pi/p}$. Alors les conjugués de α sont les $\alpha_k = \zeta^k\alpha$, avec $k \in \mathbb{Z}/p\mathbb{Z}$. Donc $\zeta = \alpha_1/\alpha_0 \in K = \mathbb{Q}(\alpha_0, \cdots, \alpha_{p-1})$. Réciproquement $\alpha_k \in \mathbb{Q}(\alpha, \zeta)$, donc $K = \mathbb{Q}(\alpha, \zeta)$.
Or $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$ est premier à $p = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ donc $[K : \mathbb{Q}] = [\mathbb{Q}(\zeta) : \mathbb{Q}][\mathbb{Q}(\alpha) : \mathbb{Q}] = p(p - 1)$.
Comme $\mathbb{Q}(\zeta)/\mathbb{Q}$ est une extension galoisienne de groupe de Galois $N = (\mathbb{Z}/p\mathbb{Z})^\times$, $N = G/H$ où $H = \text{Gal}(K : \mathbb{Q}(\zeta))$. Comme $[\mathbb{Q}(\zeta)(\alpha) : \mathbb{Q}(\zeta)] = [\mathbb{Q}(\alpha) : \mathbb{Q}]$, $X^p - a$ est encore le polynôme minimal de α dans $\mathbb{Q}(\zeta)[X]$, donc les conjugués de α sont les α_k. Comme dans l'exercice précédent, il existe un unique $h_k \in H$ tel que $h_k(\alpha) = \alpha_k$ et l'application $\phi : \mathbb{Z}/p\mathbb{Z} \to H$ qui envoie k sur h_k est donc bijective. Or $h_{k'}h_k(\alpha) = h_{k'}(\zeta^k\alpha) = \zeta^k h_{k'}(\alpha) = \zeta^{k+k'}\alpha$, ce qui prouve que ϕ est un isomorphisme de groupe.

Exercice 12. Soit $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. Montrer que K est une extension galoisienne de $\mathbb{Q}$ et décrire son groupe de Galois.

Solution. Comme les conjugués de $\sqrt{d}$ sont $\pm\sqrt(d)$ (si d n'est pas un carré), K contient les conjugués de $\sqrt{2}, \sqrt{3}$ et $\sqrt{5}$ donc est galoisienne.
$\mathbb{Q}(\sqrt(d))/\mathbb{Q}$ est une extension galoisienne de groupe de Galois $G_d = \{1, \sigma_d\}$ où $\sigma(a + b\sqrt{d}) = a - b\sqrt{d}$.
Si $\sqrt(3) \in \mathbb{Q}(\sqrt(2)$, on aurait $\sigma_2(\sqrt{3}) = \pm\sqrt{3}$, et donc $\sqrt{3} \in \mathbb{Q}$ ou $\in \mathbb{Q}\sqrt{2}$, ce qui n'est pas possible. Donc $[\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}] = 4$ et a pour groupe de galois $G_2 \times G_3 \simeq \{\pm 1\}^2$ où $(e, f)(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + be\sqrt{2} + cf\sqrt{3} + def\sqrt{6}$ si $e, f \in \{\pm 1\}$.
Si $\sqrt{5} \in \mathbb{Q}(\sqrt{3}, \sqrt{2})$, on aurait un morphisme de groupe (surjectif) $\chi : G_2 \times G_3 \to \mathbb{Z}/2\mathbb{Z}$ tel que $\sigma(\sqrt{5}) = (-1)^{\chi(\sigma)}\sqrt{5}$. Or $\{x \in \mathbb{Q}(\sqrt{3}, \sqrt{2}), \sigma(x) = (-1)^{\chi(\sigma)}x\} = \sqrt{2^{\chi(\sigma_2)}3^{\chi(\sigma_3)}}\mathbb{Q}$ et donc $5 \in 2^{\chi(\sigma_2)}3^{\chi(\sigma_3)}(\mathbb{Q}^\times)^2$, ce qui n'est pas possible d'après l'unicité de la factorisation en facteurs premiers.
Donc $\mathbb{Q}(\sqrt{5}, \sqrt{3}, \sqrt{2})$ est une extension galoisienne de degré 8 de $\mathbb{Q}$, et son groupe de Galois est $(\mathbb{Z}/2\mathbb{Z})^3$.

Exercice 13. Soient f un polynôme irréductible de $\mathbb{Q}[X]$ et K le corps de décomposition de f dans $\mathbb{C}$. On suppose que le groupe de Galois de K sur $\mathbb{Q}$ est abélien. Montrer que pour toute racine α de f, on a $K = \mathbb{Q}(\alpha)$.

Solution. Posons $G = \mathrm{Gal}(K/\mathbb{Q})$. Soient α une racine de f dans $\mathbb{C}$ et σ un élément de $\mathrm{Gal}\big(K/\mathbb{Q}(\alpha)\big)$. Soit τ un élément de G. On a $\tau(\alpha) = \tau \circ \sigma(\alpha)$, d'où puisque G est abélien, $\sigma \circ \tau(\alpha) = \tau(\alpha)$. L'extension $K/\mathbb{Q}(\alpha)$ étant galoisienne, on en déduit que $\tau(\alpha)$ est dans $\mathbb{Q}(\alpha)$. Par ailleurs, f étant irréductible, G agit transitivement sur l'ensemble des racines de f. Autrement dit, pour toute racine β de f il existe $\tau \in G$ tel que $\tau(\alpha) = \beta$. Ainsi, les racines de f sont dans $\mathbb{Q}(\alpha)$, d'où $K = \mathbb{Q}(\alpha)$.