Sur le polynôme minimal de la somme et du produit de deux nombres algébriques

1) Introduction

L'ensemble des nombres complexes algébriques sur Q étant un corps, si a et b sont deux nombres algébriques sur Q de polynômes minimaux respectifs P_1 et P_2, et si f est une fonction rationnelle à coefficients dans Q, $f(a,b)$ est aussi un nombre algébrique sur Q et donc admet un polynôme minimal $P_{f(a,b)}$.

En général, lorsque (a,b) parcourt tous les couples possibles (racine de P_1, racine de P_2), le polynôme minimal $P_{f(a,b)}$ obtenu n'est pas forcément unique (de nombreux exemples seront donnés).

Pour $f(a,b) = a+b$ ou ab, le nombre de ces polynômes minimaux est le nombre de facteurs irréductibles apparaissant dans la décomposition en facteurs irréductibles sur $Q[X]$ d'un résultant : ce résultant est $R_1(X) = res_Y(P_1(Y), P_2(X-Y))$ pour $a+b$ et $R_2(X) = res_Y(P_1(Y), Y^{d°P_2}P_2(\frac{X}{Y}))$ pour ab.

Ces deux résultants ont pour degré le produit des degrés de P_1 et P_2.

Par exemple (c'est l'exemple 3 du 6)), si $P_1(X) = X^2 - 2$ et $P_2(X) = X^4 + 1$, alors le polynôme minimal de $a+b$ est soit $X^4 - 8X^2 + 25$, soit $X^4 + 1$ (cad P_2)

C'est d'ailleurs en voyant dans une revue mathématique l'oubli du cas où $a+b$ a pour polynôme minimal X^4+1 que je me suis mis à faire cette étude.

Pour $f(a,b) = a+b$, grâce au théorème d'Isaac, on montre facilement que si les degrés de P_1 et P_2 sont premiers entre eux, tout $a+b$ a le même minimal qui est, au signe près $R_1(X)$.

Par contre, pour $f(a,b) = ab$, le fait que les degrés de P_1 et P_2 soient premiers entre eux n'implique pas à priori que tous les ab aient le même polynôme minimal qui soit $\pm R_2$.

Je donne cependant ici des conditions suffisantes supplémentaires qui permettent de le dire.

Par contre, je n'ai pas trouvé d'exemple avec $d°P_1$ et $d°P_2$ premiers entre eux et ab ayant plusieurs polynômes minimaux : j'ai seulement trouvé un cas (exemple 4 du 5)) où ab a un seul polynôme minimal qui n'est pas $\pm R_2$, mais P_2 : $P_1(X) = X^2 + X + 1$, $P_2(X) = X^3 - 2$.

2) Quelques rappels sur nombres algèbriques.

2.1) Rappelons la définition d'un nombre algébrique sur le corps Q des rationnels : c'est un nombre complexe racine d'un polynôme, non nul, à coefficients dans Q.

Soit a un nombre algébrique sur Q : l'ensemble des polynômes $P \in Q[X]$ tels que $P(a) = 0$ est un idéal I (non nul) principal (car $Q[X]$ est euclidien).

Donc I admet un seul générateur unitaire, appelé le polynôme minimal de a : outre le fait que ce polynôme minimal est un diviseur de tout polynôme de $Q[X]$ ayant a comme racine, il est irréductible sur $Q[X]$.

En fait si $P \in Q[X]$ est irréductible, unitaire, et tel que $P(a) = 0$, c'est le polynôme minimal de a sur Q.

Rappelons aussi que tout polynôme de $Q[X]$ irréductible de degré d a d racines distinctes dans C et deux polynômes irréductibles unitaires distincts n'ont aucune racine

commune (sinon cette racine commune aurait deux polynômes minimaux).

2.2) Si a est algébrique, on appelle degré de a (sur Q), le degré d de son polynôme minimum et $Q(a)$, le plus petit corps contenant Q et a, est un Q – espace vectoriel de dimension finie d, dimension qui est notée $[Q(a) : Q]$ et est appelée le degré de l'extension $Q \subset Q(a)$. Une base de ce Q – espace vectoriel est $\{1; a; a^2; \ldots; a^{d-1}\}$.

2.3) Soient a et b deux nombres algébriques sur Q et $Q(a,b)$ le plus petit corps contenant Q et a et b.
$Q(a,b)$ est un Q –espace vectoriel : comme ci-dessus sa dimension, finie, est appelée le degré de l'extension de corps $Q \subset Q(a,b)$ et est notée $r = [Q(a,b) : Q]$.
Un résultat très utile est la multiplication des degrés :
$[Q(a,b) : Q] = [Q(a)(b) : Q(a)][Q(a) : Q] = [Q(b)(a) : Q(b)][Q(b) : Q]$.

Soit L un corps extension de $\mathbb{Q}$, telle que $[L : \mathbb{Q}] = d$: alors tout élément de L est algébrique sur $\mathbb{Q}$, son degré divisant d.

En outre, si d est le degré de a sur Q et si d' est le degré de b sur $Q(a)$, alors, cf le 2.2)
$\{1; a; a^2; \ldots; a^{d-1}\}$ est une base du Q – espace vectoriel $Q(a)$ et
$\{1; b; b^2; \ldots; b^{d'-1}\}$ est une base du $Q(a)$ – espace vectoriel $Q(a)(b)$ et alors la multiplication des degrés dit aussi que
les $a^i b^j$ pour $0 \leq i \leq d-1$ et $0 \leq j \leq d'-1$ forment une base du Q – espace vectoriel $Q(a)(b) = Q(a,b)$.

2.4) Voici une première méthode pour trouver un polynôme annulateur de $u \in Q(a,b)$ à partir du fait que $Q(a,b)$ est un espace vectoriel de dimension finie sur Q (voir 2.3).
En notant $r = [Q(a,b) : Q]$, pour tout $u \in Q(a,b)$, $1, u, u^2, \ldots, u^r$ est une famille de $r+1$ vecteurs, donc cette famille est Q –liée et ainsi il existe $r+1$ rationnels λ_i non tous nuls tels que $\sum_{i=0}^{r} \lambda_i u^i = 0$, c'est-à-dire $P(X) = \sum_{i=0}^{r} \lambda_i X^i$ est un polynôme de $Q[X]$, non nul, et annulateur de u : ceci prouve que tout élément de $Q(a,b)$ est algébrique sur Q et est de degré $\leq r$ (puisque son polynôme minimal divise P).
En prenant $u = a \pm b$, $u = ab$, $u = \frac{a}{b}$ $(b \neq 0)$, on prouve que l'ensemble des nombres algébriques sur Q est un corps. .
Pour trouver en pratique ce polynôme P annulateur de u, c'est-à-dire trouver les coefficients λ_i, on peut décomposer u dans une base de $Q(a,b)$ (les $a^i b^j$,)*voir* 2.3) pour obtenir un systéme linéaire de r inconnues (les $\lambda_i \in Q$) et $r+1$ équations homogénes (voir les exemples 5 et 7 du paragraphe 6).

Reste bien sûr à trouver le polynôme minimal de u qui est un des facteurs irréductibles sur $Q[X]$ de P.

On a vu ci-dessus que le degré de tout élément u de $Q(a,b)$ est $\leq r = [Q(a,b) : Q]$: en fait c'est un diviseur de r (utiliser la multiplicatrion des degrés) et donc le polynôme minimal de u est un facteur irréductible de P dont le degré est un diviseur de r.

On verra en annexe 1 les critères d'irréductibilité utilisés ici ; **lorsque je parlerai d'irréductibilité d'un polynôme sans autre précision**, **il s'agira de l'irréductibilité sur** $Q[X]$).

3) Recherche d'un polynôme annulateur de $a+b$ et ab à l'aide de la notion de résultant.

Soient P_1 et P_2 les polynômes minimaux respectifs de a et b sur $Q[X]$ et de degrés respectifs $n_1 \geq 1$ et $n_2 \geq 1$:
$P_1(X) = X^{n_1} + \alpha_{n_1-1}X^{n_1-1} + \ldots + \alpha_1 X + \alpha_0$
$P_2(X) = X^{n_2} + \beta_{n_2-1}X^{n_2-1} + \ldots + \beta_1 X + \beta_0$

Note : **dans tout ce qui suit**, a **désignera une racine quelconque** (**dans** $\mathbb{C}$) **de** P_1 **et** b **désignera une racine quelconque** (**dans** $\mathbb{C}$) **de** P_2.

3.1) **Si l'un des polynômes** P_1 **ou** P_2 **est de degré** 1, il est immédiat de trouver en fait le polynôme minimal de $a+b$ et de ab.
Par exemple si $n_1 = 1$, donc $P_1(X) = X + \alpha_0$, alors
$a+b$ prend n_2 valeurs (les n_2 valeurs de $-\alpha_0 + b$) qui ont toutes pour polynôme minimal $P_2(X+\alpha_0)$, de degré n_2
et
si $\alpha_0 = 0$, ab prend une seule valeur 0 qui a pour polynôme minimal X
si $\alpha_0 \neq 0$, ab prend n_2 valeurs (les n_2 valeurs de $-\alpha_0 b$) qui ont toutes comme polynôme minimal $(-\alpha_0)^{n_2}P_2(\frac{X}{-\alpha_0})$, de degré n_2.

Exemple : $P_1(X) = X - 1, P_2(X) = X^4 + X^3 + X^2 + X + 1$ (il s'agit du polynôme cyclotomique Φ_5, polynôme minimal des racines 5 –ièmes de 1 autres que 1).
Donc le polynôme minimal de tout $1+b$ est $P_2(X-1) = X^4 - 3X^3 + 4X^2 - 2X + 1$.

3.2) **A partir de maintenant**, **on supposera toujours** $n_1 \geq 2$ **et** $n_2 \geq 2$:
P_1 et P_2 étant irréductibles, α_0 et β_0 sont donc non nuls.

Cas $a+b$: le résultant des deux polynômes en Y, $P_1(Y)$ et $P_2(X-Y)$ est un polynôme $R_1 \in Q[X]$, annulateur de $a+b$, puisque $R_1(a+b)$ est le résultant des deux polynômes $P_1(Y)$ et $P_2(a+b-Y)$, lesquels ont a comme racine commune. On retrouve le fait que $a+b$ est effectivement algébrique sur Q.

Cas ab : le résultant des deux polynômes en Y, $P_1(Y)$ et $Y^{n_2}P_2(\frac{X}{Y})$ (voir son écriture polynomiale en remarque 1) est un polynôme $R_2 \in Q[X]$, annulateur de ab, puisque $R_2(ab)$ est le résultant des deux polynômes $P_1(Y)$ et $Y^{n_2}P_2(\frac{ab}{Y})$, lesquels ont a comme racine commune : si $a \neq 0$ c'est évident car $Y^{n_2}P_2(\frac{ab}{Y})$ prend, pour $Y = a$, la valeur $a^{n_2}P_2(b) = 0$, mais pour $a = 0$, cf la remarque 1, $Y^{n_2}P_2(\frac{ab}{Y}) = \beta_0 Y^{n_2}$ qui prend, pour $Y = a = 0$, la valeur 0.
Là aussi on retrouve le fait que ab est effectivement algébrique sur Q.

Remarque 1 : $Y^{n_2}P_2(\frac{X}{Y}) = X^{n_2} + \beta_{n_2-1}X^{n_2-1}Y + \ldots + \beta_1 XY^{n_2-1} + \beta_0 Y^{n_2}$; comme $\beta_0 \neq 0$ (car P_2 est irréductible et $n_2 \geq 2$), $Y^{n_2}P_2(\frac{X}{Y})$ est un polynôme en Y de même degré que P_2.
Remarque 2 : voir 4.0 et 4.1 pour des résultats complémentaires sur ces deux résultants, notamment leur degré est $n_1 n_2$, et donc leur calcul peut nécessiter l'utilisation d'un logiciel.
Remarque 3 : on verra au R5 de l' annexe 2 que si $n_1 = 1$ (donc pas ≥ 2), tout $a+b$ a pour polynôme minimal $(-1)^{n_1 n_2}R_1$ et si $\alpha_0 \neq 0$ (cad $P_1(X) \neq X$) tout ab a pour polynôme minimal $(-1)_2^{n_1 n_2}R_2$. Cette remarque compléte donc le 3.1) en termes de résultants.

4) **Propriétés**.

Dans tout ce qui suit, a et b sont respectivement une racine quelconque des polynômes P_1 (coefficients α_i) et P_2 (coefficients β_i), unitaires et irréductibles sur $Q[X]$ et de **degrés respectifs** $n_1 \geq 2$ et $n_2 \geq 2$: cad a pour polynôme minimal P_1 et b a pour polynôme minimal P_2.
On notera $R_1(X) = res_Y(P_1(Y), P_2(X-Y))$ et $R_2(X) = res_Y(P_1(Y), Y^{n_2}P_2(\frac{X}{Y}))$ les deux résultants introduits au 3.2).

4.0) R_1 et $R_2 \in Q[X]$, ils sont tous les deux de degré $n_1 n_2$, et ont comme coefficient de tête $(-1)^{n_1 n_2}$. Donc $(-1)^{n_1 n_2}R_1$ et $(-1)^{n_1 n_2}R_2$ sont unitaires.
4.1)
4.1.1) cas $a+b$

tout $a+b$ est racine de R_1 (voir 3.2)) mais aussi, toute racine de R_1 est un $a+b$ et donc, les $n_1 n_2$ racines (comptées avec leur multiplicité) de R_1 sont les $n_1 n_2$ nombres $a+b$ obtenus à partir des $n_1 n_2$ couples, distincts, (a,b) où a est une racine de P_1 et b une racine de P_2.

tout conjugué d'un $a+b$ est aussi un $a+b$, cad tout conjugué d'un $a+b$ s'écrit $a'+b'$ avec a' racine de P_1, b' racine de P_2

si la décomposition en facteurs irréductibles (dans $Q[X]$) de R_1 est $R_1(X) = (-1)^{n_1 n_2}\prod_{i=1}^{I} U_i^{k_i}$ (avec les U_i irréductibles et unitaires), alors l'ensemble des valeurs (distinctes) prises par $a+b$ est l'ensemble des racines (distinctes) dans C de R_1, cad l'ensemble des $d°U_1 + d°U_2 + \ldots + d°U_I$ racines des U_i dans C, tout valeur possible de $a+b$ ayant pour polynôme minimal un des U_i.

$a_1, a_2, \ldots, a_{n_1}$ étant les racines de P_1, $b_1, b_2, \ldots, b_{n_1}$ celles de P_2,

$R_1(X) = (-1)^{n_1 n_2}\prod_{\substack{i=1,\ldots,n_1 \\ j=1,\ldots,n_2}} (X-(a_i+b_j))$: ainsi si $a+b$ est une racine de R_1, sa multiplicité est le nombre de couples (a_i, b_j) tels que $a_i + b_j = a+b$.

Exemple : si $P_1(X) = P_2(X) = X^2 - 2$, alors $R_1(X) = X^2(X^2-8)$ et les quatre couples possibles (a,b) donnent trois valeurs distinctes pour $a+b$: 0 de polynôme minimal X et $-\sqrt{2}$ et $\sqrt{2}$ qui elles ont X^2-8 comme polynôme minimal

"Certains" $a+b$ prennent la valeur $0 \Leftrightarrow P_1(X) = P_2(-X) \Leftrightarrow X$ est un facteur (irréductible) de R_1

R_1 est irréductible (cad $I = 1 = k_1$) $\Leftrightarrow$ il existe un $a+b$ de degré $n_1 n_2$ $\Leftrightarrow$ il y a $n_1 n_2$ valeurs possibles pour $a+b$ ayant toutes R_1 (au signe près) comme polynôme minimal, donc toutes de degré $n_1 n_2$.

Remarque : $a+b$ prend $n_1 n_2$ valeurs distinctes n'entraîne pas que R_1 soit irréductible : voir exemples 6,7,8 du 6) où dans ce cas R_1 est le produit de deux facteurs irréductibles.
Il peut arriver que l'un des P_i divise R_1 : voir l'exemple 3 du 6) et l'exemple $P_1(X) = P_2(X) = X^6 + \alpha_0$ du 7.3.2).

4.1.2) cas ab

tout ab est racine de R_2 (voir 3.2)) mais aussi, toute racine de R_2 est un ab
et donc, les $n_1 n_2$ racines (comptées avec leur multiplicité) de R_2 sont les $n_1 n_2$ nombres ab obtenus à partir des $n_1 n_2$ couples, distincts, (a,b) où a est une racine de P_1 et b une racine de P_2.

tout conjugué d'un ab est aussi un ab, cad tout conjugué d'un ab s'écrit $a'b'$ avec a' racine de P_1, b' racine de P_2

si la décomposition en facteurs irréductibles (dans $Q[X]$) de R_2 est $R_2(X) = (-1)^{n_1 n_2} \prod_{i=1}^{I} V_i^{k_i}$ (avec les V_i irréductibles et unitaires), alors l'ensemble des valeurs (distinctes) prises par ab est l'ensemble des racines (distinctes) dans C de R_2, cad l'ensemble des $d°V_1 + d°V_2 + \ldots + d°V_I$ racines des V_i dans C, toute valeur possible de ab ayant pour polynôme minimal un des V_i.

$a_1, a_2, \ldots, a_{n_1}$ étant les racines de P_1, $b_1, b_2, \ldots, b_{n_1}$ celles de P_2,

$R_2(X) = (-1)^{n_1 n_2} \prod_{\substack{i=1,\ldots,n_1 \\ j=1,\ldots,n_2}} (X - a_i b_j)$: ainsi si ab est une racine de R_2, sa multiplicité est le nombre de couples (a_i, b_j) tels que $a_i b_j = ab$.

Exemple : si $P_1(X) = P_2(X) = X^2 - 2$: $R_2(X) = (X-2)^2 (X+2)^2$ alors les quatre couples (a,b) donnent deux valeurs distinctes pour ab : 2 de polynôme minimal $X - 2$ et -2 de polynôme minimal $X + 2$.

ab ne peut prendre la valeur 0 et donc R_2 n'est jamais factorisable par X

R_2 est irréductible (cad $I = 1 = k_1$) $\Leftrightarrow$ il existe un ab de degré $n_1 n_2$ $\Leftrightarrow$ il y a $n_1 n_2$ valeurs possibles pour ab ayant toutes R_2 (au signe près) comme polynôme minimal, donc toutes de degré $n_1 n_2$.

Remarque : il peut arriver que l'un des P_i divise R_2 : c'est le cas de l'exemple 4 du 5) où $R_2 = P_2^2$.

4.2)

4.2.0) Si $n_1 \neq n_2$, alors ab, $\frac{a}{b}$, $\lambda a + \mu b$ (λ, μ dans $\mathbb{Q}^*$) ne sont pas dans $\mathbb{Q}$, donc sont algébriques sur $\mathbb{Q}$ de degré ≥ 2.

4.2.1) $[Q(a,b) : Q] \leq n_1 n_2$

4.2.2) Si n_1 et n_2 sont premiers entre eux alors

$[Q(a,b) : Q] = n_1 n_2$, donc (voir 2.3)) le degré de tout élément de $Q(a,b)$ (par exemple $a + b$ ou ab) est un diviseur de $n_1 n_2$, donc $\leq n_1 n_2$.

En fait, voir le 4.2.3) , on a $d°(a+b) = n_1 n_2$, mais ce n'est pas obligé pour ab.

$[Q(a,b) : Q(b)] = n_1, [Q(a,b) : Q(a)] = n_2$, cad le degré de a sur $Q(b)$ reste le degré de a sur Q, à savoir n_1, résultat analogue pour b.

Remarque : on peut avoir $[Q(a,b) : Q] = n_1 n_2$ sans que n_1 et n_2 soient premiers entre eux.

C'est le cas des exemples 4 et 5 du 6) : $P_1(X) = X^2 - 2$ et $P_2(X) = X^2 - 3$ et $P_1(X) = X^2 - 2$ et $P_2(X) = X^2 + X + 1$.

4.2.3) Théorème d'Isaacs (1970) : **si** n_1 **et** n_2 **sont premiers entre eux** alors, pour tout $a+b$ on a $d°(a+b) = n_1 n_2$; on a même plus : pour tout rationnel r non nul, $d°(a+rb) = n_1 n_2$, c'est-à-dire $a+rb$ est un élément primitif de l'extension $Q \subset Q(a,b)$.

Précisons : $a+b$ prend $n_1 n_2$ valeurs distinctes qui ont toutes le même polynôme minimal $\pm R_1(X)$, qui est de degré $n_1 n_2$. Le résultant R_1 est donc irréductible.

4.2.4) Contrairement au cas $a+b$, si n_1 et n_2 sont premiers entre eux,ab n'est pas obligatoirement de degré $n_1 n_2$.
On a cependant le résultat suivant :
si n_1 **et** n_2 **sont deux nombres premiers distincts** (cas particulier de deux nombres premiers entre eux) alors,

soit tout ab est de degré $n_1 n_2$ et a pour polynôme minimal $(-1)^{n_1 n_2} R_2$
soit tout ab est de degré n_1
soit tout ab est de degré n_2

Et, tout ab a pour polynôme minimal P_1 (resp P_2) $\Leftrightarrow$ il existe ab qui est racine de P_1 (resp P_2).

On pourra le vérifier sur les exemples 2,3,4 du 5) : en particulier à l'exemple 4, le polynôme minimal de tout ab est P_2.

Remarque : on verra au 4.3.2) des hypothèses supplémentaires sur $n_1 \geq 2$ et $n_2 \geq 2$ premiers entre eux assurant que tout ab a pour degré $n_1 n_2$.

4.3)

4.3.0) Un lemme :

Soient P et T deux polynômes $\mathbb{Q}[X]$:
si P est irréductible, $d°T \geq d°P \geq 2$ et si le reste de la division euclidienne de T par P n'est pas une constante,
alors, pour toute racine r de P, $T(r) \notin \mathbb{Q}$.

Remarque :

si $d°P = 1$, P a une seule racine r qui est dans $\mathbb{Q}$, donc $T(r) \in \mathbb{Q}$
si $T = UP + c$, avec c constante rationnelle, pour toute racine r de P, $T(r) = c \in \mathbb{Q}$

Application immédiate :

pour tout polynôme P de $\mathbb{Q}[X]$ irréductible avec $d°P \geq 2$, pour tout entier $m \geq d°P$ et tel que le reste de la division de X^m par P ne soit pas une constante
on a $r^m \notin \mathbb{Q}$ pour toute racine r de P.

4.3.1) Sur ab.

On a vu au 4.2.4) que si si n_2 et n_2 sont deux nombres premiers distincts, tout ab n'est pas forcément de degré $n_1 n_2$: on va voir ici deux jeux d'hypothèses supplémentaires permettant d'assurer que tout ab est de degré $n_1 n_2$ (donc ils ont $\pm R_2$ comme polynôme minimal).

4.3.1.1) si n_2 et n_2 sont deux nombres premiers distincts avec $2 \leq n_1 < n_2$ et si l'on a une des trois hypothèses suivantes

il existe une racine $\hat{a}$ de P_1 telle que $\hat{a}^{n_2} \notin Q$

ou

$n_2 < 2n_1$ et $P_2(X) \neq X^{n_2} + \beta_0$

ou

$n_2 \geq 2n_1$ et $P_2(X) \neq X^{n_2} + \beta_{n_2-n_1}X^{n_2-n_1} + \ldots + \beta_{n_1}X^{n_1} + \beta_0$

alors ab prend n_1n_2 valeurs distinctes, tout ab est de degré n_1n_2 et ils ont tous le même polynôme minimal $\pm R_2(X)$ qui est de degré n_1n_2. Ce résultant est donc irréductible.

4.3.1.2) si n_1 est premier, si $n_2 > n_1$ est premier avec n_1 (cad n_1 ne divise pas n_2), si $P_2 = X^{n_2} + \beta_0$, s'il existe une racine $\hat{a}$ de P_1 telle que $\hat{a}^{n_2} \notin Q$, si le plus grand diviseur (propre) de n_2 est $< \frac{2n_2}{n_1}$ alors ab prend n_1n_2 valeurs distinctes, tout ab est de degré n_1n_2 et ils ont tous le même polynôme minimal $\pm R_2(X)$ qui est de degré n_1n_2. Ce résultant est donc irréductible.

preuves :

preuve 4.0)

Voir R4 de l'annexe 2.

preuve 4.1.1) (c'est le cas $a+b$)

On a vu au 3.1, que tout $a+b$ est racine de R_1.

Montrons la réciproque.

$R_1(\theta) = 0 \Leftrightarrow P_1(Y)$ et $P_2(\theta - Y)$ ont une racine commune

$R_1(\theta) = 0 \Leftrightarrow$ il existe a dans C tel que $P_1(a) = 0$ et $P_2(\theta - a) = 0$,

donc $R_1(\theta) = 0 \Leftrightarrow$ il existe a racine de P_1 et b racine de P_2 tels que $\theta = a + b$.

D'où, si P est le polynôme minimal de $a+b$, comme P divise R_1 (puisque $R_1(a+b) = 0$), toute racine de P est racine de R_1 et donc tout conjugué de $a+b$ est de la forme $a' + b'$ avec a' racine de P_1 et b' racine de P_2.

Rappelons, cf le 2.1), que tout U_i a $d°U_i$ racines distinctes et si $i \neq j$, U_i et U_j n'ont aucune racine commune.

Comme tout $a+b$ est racine de R_1, tout $a+b$ est racine d'un U_i et réciproquement, puisque toute racine de R_1 est un $a+b$.

Montrons que $R_1(X) = (-1)^{n_1n_2} \prod_{\substack{i=1,\ldots,n_1 \\ j=1,\ldots,n_2}} (X - (a_i + b_j))$.

On utilise R0 de l'annexe 2.

En effet, $R_1(X) = res_Y(P_1(Y), P_2(X-Y))$: les racines de $P_1(Y)$ sont les a_i, celles de $P_2(X-Y)$ sont les $X - b_j$ et P_1 est unitaire, P_2 a pour coefficient de tête $(-1)^{n_1}$, donc

$R_1(X) = 1^{n_2}((-1)^{n_2})^{n_1} \prod_{\substack{i=1,\ldots,n_1 \\ j=1,\ldots,n_2}} ((X - b_j) - a_i)$.

Montrons que "certains" $a+b$ prennent la valeur $0 \Leftrightarrow P_1(X) = P_2(-X) \Leftrightarrow X$ est un facteur (irréductible) de R_1 :

si $a+b$ prend la valeur 0, alors X, polynôme minimal de 0, est un facteur de R_1, donc $R_1(0) = 0$ et $P_1(Y)$ et $P_2(-Y)$ ont une racine commune r qui a alors $P_1(X)$ et $P_2(-X)$ comme polynômes minimaux ($P_2(-X)$ est irréductible, $P_2(X)$ l'étant). Donc $P_1(X) = P_2(-X)$.

Réciproquement si $P_1(X) = P_2(-X)$, pour tout a racine de P_1, $b = -a$ est racine de P_2 et $a+b$ prend la valeur 0, laquelle a pour polynôme minimal X.

Montrons que

R_1 est irréductible $\Leftrightarrow$ il existe un $a+b$ de degré $n_1n_2 \Leftrightarrow$ il y a n_1n_2 valeurs possibles pour

$a+b$ ayant toutes $\pm R_1$ comme polynôme minimal.
Les trois affirmations sont notées respectivement $1, 2, 3$:
si R_1 est irréductible, le polynôme minimal de tout $a+b$ est $\pm R_1$ (puisque tout $a+b$ est racine de R_1) donc tout $a+b$ est de degré $n_1 n_2$; mais toute racine de R_1 est un $a+b$, or R_1 a $n_1 n_2$ racines distinctes, donc il y a $n_1 n_2$ valeurs possibles pour $a+b$:
on a donc montré que $1 \Rightarrow 2$ et 3.
Maintenant, s'il existe $a+b$ de degré $n_1 n_2$, son polynôme minimal est de degré $n_1 n_2$ et est unitaire, et comme il divise R_1, $\pm R_1$ est ce polynôme minimal, donc R_1 est irréductible : donc $2 \Rightarrow 1$ d'où $1 \Leftrightarrow 2$ et comme $2 \Rightarrow 1 \Rightarrow 3$ et que $3 \Rightarrow 2$ de façon triviale, on a $2 \Leftrightarrow 3$. □

preuve 4.1.2) (c'est le cas ab)
Toutes les preuves sont identiques au cas $a+b$, sauf la preuve de $R_2(\theta) = 0 \Leftrightarrow$ il existe a racine de P_1 et b racine de P_2 tels que $\theta = ab$.
Précisons cette preuve :
$R_2(\theta) = 0 \Leftrightarrow P_1(Y)$ et $Y^{n_2} P_2(\frac{\theta}{Y})$ ont une racine commune
$R_1(\theta) = 0 \Leftrightarrow$ il existe a dans C tel que $P_1(a) = 0$ et $a^{n_2} P_2(\frac{\theta}{a}) = 0$ (licite car $n_1 \geq 2$ et donc $a \neq 0$)
$R_1(\theta) = 0 \Leftrightarrow$ il existe a racine de P_1 et b racine de P_2 tels que $b = \frac{\theta}{a}$.

Montrons que $R_2(X) = (-1)^{n_1 n_2} \prod_{\substack{i=1,\dots,n_1 \\ j=1,\dots,n_2}} (X - a_i b_j)$.

On utilise R0 de l'annexe 2.
En effet, $R_2(X) = res_Y(P_1(Y), Y^{n_2} P_2(\frac{X}{Y}))$: les racines de $P_1(Y)$ sont les a_i, celles de $Y^{n_2} P_2(\frac{X}{Y})$ sont les $\frac{X}{b_j}$ et P_1 est unitaire, $Y^{n_2} P_2(\frac{X}{Y})$ a pour coefficient de tête β_0, donc

$$R_2(X) = 1^{n_2} (\beta_0)^{n_1} \prod_{\substack{i=1,\dots,n_1 \\ j=1,\dots,n_2}} (\frac{X}{b_j} - a_i) = (\beta_0)^{n_1} \prod_i \frac{1}{\prod_j b_j} \prod_j (X - a_i b_j),$$

soit $R_2(X) = {\beta_0}^{n_1} (\frac{1}{(-1)^{n_2} \beta_0})^{n_1} \prod_{\substack{i \\ j}} (X - a_i b_j)$.

Quant à la preuve du fait ab que ne peut prendre la valeur 0 et donc R_2 n'est jamais factorisable par X, c'est évident car ici P_1 et P_2 sont de degrés ≥ 2
et étant irréductibles ils ne peuvent avoir 0 comme racine, donc a et b sont toujours non nuls. □

preuve 4.2.0)
Si $ab \in \mathbb{Q}$, comme $a \neq 0$ car de degré ≥ 2, $b = \frac{q}{a} \in Q(a)$; or $[\mathbb{Q}(a) : \mathbb{Q}] = n_1$, donc n_2 divise n_1; de même n_1 divise n_2, soit $n_1 = n_2$, donc contradiction.
Si $\frac{a}{b} \in \mathbb{Q}$, $a \in \mathbb{Q}(b)$, donc n_1 divise n_2, de même n_2 divise n_1 car $\frac{b}{a}$ est aussi dans $\mathbb{Q}$, ….
Si $\lambda a + \mu b \in \mathbb{Q}$, b est dans $Q(a)$ et a dans $Q(b)$, ... □

preuve 4.2.1)

On a vu au 2.2)
$[Q(a,b) : Q] = [Q(a)(b) : Q(a)][Q(a) : Q] = [Q(b)(a) : Q(b)][Q(b) : Q]$
Soit $[Q(a,b) : Q] = [Q(a)(b) : Q(a)]n_1 = [Q(b)(a) : Q(b)]n_2$.
Mais P_1 qui est dans $Q[X]$ est aussi dans $Q(b)[X]$, donc est un polynôme annulateur de a sur $Q(b)$ et ainsi $[Q(b)(a) : Q(b)] \leq n_1$ et $[Q(a,b) : Q] \leq n_1 n_2$. □

preuve 4.2.2)

Maintenant, si n_1 et n_2 sont premiers entre eux, comme ils divisent $[Q(a,b) : Q]$, c'est que $n_1 n_2$ divise $[Q(a,b) : Q]$, et vu l'inégalité précédente, $[Q(a,b) : Q] = n_1 n_2$.
Les deux autres égalités $[Q(a)(b) : Q(a)] = n_2$ et $[Q(b)(a) : Q(b)] = n_1$ s'en déduisent immédiatement.
Voir fin du 2.4 pour le fait que les degrés de $a+b$ et ab divisent $n_1 n_2$. □

preuve 4.2.3) Pour ce qui est du théorème d'Isaac lui-même, je laisse le lecteur faire une recherche sur le web.
Tout $a+b$ étant algébrique de degré $n_1 n_2$ sur Q (Isaac), son polynôme minimal M est de degré $n_1 n_2$; mais, voir 2.5), $a+b$ est racine de $R_1(X) = res_Y(P_1(Y), P_2(X-Y))$ avec $d°R_1 = n_1 n_2$ et de coefficient de tête ± 1 : donc R_1 est un multiple de M, et ces deux polynômes ayant le même degré, $M = \pm R_1$.
Et comme on a vu dans la preuve du 3.1) que toute racine de R_1 est un $a+b$, c'est que $a+b$ prend $n_1 n_2$ valeurs distinctes (un polynôme irréductible sur Q a ses racines distinctes). □

preuve 4.2.4)

D'après le 4.2.2), $[\mathbb{Q}(a,b);\mathbb{Q}] = n_1 n_2$: comme $ab \in \mathbb{Q}(a,b)$, le degré de ab divise $n_1 n_2$ (voir 2.3)), donc tout ab est de dégré 1 ou n_1 ou n_2 ou $n_1 n_2$.
Mais ab ne peut être de degré 1 (voir 4.2.0)), donc tout ab est de degré n_1 ou n_2 ou $n_1 n_2$.
soit R_2 est irréductible et, ab prend $n_1 n_2$ valeurs qui ont toutes pour polynôme minimal $\pm R_2$ (voir 4.1.2))
soit R_2 est réductible et $R_2 = \prod_i V_i^{k_1}$, chaque V_i (de degré ≥ 2 et $< n_1 n_2$) étant polynôme minimal de certains ab (voir 4.1.2)) : donc tout V_i est de degré n_1 ou n_2.
En notant m_1 le nombre de V_i de degré n_1 et m_2 le nombre de V_i de degré n_2 on obtient $m_1 n_1 + m_2 n_2 = n_1 n_2$ et ainsi n_1 divise m_2 et n_2 divise m_1 ; donc si m_1 et m_2 sont non nuls, $m_1 \geq n_2$, $m_2 \geq n_1$ et $m_1 n_1 + m_2 n_2 = n_1 n_2 \geq 2 n_1 n_2$, ce qui est impossible.
Donc soit $m_1 = 0$ et tout ab est de degré n_2, soit $m_2 = 0$ et tout ab est de degré n_1.

Enfin, si un ab est racine de P_i ($i = 1$ ou 2), c'est que cet ab a pour polynôme minimal P_i, donc est de degré n_i, et cf ci-dessus, tout ab a pour degré n_i. □

preuve 4.3.0) Le lemme.

La division euclidienne de T par P donne $T = UP + R$ avec U et R dans $\mathbb{Q}[X]$ et $d°R < d°P$ (puisque par hypothèse R n'est pas une constante, R n'est pas le polynôme nul).
S'il existe une racine r de P telle que $T(r) \in \mathbb{Q}$, alors $T(r) = R(r) \in \mathbb{Q}$.
Donc r est racine du polynôme G tel que $G(X) = R(X) - R(r) \in \mathbb{Q}[X]$.
Mais G ne peut être le polynôme nul, car cela voudrait dire que R serait une constante ce qui est exclu par l"hypothèse : donc G est un polynôme non nul de degré celui de R et ainsi $d°G < d°P$, ce qui est en contradiction avec le fait que P (quitte à le diviser par son coefficient de tête) est le polynôme minimal de r.
Donc il n'existe pas de racine r de P telle que $T(r) \in \mathbb{Q}$. □

preuve 4.3.1.1)

Notons que a (racine quelconque de P_1) et b (racine quelconque de P_2) ne sont pas nuls car ils sont de degré ≥ 2.

Commençons par montrer que tout ab est de degré $n_1 n_2$.

n_1 et n_2 sont donc premiers entre eux et cf le 4.2.2), le degré d de ab divise $n_1 n_2$, donc (n_1 et n_2 étant des nombres premiers distincts) $d = 1$ ou n_1 ou n_2 ou $n_1 n_2$.

$\underline{d = 1}$ est impossible d'après le 4.2.0)

$\underline{\text{si } d = n_1}$, alors ab a pour polynôme minimal un polynôme à coefficients dans Q de degré n_1 :

$(ab)^{n_1} + c_{n_1-1}(ab)^{n_1-1} + \ldots + c_1(ab) + c_0 = 0$.

Puisque $a^{n_1} \neq 0$, b est racine d'un polynôme à coefficients dans $Q(a)$ qui est non nul et ainsi le degré de b sur $Q(a)$ est $\leq n_1$, or c'est $n_2 > n_1$ cf le 4.2.2).

$\underline{\text{si } d = n_2}$, alors ab a pour polynôme minimal un polynôme à coefficients c_i dans Q de degré n_2 :

$(ab)^{n_2} + c_{n_2-1}(ab)^{n_2-1} + \ldots + c_1(ab) + c_0 = 0$.

Mais $P_2(b) = 0$, soit $b^{n_2} = -\beta_{n_2-1} b^{n_1-1} - \ldots - \beta_1 b - \beta_0$ (les β_i sont dans Q) et ainsi $G(b) = \sum_0^{n_2-1} (-a^{n_2}\beta_i + c_i a^i) b^i = 0$, cad b est racine d'un polynôme G à coefficients dans $Q(a)$, de degré $\leq n_2 - 1$.

Pour conclure, il faut justifier que G n'est pas le polynôme nul.

$\underline{\text{Soit on a l'hypothèse}}$: il existe une racine $\hat{a}$ de P_1 telle que $\hat{a}^{n_2} \notin Q$ et prenons $a = \hat{a}$.

Le polynôme G a pour terme constant $-\hat{a}^{n_2}\beta_0 + c_0$, avec β_0 non nul, car P_2 est irréductible et de degré ≥ 2 : ce terme constant ne peut être nul car sinon $\hat{a}^{n_2} = \frac{c_0}{\beta_0} \in Q$, ce qui est contraire à l'hypothèse faite sur $\hat{a}^{n_2}$ et donc $\underline{G \text{ n'est pas le polynôme nul}}$.

$\underline{\text{Soit on a l'hypothèse}}$: $n_2 < 2n_1$ et $P_2(X) \neq X^{n_2} + \beta_0$ OU $n_2 \geq 2n_1$ et $P_2(X) \neq X^{n_2} + \beta_{n_2-n_1} X^{n_2-n_1} + \ldots + \beta_{n_1} X^{n_1} + \beta_0$.

On va montrer que cela implique aussi que le polynôme G n'est pas le polynôme nul.

Supposons que G soit le polynôme nul.

Alors pour tout $i = 0, 1, \ldots, n_2 - 1$ on a $-a^{n_2}\beta_i + c_i a^i = 0$.

Donc $-a^{n_2}\beta_0 + c_0 = 0$, et comme $\beta_0 \neq 0$, $a^{n_2} \in Q$ et ainsi pour tout $i = 0, 1, \ldots, n_2 - 1$ on a $c_i a^i \in Q$: donc a étant algébrique sur Q de degré $n_1 < n_2$, $c_1 = c_2 = \ldots = c_{n_1-1} = 0$, ce qui implique $\beta_1 = \beta_2 = \ldots = \beta_{n_1-1} = 0$ d'où nécessairement $P_2(X) = X^{n_2} + \beta_{n_2-1} X^{n_2-1} + \ldots + \beta_{n_1} X^{n_1} + \beta_0$.

Mais pour tout $i = 0, 1, \ldots, n_2 - 1$ on a aussi $a^{n_2-i}\beta_i = c_i \in Q$ et pour la même raison que ci-dessus, pour $1 \leq n_2 - i \leq n_1 - 1$, soit $n_2 - n_1 + 1 \leq i \leq n_2 - 1$ (on a bien $1 \leq n_1 - 1$) on a $\beta_i = 0$ et $P_2(X) = X^{n_2} + \beta_{n_2-n_1} X^{n_2-n_1} + \ldots + \beta_1 X + \beta_0$.

En combinant ces deux relations sur P_2, on obtient que si G est le polynôme nul, alors

si $n_2 < 2n_1$, soit $n_2 - n_1 < n_1$, on a $P_2(X) = X^{n_2} + \beta_0$

si $n_2 > 2n_1$, soit $n_2 - n_1 > n_1$, on a $P_2(X) = P_2(X) = X^{n_2} + \beta_{n_2-n_1} X^{n_2-n_1} + \ldots + \beta_{n_1} X^{n_1} + \beta_0$

ce qui est en contradiction avec l'hypothèse faite, donc cette hypothèse implique que $\underline{G \text{ n'est pas le polynôme nul}}$.

Note : on ne peut avoir $n_2 = 2n_1$ puisque n_2 est premier ≥ 3.

Donc, lorsque $d = n_2$, G n'est pas le polynôme nul, donc le degré de b sur $Q(a)$ (ou $Q(\hat{a})$) est $\leq n_2 - 1$, alors que ce degré est en fait n_2 (voir 4.2.2)), donc $d \neq n_2$ et la seule possibilité est $d°ab = n_1 n_2$, et ainsi tout ab est de degré $n_1 n_2$, ab prend $n_1 n_2$ valeurs qui

ont toutes le même polynôme minimal $\pm R_2$ d'après le 4.1.2).
Note : le 4.2.2) est vrai pour toute racine a de P_1 et toute racine de P_2. □

preuve 4.3.1.2)

n_1 et n_2 étant premiers entre eux, d'après 4.2.2 le degré d de ab divise $n_1 n_2$, donc soit d divise n_2, soit $d = n_1 d'$ avec d' divise n_2 (car $n_1 n_2 = kd$ et n_1 étant premier, soit n_1 divise k, soit n_1 divise d).
Commençons par montrer que $\hat{a}b$ est de degré $n_1 n_2$.
On notera $P(X) = X^d + c_{d-1}X^{d-1} + \ldots + c_1 X + c_0$ le polynôme minimal de $\hat{a}b$ et on va montrer que la seule possibilité est $d = n_1 n_2$.

si d divise n_2 □

soit $d < n_2$: comme $P(\hat{a}b) = 0$ et que $\hat{a}^d \neq 0$, b est racine d'un polynôme à coefficients dans $Q(\hat{a})$ non nul et de degré $d < n_2$, ce qui est contraire au fait que le degré de b sur $Q(\hat{a})$ est n_2 d'après le 4.2.2)

soit $d = n_2$: $(\hat{a}b)^{n_2} = -\hat{a}^{n_2}\beta_0$ et b est racine d'un polynôme $P_{\hat{a}}$ à coefficients dans $Q(\hat{a})$ de degré $\leq n_2 - 1$ et de terme constant $-\hat{a}^{n_2}\beta_0 + c_0$ qui est non nul car sinon, cf $c_0 \neq 0$ (car P est irréductible de degré $d = n_2 \geq 2$) $\hat{a}^{n_2}$ serait dans Q ce qui est exclu ; donc $P_{\hat{a}}$ n'est pas le polynôme nul et comme ci-dessus on arrive à une contradiction

si $d = n_1 d'$ avec d' divise n_2 avec $d' < n_2$

Pour tout $i \in \{0;1;\ldots;d\}$, $i = q_i n_2 + r_i$ avec r_i dans $\{0;1;\ldots;n_2 - 1\}$ et ainsi $(\hat{a}b)^i = \hat{a}^i(-\beta_0)^{q_i} b^{r_i}$: cette puissance sera une constante par rapport à b si et seulement si $r_i = 0$.
Or $i \leq d = n_1 d' < n_1 \frac{2n_2}{n_1} = 2n_2$, donc $i = q_i n_2$ si et seulement si $i = 0$ ou n_2.
Donc b est racine d'un polynôme $P_{\hat{a}}$ à coefficients dans $Q(\hat{a})$ de degré $\leq n_2 - 1$ et de terme constant $-c_{n_2}\hat{a}^{n_2}\beta_0 + c_0$ qui est non nul car sinon, comme ci-dessus $\hat{a}^{n_2}$ serait dans Q, donc P_a n'est pas le polynôme nul et encore contradiction (le degré de b sur $Q(\hat{a})$ est n_2, d'après le 4.2.2)).
La seule possibilité est donc $d = n_1 n_2$, cad le degré de $\hat{a}b$ est $n_1 n_2$ et d'après le 4.1.2, ab prend $n_1 n_2$ valeurs distinctes, qui ont toutes le même polynôme minimal $\pm R_2(X)$. □

5) **Quatre exemples avec** $n_1 = d°P_1$ et $n_2 = d°P_2$ premiers entre eux : illustration du 4.3

Les polynômes minimaux P_1 et P_2 (unitaires par définition) choisis ici, ainsi que ceux des exemples du paragraphe suivant, sont à coefficients dans Z, cad a et b sont des entiers algébriques.
On sait que l'ensemble des entiers algébriques forment un anneau : cet aspect se vérifie sur tous les exemples proposés par le fait que les polynômes minimaux obtenus pour $a + b$ et ab (qui sont unitaires par définition) sont eux aussi à coefficients dans Z.

Note : On verra au 7) quelques généralités sur le cas $P_1(X) = X^{n_1} + \alpha_0$ et $P_2(X) = X^{n_2} + \beta_0$.

Exemple 1 : $P_1(X) = X^3 - 2$, $P_2(X) = X^4 + 1$.

P_1 est irréductible car il est de degré 3 et il n'a pas de racine rationnelle et pour $X^4 + 1$ voir l'exemple 6 du 6) où ce polynôme apparaît aussi.

Cas $a + b$

n_1 et n_2 étant premiers entre eux le 4.3.1) s'applique : $a+b$ prend 12 valeurs qui ont toutes comme polynôme minimal $\pm R_1$ avec $R_1 = res_Y(P_1(Y), P_2(X-Y))$.
R_1 est le déterminant de la matrice ci-dessous :

$$\begin{pmatrix} -2 & 0 & 0 & 0 & X^4+1 & 0 & 0 \\ 0 & -2 & 0 & 0 & -4X^3 & X^4+1 & 0 \\ 0 & 0 & -2 & 0 & 6X^2 & -4X^3 & X^4+1 \\ 1 & 0 & 0 & -2 & -4X & 6X^2 & -4X^3 \\ 0 & 1 & 0 & 0 & 1 & -4X & 6X^2 \\ 0 & 0 & 1 & 0 & 0 & 1 & -4X \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix},$$

Ce déterminant est
$X^{12} - 8X^9 + 3X^8 + 24X^6 + 96X^5 + 3X^4 - 32X^3 + 120X^2 - 24X + 17 = R_1(X)$ qui est donc le polynôme minimal des 12 valeurs prises par $a+b$.

Cas ab

L'hypothèse du 4.3.1.2) est vérifiée car

$n_1 = 3$ est un nombre premier

$n_2 = 4$ est premier avec n_1

$P_2(X)$ est de la forme $X^{n_2} + \beta_0$

il existe $\hat{a}$ tel que $\hat{a}^4 \notin Q$ (d'après le lemme 4.3.0) puisque $X^4 = XP_1 + 2X$; ou directement : pour tout a car si $a^4 \in Q$, comme $a^4 = 2a$ c'est que a est dans Q, ce qui est faux) .

le plus grand diviseur propre de $n_2 = 4$ est $2 < \frac{2n_2}{n_1} = \frac{8}{3}$

et donc ab prend 12 valeurs ayant toutes pour polynôme minimal $\pm R_2$.
$R_2 = res_Y(P_1(Y), Y^4 P_2(\frac{X}{Y}))$ est le déterminant de la matrice

$$\begin{pmatrix} -2 & 0 & 0 & 0 & X^4 & 0 & 0 \\ 0 & -2 & 0 & 0 & 0 & X^4 & 0 \\ 0 & 0 & -2 & 0 & 0 & 0 & X^4 \\ 1 & 0 & 0 & -2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Ce déterminant est $X^{12} + 16 = R_2(X)$ qui est donc le polynôme minimal des douze valeurs prises par ab.

Remarque 1 : on pouvait ici trouver ce résultat sans passer par la notion de résultant.
En effet pour tout ab, $(ab)^{12} = 2^4 \times (-1)^3 = -16$ et $X^{12} + 16$ est annulateur des douze ab.
Et d'après le 5) de l'annexe 1, $R_2(X) = X^{12} + 16$ est irréductible car le module de ses racines est $\leq \sqrt[12]{16} < 1.26 < k - \frac{1}{2}$ pour $k \geq 2$, et comme $R_2(2) \neq 0$ et $R_2(3) = 531457$ est un nombre premier, R_2 est bien irréductible.
Donc $X^{12} + 16$ est le polynôme minimal de tout ab.
Remarque 2 : montrons que pour tout ab, $d°ab = 12$ sans utiliser le 4.3.1.2) et sans en refaire la preuve dans ce cas particulier.

Cf le 4.2.2), le degré de ab est un diviseur de $n_1 n_2$ soit 1 ou 2 ou 3 ou 4 ou 6 ou 12, ce qui fait cinq cas à examiner :

si $d°ab = 1$, alors $ab = q \in Q^*$ et $2b^3 - q^3 = 0$ ce qui est en contradiction avec $d°b = 4$

si $d°ab = 2$, alors $(ab)^2 + c_1 ab + c_0 = 0$, avec $c_i \in Q$ (cf ab a pour polynôme minimal un second degré) et comme $a \neq 0$, le degré de b sur $Q(a)$ est ≤ 2, alors que c'est 4 (voir 3.2) : encore contradiction

si $d°ab = 3$, alors $(ab)^3 + c_2(ab)^2 + c_1 ab + c_0 = 0$, mais $(ab)^3 = 2b^3$ et le degré de b sur $Q(a)$ est ≤ 3, alors que c'est 4 (voir 4.2.2) : encore contradiction

si $d°ab = 4$, alors $(ab)^4 + c_3(ab)^3 + c_2(ab)^2 + c_1 ab + c_0 = 0$, mais $(ab)^4 = -a^4$, ce qui fait un terme constant $-a^4 + c_0 \neq 0$ (sinon $a^4 = 2a \in Q$, ce qui est faux), donc b est racine d'un polynôme non nul à coefficients dans $Q(a)$ et de degré ≤ 3, donc le degré de b sur $Q(a)$ est ≤ 3, alors que c'est 4 (voir 4.2.2) : encore contradiction

si $d°ab = 6$, alors $(ab)^6 + c_5(ab)^5 + c_4(ab)^4 + c_3(ab)^3 + c_2(ab)^2 + c_1 ab + c_0 = 0$, soit $-4b^2 - 2c_5 a^2 b - 2c_4 a + 2c_3 b^3 + c_2(ab)^2 + c_1 ab + c_0 = 0$: le coefficient de b^2 est $c_2 a^2 - 4 \neq 0$ (sinon $c_2 a^2 = 4$, donc $c_2 \neq 0$ et $a^2 = \frac{2}{a} \in Q$, soit $a \in Q$, ce qui est faux), donc b est racine d'un polynôme non nul à coefficients dans $Q(a)$ et de degré ≤ 3, donc le degré de b sur $Q(a)$ est ≤ 3, alors que c'est 4 (voir 4.2.2) : encore contradiction. On peut aussi invoquer le terme constant $-2c_4 a + c_0$: il est non nul, car sinon $2c_4 a = c_0$, or $c_0 \neq 0$ (terme constant d'un polynôme minimal de degré ≥ 2), donc c_4 aussi et a serait dans Q ce qui est faux et on obtient aussi que b est racine d'un polynôme non nul à coefficients dans $Q(a)$ et de degré ≤ 3.

La seule possibilité est donc $d°ab = 12$.

Exemple 2 : $P_1(X) = X^2 - 2$, $P_2(X) = X^3 - 7$.

Ces deux polynômes sont évidemment irréductibles car ils sont de degré ≤ 3 et sans racine rationnelle.

Cas $a + b$

n_1 et n_2 étant premiers entre eux le 4.3.1 s'applique : $a + b$ prend 6 valeurs qui ont toutes comme polynôme minimal $\pm R_1$ avec $R_1 = res_Y(P_1(Y), P_2(X - Y))$.

Les six valeurs possibles pour $a + b$ sont $\pm\sqrt{2} + j^k \sqrt[3]{7}$, avec $k = 0, 1, 2$.

R_1 est le déterminant de la matrice ci-dessous :

$$\begin{pmatrix} -2 & 0 & 0 & X^3 - 7 & 0 \\ 0 & -2 & 0 & -3X^2 & X^3 - 7 \\ 1 & 0 & -2 & +3X & -3X^2 \\ 0 & 1 & 0 & -1 & 3X \\ 0 & 0 & 1 & 0 & -1 \end{pmatrix}$$

soit $X^6 - 6X^4 - 14X^3 + 12X^2 - 84X + 41 = R_1(X)$ qui est donc le polynôme minimal des 6 valeurs de $a + b$.

Remarque 1 : le 5) de l'annexe 1 permet de vérifier que ce polynôme R_1 est effectivement irréductible.

En effet ses racines sont $\pm\sqrt{2} + j^k \sqrt[3]{7}$, donc leur module est majoré par $\sqrt{2} + \sqrt[3]{7} \simeq 3.32 < k - \frac{1}{2}$ pour $k \geq 4$ et comme $R_1(11) \neq 0$ et $R_1(12) = 2838137$ est premier, R_1 est irréductible.

Remarque 2 : une variante pour obtenir ce polynôme minimal sans déterminant :

le polynôme minimal de $\sqrt{2} + \sqrt[3]{7}$ a pour racines tous ses conjugués (par définition)

lesquels (voir le 4.1.1)) sont obligatoirement de la forme $\pm\sqrt{2}+j^k\sqrt[3]{7}$, d'où l'idée de considérer le polynôme
$(X-\sqrt{2}-\sqrt[3]{7})(X-\sqrt{2}-j\sqrt[3]{7})(X-\sqrt{2}-j^2\sqrt[3]{7})(X+\sqrt{2}-\sqrt[3]{7})(X+\sqrt{2}-j\sqrt[3]{7})(X+\sqrt{2}-j^2\sqrt[3]{7})$.
L'identité $(a-b)(a-jb)(a-j^2b)=a^3-b^3$ permet de voir que ce polynôme est
$((X-\sqrt{2})^3-7)((X+\sqrt{2})^3-7)=(X^2-2)^3-7((X+\sqrt{2})^3+(X-\sqrt{2})^3+49$, soit
$X^6-6X^4-14X^3+12X^2-84X+41$.
Donc $X^6-6X^4-14X^3+12X^2-84X+41$ est annulateur de $\sqrt{2}+\sqrt[3]{7}$ et comme il est irréductible (remarque 1 ci-dessus) c'est le polynôme minimal

Cas ab

On est dans le cadre du 4.2.4) puisque n_1 et n_2 sont deux nombres premiers distincts, donc tout ab a le même polynôme minimal qui est soit $\pm R2$, soit un polynôme de degré n_1, soit un polynôme de degré n_2 : on va montrer que c'est $\pm R_2$.
Pour tout a racine de P_1, $a^{n_2}=a^3\notin Q$ (d'après le lemme 4.3.0) puisque $X^3=XP_1+2X$ ou directement car $a^3=q\in Q$ implique $2a=q$ donc a dans Q, ce qui est exclu).
On peut alors appliquer le 4.3.1.1) : ab prend 6 valeurs qui ont toutes comme polynôme minimal $(-1)^{n_1n_2}R_2$ avec $R_2=res_Y(P_1(Y),Y^{n_2}P_2(\frac{X}{Y}))$, de degré 6 et de coefficient de tête $(-1)^{n_1n_2}=1$, et qui est donc irréductible.
Je laisse le lecteur calculer ce résultant ... car il est facile de voir que
$(ab)^6=2^3\times 7^2=392$, donc X^6-392 est annulateur de tout ab, et comme tout ab est de degré 6 sur Q, X^6-392 est forcément le polynôme minimal de tout ab et c'est R_2.
Remarque 1 : montrons directement (cad sans appliquer le 4.3.1.1), ...mais en le redémontrant sur cet exemple) que $d°ab=6$
Cf le 4.2.2, le degré de ab est un diviseur de n_1n_2 soit 1 ou 2 ou 3 ou 6, car il divise 2×3.

si $d°ab=1$, ab est dans Q et b^2 aussi, contraire à $d°b=3$ (ou on applique 4.2.0))

si $d°ab=2$, ab est racine d'un second degré, $(ab)^2+c_1ab+c_0=0$ avec u,v dans Q, $2b^2+c_1ab+c_0=0$ et le degré de b sur $Q(a)$ est ≤ 2 or il est 3, cf le 3.2, donc contradiction

si $d°ab=3$, ab est racine d'un troisième degré, $(ab)^3+c_2(ab)^2+c_1ab+c_0=0$ avec u,v,w dans Q, $14a+2c_2b^2+c_1ab+c_0=0$, donc b est racine d'un polynôme non nul (le terme constant $14a+c_0$ est non nul car $a\notin Q$), à coefficients dans $Q(a)$ et de degré ≤ 2, donc le degré de b sur $Q(a)$ est ≤ 2, alors que c'est 3 (voir 3.2) : encore contradiction
Donc $d°ab=6$.
Remarque 2 : le 5) de l'annexe 1 permet encore de prouver directement l'irréductibilité de X^6-392 :
le module des racines est $\sqrt[6]{392}\simeq 2,705<k-\frac{1}{2}$ pour $k\geq 4$ et comme $4^6-392\neq 0$ et $5^6-392=15233$ est un nombre premier X^6-392 est irréductible.

Exemple 3 : $P_1(X)=X^3+X+7$, $P_2(X)=X^5-2$.

P_1 est irréductible car il est de degré 3 sans racine rationnelle, et P_2 l'est d'après le 4) de l'annexe 1.
Les racines de $P_1(X)$, qui est de la forme X^3+pX+q, s'obtiennent par les formules de Cardan (voir mes pages sur troisième degré) :
$\alpha+\beta, j\alpha+j^2\beta, j^2\alpha+j\beta$ avec $\alpha=\sqrt[3]{-\frac{7}{2}+\frac{\sqrt{3981}}{18}}$, $\beta=-\sqrt[3]{\frac{7}{2}+\frac{\sqrt{3981}}{18}}$
$(4p^3+27q^2=4+27\times 49=1327=\frac{3981}{3})$

Contrôle : $\alpha\beta = -\frac{1}{3}$, donc $(\alpha+\beta)^3 + \alpha + \beta + 7 = \alpha^3 + \beta^3 + 7 = -\frac{7}{2} - \frac{7}{2} + 7 = 0$.

Cas $a+b$

n_1 et n_2 étant premiers entre eux le 4.3.1) s'applique : $a+b$ prend 15 valeurs qui ont toutes comme polynôme minimal $\pm R_1$ avec $R_1 = res_Y(P_1(Y), P_2(X-Y))$.

R_1 est le déterminant de la matrice

$$\begin{pmatrix} 7 & 0 & 0 & 0 & 0 & X^5-2 & 0 & 0 \\ 1 & 7 & 0 & 0 & 0 & -5X^4 & X^5-2 & 0 \\ 0 & 1 & 7 & 0 & 0 & 10X^3 & -5X^4 & X^5-2 \\ 1 & 0 & 1 & 7 & 0 & -10X^2 & 10X^3 & -5X^4 \\ 0 & 1 & 0 & 1 & 7 & 5X & -10X^2 & 10X^3 \\ 0 & 0 & 1 & 0 & 1 & -1 & 5X & -10X^2 \\ 0 & 0 & 0 & 1 & 0 & 0 & -1 & 5X \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 \end{pmatrix}$$

soit $-X^{15} - 5X^{13} - 35X^{12} - 10X^{11} - 134X^{10} - 500X^9 - 240X^8 - 2735X^7 - 3530X^6$
$-1273X^5 + 6355X^4 - 12\,695X^3 - 1320X^2 - 22\,405X - 16\,167$

Le polynôme minimal de tout $a+b$ est donc l'opposé de ce résultant.

Notons que le produit des quinze valeurs de $a+b$ est 16167.

Cas ab

On est dans le cadre du 4.2.4) puisque n_1 et n_2 sont deux nombres premiers distincts, donc tout ab a le même polynôme minimal qui est soit $(-1)^{n_1 n_2} R2 = -R_2$, soit un polynôme de degré n_1, soit un polynôme de degré n_2 : on va montrer que c'est $-R_2$.

On remarque que pour tout a, $a^{n_2} = a^5 \notin Q$ (d'après le lemme 4.3.0)) car $X^5 = (X^2-1)P_1 - 7X^2 + X + 7$ ou directement : si $a^5 = q \in Q$, comme $a^3 = -a - 7$, $a^5 = -a^3 - 7a^2 = a + 7 - 7a^2 = q$ et a serait de degré ≤ 2, alors que c'est 3.

Donc la première hypothèse du 4.3.1.1) est vérifiée et ainsi ab prend 15 valeurs qui ont toutes comme polynôme minimal $-R_2$ avec $R_2 = res_Y(P_1(Y), Y^5 P_2(\frac{X}{Y}))$.

R_2 est le déterminant de la matrice

$$\begin{pmatrix} 7 & 0 & 0 & 0 & 0 & X^5 & 0 & 0 \\ 1 & 7 & 0 & 0 & 0 & 0 & X^5 & 0 \\ 0 & 1 & 7 & 0 & 0 & 0 & 0 & X^5 \\ 1 & 0 & 1 & 7 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 7 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & -2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & -2 \end{pmatrix}$$

soit $R_2(X) = -X^{15} + 70X^{10} - 984X^5 - 134\,456$

Le polynôme minimal de tout ab est donc $-R_2$.

Remarque 1 : on peut trouver un polynôme annulateur des quinze valeurs de ab sans passer par le résultant en utilisant le 2.4), mais à vrai dire ce n'est pas mieux, car j'utilise

aussi un logiciel pour résoudre le systéme 3×3 obtenu :
$(ab)^5 = 2a^5 = 2(-7a^2 + a + 7)$, puisque $a^3 = -a - 7$ et on multiplie par a^2
$(ab)^{10} = 4(49a^4 + a^2 + 49 - 14a^3 - 98a^2 + 14a)$
$(ab)^{10} = 4(-146a^2 - 315a + 147)$
$(ab)^{15} = 8(-7a^2 + a + 7)(-146a^2 - 315a + 147)$
$(ab)^{15} = 8(-3388a^2 - 11271a - 13384)$.
Mais a étant algébrique de degré 3, $Q(a)$ est un espace vectoriel de dimension 3 sur Q, donc $\{1; a; a^2\}$ est une Q –base de $Q(a)$ et ainsi la famille 1, $(ab)^5$, $(ab)^{10}$, $(ab)^{10}$ est Q –liée, c'est-à-dire il existe quatre rationnels tels que
$\lambda_3(ab)^{15} + \lambda_2(ab)^{10} + \lambda_1(ab)^5 + \lambda_0 = 0$, ce qui donne le systéme
$-8 \times 3388\lambda_3 - 4 \times 146\lambda_2 - 2 \times 7\lambda_1 = 0$
$-8 \times 11271\lambda_3 - 4 \times 315\lambda_2 + 2\lambda_1 = 0$
$-8 \times 13384\lambda_3 + 4 \times 147\lambda_2 + 2 \times 7\lambda_1 + \lambda_0 = 0$
La matrice de ce systéme d'inconnues $\lambda_3, \lambda_2, \lambda_1$ (λ_0 est un paramètre) est

$$\begin{pmatrix} -8 \times 3388 & -4 \times 146 & -14 \\ -8 \times 11271 & -4 \times 315 & 2 \\ -8 \times 13384 & 4 \times 147 & 14 \end{pmatrix},$$

dont l'inverse (mapple) est $\begin{pmatrix} -\frac{6}{806\,393} & -\frac{1}{45\,158\,008} & -\frac{1}{134\,456} \\ \frac{191}{460\,796} & -\frac{599}{806\,393} & \frac{5}{9604} \\ -\frac{119\,853}{1612\,786} & \frac{175\,150}{5644\,751} & -\frac{123}{16\,807} \end{pmatrix}$.
D'où en prenant $\lambda_0 = -134456$ et en multipliant cette matrice inverse par la colonne du second membre

$$\begin{pmatrix} 0 \\ 0 \\ -134456 \end{pmatrix},$$ on obtient

$\lambda_3 = 1$, $\lambda_2 = \frac{-5 \times 134456}{9604} = -70, \lambda_1 = \frac{123 \times 134456}{16807} = 984$.
Un polynôme annulateur des ab est donc $P(X) = X^{15} - 70X^{10} + 984X^5 + 134456$.
Comme on sait (par le 4.3.2.1)) que pour tout ab, $d°ab = n_1 n_2 = 15$, c'est que ce polynôme P est le polynôme minimal de tout ab.
Remarque 2 : le 5) de l'annexe 1 ne me permet pas de conclure à l'irréductibilité de $P(X) = X^{15} - 70X^{10} + 984X^5 + 134456$, car les racines de P ont un module $\leq \sqrt[5]{2}\,(|\alpha| + |\beta|) < 1.61 < k - \frac{1}{2}$ pour $k \geq 3$ et pour tout $k = 3$ à 37, $P(k)$ n'est pas premier (site dcode)....et je fatigue pour aller plus loin!

Exemple 4 : $P_1(X) = X^2 + X + 1$, $P_2(X) = X^3 - 2$.
P_1 et P_2 sont irréductibles car ils sont de degré ≤ 3 et sont sans racine rationnelle.

Cas $a + b$
n_1 et n_2 étant premiers entre eux, le 4.3.1) s'applique : $a + b$ prend 6 valeurs qui ont toutes comme polynôme minimal $\pm R_1$ avec $R_1 = res_Y(P_1(Y), P_2(X - Y))$.
R_1 est le déterminant de la matrice

$$\begin{pmatrix} 1 & 0 & 0 & X^3-2 & 0 \\ 1 & 1 & 0 & -3X^2 & X^3-2 \\ 1 & 1 & 1 & 3X & -3X^2 \\ 0 & 1 & 1 & -1 & 3X \\ 0 & 0 & 1 & 0 & -1 \end{pmatrix}$$

soit $X^6+3X^5+6X^4+3X^3+9X+9$: c'est donc le polynôme minimal de tout $a+b$.

Remarque 1 : on peut vérifier l'irréductibilité de R_1 en utilisant le 5) de l'annexe 1.
En effet les racines de R_1 sont de la forme $j^k+j^{k'}\sqrt[3]{2}$ (avec $k=1,2$ et $k'=0,1,2$), donc elles sont de module $< 1+\sqrt[3]{2} < 2,26 < k-\frac{1}{2}$ pour $k \geq 3$ et $R_1(3) \neq 0$, $R_1(4)=8941$ est un nombre premier.
Remarque 2 : détermination de ce polynôme minimal sans utiliser la notion de résultant.
D'après le 2.3) et le 4.2.2), une base du Q espace vectoriel $Q(a,b)$ est $\{1;a;b;ab;b^2;ab^2\}$: on exprime alors les puissances de $(a+b)$ dans cette base.
$(a+b)^0=1$
$a+b=a+b$
$(a+b)^2=-1-a+2ab+b^2$
$(a+b)^3=3-3b-3ab+3ab^2$
$(a+b)^4=9a+6b-6b^2-6ab^2$
$(a+b)^5=-21-21a+15ab+12b^2$
$(a+b)^6=45-36b-36ab+27ab^2$
....et je laisse le lecteur trouver, par résolution d'un systéme, 7 rationnels tels que $\sum_{i=0}^{6}\lambda_i(a+b)^i=0$, cad retrouver le polynôme minimal ci-dessus.

Cas ab
Là encore, on est dans le cadre du 4.2.4) puisque n_1 et n_2 sont deux nombres premiers distincts, donc tout ab a le même polynôme minimal qui est soit $\pm R2$, soit un polynôme de degré n_1, soit un polynôme de degré n_2.
En fait ici le lemme 4.3.0) ne s'applique car $X^3=(X-1)P_1+1$, cad le reste est constant : pour toute racine a de P_1 on a $a^3=1 \in \mathbb{Q}$ (évidemment puisque $a=j$ ou j^2..).
Mais, puisque $a^3=1$, pour tout a, tout b, on a $(ab)^3=a^3b^3=1\times 2=2$, donc tout ab a pour polynôme minimal P_2 et est donc de degré $3=n_2$.

Remarque : cf le 4.1.1), P_2 est donc le seul facteur irréductible de R_2, donc $R_2=P_2^2$: je laisse le lecteur le vérifier par un calcul de déterminant.

6) Huit exemples avec $n_1=d°P_1$ et $n_2=d°P_2$ non premiers entre eux.

Dans le tableau d'exemples ci-dessous, a et b sont respectivement une racine quelconque des polynômes P_1 et P_2, unitaires et irréductibles sur $Q[X]$.
Rappelons que tout polynôme cyclotomique Φ_n (polynôme unitaire dont toutes les racines sont les $\varphi(n)$ racines nièmes de 1 primitives) est irréductible sur $Q[X]$.
Exemples utilisés ici :
$\Phi_3(X)=X^2+X+1$, $\Phi_8(X)=X^4+1$, $\Phi_{24}(X)=X^8-X^4+1$.

Puisque n_1 et n_2 ne sont pas premiers entre eux, les 4.2.3), 4.2.4), 4.3.1.1), 4.3.1.2) ne s'appliquent pas et donc on ne sait pas à prioiri si pour $a+b$ et pour ab il y a un seul polynôme minimal possible.

Proposant parfois plusieurs méthodes (notamment pour l'irréductibilité), certains exemples seront peut être longuets.

Pour quelques exemples je vérifierai le 4.1.1) et le 4.1.2), cad je calculerai R_1 et R_2 pour en déduire les polynômes minimaux de $a+b$ et de ab.

En outre **ces exemples ont été faits avant d'avoir mis au point les quelques généralités du 7) sur le cas** $P_1(X) = X^{n_1} + \alpha_0$ et $P_2(X) = X^{n_2} + \beta_0$.

	P_1 P_2	polynôme minimal de $a+b$	polynôme minimal de ab
1	X^2-2 X^2-2	$X^2-8=2^2((\frac{X}{2})^2-2)$ si $a=b$ X si $a\neq b$	$X-2$ si $a=b$ $X+2$ si $a\neq b$
2	X^2-2 X^2-3	X^4-10X^2+1	X^2-6
3	X^2-2 X^4+1	$X^4+1=P_2(X)$ si $a=-(b+\frac{1}{b})$ X^4-8X^2+25 si $a=b+\frac{1}{b}$	X^2+2X+2 si $a=-(b+\frac{1}{b})$ X^2-2X+2 si $a=b+\frac{1}{b}$
4	X^5-4 X^5-4	$X^5-128=2^5P_1(\frac{1}{2}X)$ si $a=b$ $X^{10}+44X^5-16$ si $a\neq b$	X^5-16
5	X^5-4 X^5-8	$X^5-10X^3+20X-12$ si $ab=2$ $X^{20}+10X^{18}+\ldots+20736$ si $ab\neq 2$ (voir dans la preuve les 21 coefficients)	$X-2$ si $ab=2$ $X^4+2X^3+4X^2+8X+16$ si $ab\neq 2$
6	X^2-2 X^2+X+1	$X^4+2X^3-X^2-2X+7$	X^4+2X^2+4
7	X^2-2 X^8-X^4+1	$X^8-4X^6+15X^4-4X^2+1$ si $a=-(b^3+\frac{1}{b^3})$ $X^8-12X^6+47X^4-84X^2+169$ si $a=b^3+\frac{1}{b^3}$	$X^4+2X^3+2X^2+4X+4$ si $a=-(b^3+\frac{1}{b^3})$ $X^4-2X^3+2X^2-4X+4$ si $a=b^3+\frac{1}{b^3}$
8	X^6-4X^3+2 X^6-4X^3+2	$2^6P_1(\frac{1}{2}X)$ si $a=b$ $P_1(-X)$ si $a\neq b,(ab)^3\neq 2$ $X^9-12X^6-6X^3-64$ si $a\neq b,(ab)^3=2$	X^6-12X^3+4 si $a=b$ ou si $a\neq b,(ab)^3\neq 2$ X^3-2 si $a\neq b,(ab)^3=2$

Preuves :

dans tout ce qui suit, irréductible signifiera irréductible sur $Q[X]$.

exemple 1

Il est immédiat que $a+b$ prend trois valeurs : 0 si $a \neq b$ cad si $a=-b$ et $-2\sqrt{2}$ ou $2\sqrt{2}$ si $a=b$ et ab prend deux valeurs -2 (si $a \neq b$) et 2 si $a=b$, ce qui donne comme polynômes minimaux pour $a+b$ les polynômes X et X^2-8, et les polynômes minimaux pour ab sont $X-2$ et $X+2$.

Remarque : vérification du 4.1.1) et 4.1.2).

cas $a+b$: $R_1(X)$ est le déterminant de

$$\begin{pmatrix} -2 & 0 & X^2-2 & 0 \\ 0 & -2 & -2X & X^2-2 \\ 1 & 0 & 1 & -2X \\ 0 & 1 & 0 & 1 \end{pmatrix}$$, soit en développant par rappport à la première colonne

$R_1(X)=X^4-8X^2$, dont la décomposition en facteurs irréductibles est $X^2(X^2-8)$ et les polynômes minimaux pour $a+b$ sont bien X^2-8 et X.

cas ab : $R_2(X)$ est le déterminant de

$$\begin{pmatrix} -2 & 0 & X^2 & 0 \\ 0 & -2 & 0 & X^2 \\ 1 & 0 & -2 & 0 \\ 0 & 1 & 0 & -2 \end{pmatrix}$$, soit en développant par rappport à la première colonne

$R_1(X)=X^4-8X^2+16$, dont la décomposion en facteurs irréductibles est $(X-2)^2(X+2)^2$ et les polynômes minimaux pour ab sont bien $X-2$ et $X+2$.

exemple 2

X^2-2 et X^2-3 sont évidemment irréductibles car ils n'ont pas de racine rationnelle et sont de degré ≤ 3.

Cas $a+b$

$u=a+b$

$u^2=5+2ab$

$u^4=25+20ab+24=49+10(u^2-5)$

Donc un polynôme annulateur de $a+b$ est X^4-10X^2+1.

Mais ceci est valable pour tout $a+b$, c'est à dire que X^4-10X^2+1 a pour racines $\pm\sqrt{2}\pm\sqrt{3}$:

$X^4-10X^2+1=(X-(\sqrt{2}+\sqrt{3}))(X+(\sqrt{2}+\sqrt{3}))(X-(\sqrt{2}-\sqrt{3}))(X+(\sqrt{2}-\sqrt{3}))$ et bien sûr il n'a aucune rationnelle.

Donc si X^4-10X^2+1 est réductible dans $Q[X]$, c'est que c'est le produit de deux seconds degrés lesquels ne peuvent être, à une constante multiplicative rationnelle près, que de la forme $(X-r)(X-r')$ où r et r' sont deux (distinctes) de ses racines : or il est facile de vérifier que soit $r+r'$, soit rr' n'est pas dans Q et donc cette décomposition est impossible : X^4-10X^2+1 est irréductible sur Q et c'est le polynôme minimal de tout $a+b$.

Remarque 1 : puisque tout $a+b$ est de degré 4, degré qui doit diviser $[Q(a,b):Q] \leq n_1 n_2 = 4$ (cf 4.2.1) c'est que $[Q(a,b):Q]=4$.

Cas ab

On a évidemment $(ab)^2 = 6$ et $X^2 - 6$ est irréductible donc c'est le polynôme minimal de ab.

exemple 3

$X^2 - 2$ est évidemment irréductible, $X^4 + 1$ aussi puisqu'il est cyclotomique, mais cela résulte plus simplement de $X^4 + 1 = (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1)$ et du 2.2) de l'annexe 1.

Tout ϵ_i désignant ± 1, il y a 8 couples possibles pour (a, b) puisque $a = \epsilon_1\sqrt{2}$ et $b = \frac{\sqrt{2}}{2}(\epsilon_2 + i\epsilon_3)$.

On notera tout d'abord que $(b + \frac{1}{b})^2 = \frac{b^4 + 1}{b^2} + 2 = 2$ et donc a et $b + \frac{1}{b}$ sont égaux ou opposés, quelque soient la valeur de a et la valeur de b : $a = b + \frac{1}{b} \Leftrightarrow b^2 - ab + 1 = 0$ et $a = -(b + \frac{1}{b}) \Leftrightarrow b^2 + ab + 1 = 0$.

Ceci se voit aussi en remarquant que b est racine de $(X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1) = (X^2 + aX + 1)(X^2 - aX + 1)$.

cas $a + b$

Les huit couples possibles pour (a, b) donnent huit valeurs distinctes pour $a + b$.

Les quatre valeurs de $a + b$ correspondant à $\epsilon_1 = -\epsilon_2 \Leftrightarrow a = -(b + \frac{1}{b})$ sont $\frac{\sqrt{2}}{2}(\epsilon_1 + i\epsilon_3)$: ce sont les racines de $X^4 + 1$, et donc ces 4 valeurs de $a + b$ ont évidemment $X^4 + 1$ comme polynôme minimal.

Autre façon : $a + b = \frac{-1}{b}$ implique $(a + b)^4 = \frac{1}{b^4} = -1$ et on retrouve $X^4 + 1$.

Les quatre valeurs de $a + b$ correspondant à $\epsilon_1 = \epsilon_2 \Leftrightarrow a = b + \frac{1}{b}$ sont $u = a + b = \frac{\sqrt{2}}{2}(3\epsilon_1 + i\epsilon_3)$:

$u^2 = 4 + 3\epsilon_1\epsilon_3 i$, $u^4 = 7 + 24\varepsilon_1\varepsilon_3 i = 8(4 + 3\epsilon_1\epsilon_3 i) - 25 = 8u^2 - 25$, et donc ces quatre valeurs sont racines de $X^4 - 8X^2 + 25$.

Ce polynôme $X^4 - 8X^2 + 25$ est effectivement irréductible sur Q :

ses racines dans C étant connues, par regroupement 2 à 2 des racines conjuguées, sa décomposition en facteurs irréductibles sur R est $(X^2 - 3\sqrt{2}X + 5)(X^2 + 3\sqrt{2}X + 5)$, donc (voir 2.2) de l'annnexe 1) il est irréductible sur Q. Bien entendu cette factorisation se retrouve via $X^4 - 8X^2 + 25 = (X^2 + 5)^2 - 18X^2$.

Ces quatre valeurs de $a + b$ ont donc $X^4 - 8X^2 + 25$ comme polynôme minimal.

Autre façon : $a + b = 2b + \frac{1}{b}$ implique $(a + b)^2 = 4b^2 + \frac{1}{b^2} + 4$,

$(a + b)^4 = 16b^4 + \frac{1}{b^4} + 16 + 8 + 32b^2 + \frac{8}{b^2}$, soit $(a + b)^4 = 8(a + b)^2 - 25$ et on retrouve $X^4 - 8X^2 + 25$.

Remarque :

$[Q(a, b) : Q] = [Q(a)(b) : Q(a)][Q(a) : Q] = 2[Q(a)(b) : Q(a)]$; $[Q(a)(b) : Q(a)]$ est le degré de b sur $Q(a)$, or b étant racine de $X^2 \pm aX + 1$, il est de degré 1 ou 2, mais 1 est impossible, car b qui n'est pas réel ne peut être dans $Q(a)$, donc $[Q(a)(b) : Q(a)] = 2$ et $[Q(a, b) : Q] = 4$.

Donc tout élément de $Q(a,b)$ est de degré 1 ou 2 ou 4.
Et le théorème sur la multiplication des degrés (voir 2.3) dit alors qu'une base de l'espace vectoriel $Q(a,b)$ sur Q est $\{1,a,b,ab\}$, a étant degré 2 sur Q et b de degré 2 sur $Q(a)$.
Donc tout élément u de $Q(a,b)$ est une combinaison linéaire à coefficients dans Q de $1,a,b,ab$: ainsi $1,u,u^2,u^3,u^4$ sont forcéments Q –liés, ce qu'on a effectivement constaté ci-dessus pour $u=a+b,$ qui est de degré 4.

cas ab

ab ne prend que les 4 valeurs $\pm 1 \pm i$:

si $a=-b-\frac{1}{b} \Leftrightarrow b$ racine de $X^2+aX+1,$ alors

$(ab)^2=2b^2=2(-ab-1)$ et ab est racine de X^2+2X+2 qui est irréductible sur Q

si $a=b+\frac{1}{b} \Leftrightarrow b$ racine de $X^2-aX+1,$ alors

$(ab)^2=2b^2=2(ab-1)$ et ab est racine de X^2-2X+2 qui est irréductible sur Q.
Remarque : $(X^2+2X+2)(X^2-2X+2)= X^4+4$.

exemple 4

a et b sont donc les racines deX^5-4 (irréductible d'après le 4) de l'annexe 1) ,
c'est-à-dire a prend les valeurs $a_j=\sqrt[5]{4}\,\zeta^j$ pour $j=0,1,2,3,4$ et b prend les valeurs
$b_k=\sqrt[5]{4}\,\zeta^k$ pour $k=0,1,2,3,4$ avec $\zeta=e^{\frac{2i\pi}{5}}$ $(i^2=-1)$.
Rappel : ζ^1 et ζ^4 sont conjugués, de même ζ^2 et ζ^3.
ζ est algébrique de degré 4 sur Q : ζ étant racine de
$X^4+X^3+X^2+X+1=(X-\zeta)(X-\zeta^4)(X-\zeta^2)(X-\zeta^3)$
$=(X^2-2\cos\frac{2\pi}{5}X+1)(X^2-2\cos\frac{4\pi}{5}X+1),$
on voit que $\cos\frac{2\pi}{5}+\cos\frac{4\pi}{5}=\frac{-1}{2},$ $\cos\frac{2\pi}{5}\cos\frac{4\pi}{5}=\frac{-1}{4}$ et donc $\cos\frac{2\pi}{5}$ et $\cos\frac{4\pi}{5}$ sont les racines de $4X^2+2X-1$, à savoir $\frac{-1\pm\sqrt{5}}{4}$, qui ne sont pas rationnelles, et d'après le 2) de l'annexe 1, $X^4+X^3+4X+X+1$ est irréductible, ce qui prouve que ζ est algébrique sur Q de degré 4.
Bien sûr, l'irréductibilité de $X^4+X^3+X^2+X+1$ résulte du fait que ce polynôme est en fait Φ_5.

Déterminons le degré r de l'extension $Q(a,b)$ de Q.

si $a=b$, alors $Q(a,b)=Q(a)$ et $r=5$, puisque a est algébrique de degré 5 sur Q.

si $a\neq b,$ commencons par montrer que $Q(a,b)=Q(\sqrt[5]{4},\zeta),$ puis $r=20$.

On a évidemment $Q(a,b)\subset Q(\sqrt[5]{4},\zeta)$ car $Q(\sqrt[5]{4},\zeta)$ contient a et b.
$\frac{a}{b}=\zeta^{j-k}$ avec $j-k$ non multiple de 5 : ainsi ζ^{j-k} est un générateur du groupe des racines 5ièmes de 1, et comme $\zeta^{j-k}=\frac{a}{b}\in Q(a,b),$ ζ est aussi dans $Q(a,b)$.
Donc $\sqrt[5]{4}=\frac{a}{\zeta^j}\in Q(a,b),$ ce qui prouve $Q(\sqrt[5]{4},\zeta)\subset Q(a,b),$ soit finalement
$Q(\sqrt[5]{4},\zeta)=Q(a,b)$.
Ainsi $r=[Q(\sqrt[5]{4})(\zeta):Q(\sqrt[5]{4})][Q(\sqrt[5]{4}):Q]=[Q(\zeta)(\sqrt[5]{4}):Q(\zeta)][Q(\zeta):Q]$ et
$r=5[Q(\sqrt[5]{4})(\zeta):Q(\sqrt[5]{4})]=4[Q(\zeta)(\sqrt[5]{4}):Q(\zeta)],$ puisque $\sqrt[5]{4}$ est algébrique de degré 5 sur Q car racine de X^5-4 irréductible et ζ est algébrique sur Q de degré 4 sur Q.

Donc r étant divisible par 4 et 5, il est divisible par 20; mais ζ étant racine de $X^4+X^3+X^2+X+1 \in Q(\sqrt[5]{4})[X]$, son degré sur $Q(\sqrt[5]{4})$ est ≤ 4, donc $r = 5[Q(\sqrt[5]{4})(\zeta) : Q(\sqrt[5]{4})] \leq 20$, et comme 20 divise r, c'est que dans ce cas $r = 20$: on retrouvera le même degré d'extension dans l'exemple 8 pour le cas $ab \neq 2$.

Cas $a+b$

Il y a 15 valeurs possibles pour $a+b$: cinq avec $j = k = 0,1,2,3,4$ et 10 avec $0 \leq j < k \leq 4$ (car évidemment $a_j + b_k = a_k + b_j$)

pour les cinq valeurs de $a+b$ telles que $a = b$, $a+b = 2a = 2\sqrt[5]{4}\,\zeta^j$ pour $j = 0,1,2,3,4$, et on a $(a+b)^5 = 128$, et comme $X^5 - 128$ est irréductible (voir 4) de l'annexe 1), c'est le polynôme minimal de ces cinq valeurs de $a+b$.

Autre façon : $P_1(\frac{a+b}{2}) - 4 = P_1(a) - 4 = 0$, donc $P_1(\frac{X}{2}) - 4 = \frac{X^5}{32} - 4$ est annulateur pour $a+b$, donc $32(\frac{X^5}{32} - 4) = X^5 - 128$ est aussi annulateur.

pour les dix valeurs $a+b = \sqrt[5]{4}\,(\zeta^j + \zeta^k)$ pour $0 \leq j < k \leq 4$ (on verra plus loin qu'elles sont effectivement distinctes)

on pose $u = a+b = \sqrt[5]{4}\,(\zeta^j + \zeta^k)$

$u^5 = 4(2 + 5\zeta^{4j}\zeta^k + 5\zeta^j\zeta^{4k} + 10\zeta^{3j}\zeta^{2k} + 10\zeta^{2j}\zeta^{3k})$

$u^{10} = (u^5)^2 = 16[4 + 25\zeta^{3j}\zeta^{2k} + 25\zeta^{2j}\zeta^{3k} + 100\zeta^j\zeta^{4k} + 100\zeta^{4j}\zeta^k$

$+20\zeta^{4j}\zeta^k + 20\zeta^j\zeta^{4k} + 40\zeta^{3j}\zeta^{2k} + 40\zeta^{2j}\zeta^{3k}$

$+50 + 100\zeta^{2j}\zeta^{3k} + 100\zeta^j\zeta^{4k} + 100\zeta^{4j}\zeta^k + 100\zeta^{3j}\zeta^{2k} + 200]$

$u^{10} = 16[254 + 220\zeta^{4j}\zeta^k + 220\zeta^j\zeta^{4k} + 165\zeta^{3j}\zeta^{2k} + 165\zeta^{2j}\zeta^{3k}]$

Et comme $16 \times 220 + 44 \times 20 = 16 \times 165 + 44 \times 40 = 4400$, on obtient

$u^{10} + 44u^5 = 16 \times 254 + 44 \times 8 + 4400(\zeta^{4j}\zeta^k + \zeta^{3j}\zeta^{2k} + \zeta^{2j}\zeta^{3k} + \zeta^j\zeta^{4k})$.

Mais $(\zeta^j)^5 - (\zeta^k)^5 = 0 = (\zeta^j - \zeta^k)(\zeta^{4j} + \zeta^{3j}\zeta^k + \zeta^{2j}\zeta 2^k + \zeta^j\zeta^{3k} + \zeta^{4k})$ et puisque $\zeta^j \neq \zeta^k$,

$\zeta^{4j} + \zeta^{3j}\zeta^k + \zeta^{2j}\zeta^{2k} + \zeta^j\zeta^{3k} + \zeta^{4k} = 0$, soit en multipliant par ζ^k,

$\zeta^{4j}\zeta^k + \zeta^{3j}\zeta^{2k} + \zeta^{2j}\zeta^{3k} + \zeta^j\zeta^{4k} + 1 = 0$.

Finalement $u^{10} + 44u^5 = 4416 - 4400 = 16$ et ainsi un polynôme annulateur de ces dix valeurs de $a+b$ est $P(X) = X^{10} + 44X^5 - 16$.

Ce polynôme P est-il irréductible ?

En tout cas il n'a aucune racine rationnelle puisque $(\frac{p}{q})^{10} + 44(\frac{p}{q})^5 - 16 = 0$ avec p et $q > 0$ premiers entre eux implique que p divise 16 et $q = 1$, ce qui donne aucune racine de P.

Appliquons le 4) de l'annexe 1 pour montrer l'irréductibilité de $P(X) = X^{10} + 44X^5 - 16$.

En résolvant $z^2 + 44z - 16 = 0$ on voit que les racines de P peuvent s'écrire sous la forme $\sqrt[5]{-22 + 10\sqrt{5}}\,\zeta^l$ et $-\sqrt[5]{22 + 10\sqrt{5}}\,\zeta^l$,

Donc pour toute racine z de P, $|z| \leq \sqrt[5]{22 + 10\sqrt{5}} = 2.13\ldots < 2.14 < k - \frac{1}{2}$ pour $k \geq 3$..

Comme $P(4) \neq 0$ et $P(5) = 9903109$ est un nombre premier, P est irréductible et P est le polyôme minimal des dix valeurs de $a+b$ avec $0 \leq j < k \leq 4$, lesquelles valeurs sont effectivement distinctes puisque racines d'un polynôme irréductible.

Remarque 1 : de part la construction ci-dessus de P, les dix racines de P (divisées par $\sqrt[5]{4}$) sont évidemment

$1+\zeta, 1+\zeta^2, 1+\zeta^3, 1+\zeta^4, \zeta+\zeta^2, \zeta+\zeta^3, \zeta+\zeta^4, \zeta^2+\zeta^3, \zeta^2+\zeta^4, \zeta^3+\zeta^4$

Les deux réelles sont $\sqrt[5]{4}\,(\zeta + \zeta^4) = 2\sqrt[5]{4}\cos\frac{2\pi}{5}$ et $\sqrt[5]{4}\,(\zeta^2 + \zeta^3) = 2\sqrt[5]{4}\cos\frac{4\pi}{5}$.

Donc $\sqrt[5]{-22 + 10\sqrt{5}} = 2\sqrt[5]{4}\cos\frac{2\pi}{5}$ et $-\sqrt[5]{22 + 10\sqrt{5}} = 2\sqrt[5]{4}\cos\frac{4\pi}{5}$.

Cas ab

Il y a cinq valeurs possibles pour ab : $\sqrt[5]{16}\,\zeta^l$ pour $l = 0,1,2,3,4$ qui vérifient toutes $(ab)^5 = 16$ et donc le polynôme minimal de ces cinq valeurs est $X^5 - 16$ (il est irréductible d'après le 4 de l'annexe 1).

Remarque 2 : vérification du 4.1.1) et 4.1.2).

cas $a+b$: $R_1(X)$ est le déterminant de

$$\begin{pmatrix}
-4 & 0 & 0 & 0 & 0 & X^5-4 & 0 & 0 & 0 & 0 \\
0 & -4 & 0 & 0 & 0 & -5X^4 & X^5-4 & 0 & 0 & 0 \\
0 & 0 & -4 & 0 & 0 & 10X^3 & -5X^4 & X^5-4 & 0 & 0 \\
0 & 0 & 0 & -4 & 0 & -10X^2 & 10X^3 & -5X^4 & X^5-4 & 0 \\
0 & 0 & 0 & 0 & -4 & 5X & -10X^2 & 10X^3 & -5X^4 & X^5-4 \\
1 & 0 & 0 & 0 & 0 & -1 & 5X & -10X^2 & 10X^3 & -5X^4 \\
0 & 1 & 0 & 0 & 0 & 0 & -1 & 5X & -10X^2 & 10X^3 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 5X & -10X^2 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 5X \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1
\end{pmatrix}$$

soit (via mapple) : $-X^{25} + 40X^{20} + 9360X^{15} + 245\,120X^{10} - 180\,480X^5 + 32\,768$ et on peut vérifier qu'il est égal à
$-(X^5 - 128)(X^{10} + 44X^5 - 16)^2$ et on retrouve bien les deux polynômes minimaux pour $a+b$.

cas ab : $R_2(X)$ est le déterminant de

$$\begin{pmatrix}
-4 & 0 & 0 & 0 & 0 & X^5 & 0 & 0 & 0 & 0 \\
0 & -4 & 0 & 0 & 0 & 0 & X^5 & 0 & 0 & 0 \\
0 & 0 & -4 & 0 & 0 & 0 & 0 & X^5 & 0 & 0 \\
0 & 0 & 0 & -4 & 0 & 0 & 0 & 0 & X^5 & 0 \\
0 & 0 & 0 & 0 & -4 & 0 & 0 & 0 & 0 & X^5 \\
1 & 0 & 0 & 0 & 0 & -4 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & -4 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & -4 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -4 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -4
\end{pmatrix}$$

soit (via mapple) $-X^{25} + 80X^{20} - 2560X^{15} + 40\,960X^{10} - 327\,680X^5 + 1048\,576 = -(X^5 - 16)^5$ et on retrouve bien l'unique polynôme minimal pour ab.

exemple 5

Les polynômes $X^5 - 4$ et $X^5 - 8$ sont irréductibles d'après le 4) de l'annexe 1.
Les cinq racines de $X^5 - 4$ sont $a_j = \sqrt[5]{4}\,\zeta^j$ pour $j = 0,1,2,3,4$ et celles de $X^5 - 8$ sont $b_k = \sqrt[5]{8}\,\zeta^k$ pour $k = 0,1,2,3,4$ avec $\zeta = e^{\frac{2i\pi}{5}}$ ($i^2 = -1$).
Rappel : ζ et ζ^4 sont conjuguées, de même ζ^2 et ζ^3.

Déterminons le degré r de l'extension $Q(a,b)$ de Q.

si $ab = 2$, alors $Q(a,b) = Q(a)$ et $r = 5$, puisque a est algébrique de degré 5 sur Q.

si $ab \neq 2$, commencons par montrer que $Q(a,b) = Q(\sqrt[5]{2},\zeta)$, puis $r = 20$.

On a évidemment $Q(a,b) \subset Q(\sqrt[5]{2},\zeta)$ car $Q(\sqrt[5]{2},\zeta)$ contient a et b.

$ab = 2\zeta^l$ avec l non multiple de 5 (sinon $ab = 2$) : ainsi ζ^l est un générateur du groupe des racines 5ièmes de 1, et comme $\zeta^l = \frac{ab}{2} \in Q(a,b)$, ζ est aussi dans $Q(a,b)$.

Donc $\sqrt[5]{4} = \frac{a}{\zeta^j}$ et $\sqrt[5]{8} = \frac{b}{\zeta^k}$ sont dans $Q(a,b)$, et par conséquent $\sqrt[5]{2} = \frac{\sqrt[5]{8}}{\sqrt[5]{4}}$ est aussi dans $Q(a,b)$, ce qui prouve $Q(\sqrt[5]{2},\zeta) \subset Q(a,b)$, soit finalement $Q(\sqrt[5]{2},\zeta) = Q(a,b)$.

Ainsi $r = [Q(\sqrt[5]{2})(\zeta) : Q(\sqrt[5]{2})][Q(\sqrt[5]{2}) : Q] = [Q(\zeta)(\sqrt[5]{2}) : Q(\zeta)][Q(\zeta) : Q]$ et $r = 5[Q(\sqrt[5]{2})(\zeta) : Q(\sqrt[5]{2})] = 4[Q(\zeta)(\sqrt[5]{2}) : Q(\zeta)]$, puisque $\sqrt[5]{2}$ est algébrique de degré 5 car racine de $X^5 - 2$ irréductible (d'après le 4) de l'annexe 1) et puisque ζ est algébrique de degré $\varphi(5) = 4$ sur Q (voir preuve directe à l'exemple 2).

Donc r étant divisible par 4 et 5, il est divisible par 20; mais ζ étant racine de $X^4 + X^3 + X^2 + X + 1 \in Q(\sqrt[5]{2})[X]$, son degré sur $Q(\sqrt[5]{2})$ est ≤ 4, donc $r = 5[Q(\sqrt[5]{2})(\zeta) : Q(\sqrt[5]{2})] \leq 20$, et comme 20 divise r, c'est que dans ce cas $r = 20$.

Cas $a + b$

si $ab = 2$, $a = \sqrt[5]{4}\zeta^j$ avec $j \in \{0;1;2;3;4\}$ et $b = \sqrt[5]{8}\zeta^{-j} = \sqrt[5]{8}\zeta^{5-j}$, ce qui donne cinq valeurs prises par $a + b$.

On peut obtenir un polynôme annulateur en faisant le produit des cinq $(X - (a + b))$, mais là le calcul des puissances de $a + b$ me semble plus rapide ($ab = 2, a^5 = 4, b^5 = 8$) :

$u = a + b$

$u^3 = a^3 + b^3 + 3ab(a + b) = a^3 + b^3 + 6u$

$u^5 = a^5 + b^5 + 5ab(a^3 + b^3) + 10a^2b^2(a + b) = 12 + 10(u^3 - 6u) + 40u$

Et donc u est racine de $X^5 - 10X^3 + 20X - 12$: ce polynôme est-il le polynôme minimal de ces cinq valeurs de $a + b$?

Considérons la valeur $a + b = \sqrt[5]{4} + \sqrt[5]{8} = \sqrt[5]{4} + \frac{2}{\sqrt[5]{4}}$: si elle était égale à un rationnel q, alors $(\sqrt[5]{4})^2 - \sqrt[5]{4} + 2 = 0$ et $\sqrt[5]{4}$ serait algébrique sur Q de degré ≤ 2 or $\sqrt[5]{4}$ est de degré 5 (racine de $X^5 - 4$ irréductible), donc $a + b = \sqrt[5]{4} + \sqrt[5]{8}$ n'est pas rationnel, et ainsi son degré qui divise 5 ($Q(a,b)$ est une extension de Q de degré 5) est 5.

Le polynôme minimal de $\sqrt[5]{4} + \sqrt[5]{8}$ est donc de degré 5 : c'est obligatoirement $X^5 - 10X^3 + 20X - 12$, lequel est donc irréductible et est le polynôme minimal de toutes les valeurs $a + b$ lorsque $ab = 2$.

si $ab \neq 2$

Il est facile de voir qu'il y a alors 20 couples (a,b) possibles (25 – les cinq couples du cas $ab = 2$) qui donnent 20 valeurs pour $a + b$.

Mais ici $Q(a,b)$ est une extension de Q de degré 20 et donc le degré de $a + b$ peut prendre la valeur 20 : je renonce aux calculs ...à la main, et je vais utiliser la méthode des résultants pour trouver un polynôme annulateur.

D'après le 4.1.1), un polynôme annulateur, de chacune de ces vingt valeurs de $a + b$, est $R_1(X) = res_Y(P_1(Y), P_2(X - Y))$ soit le résultant des deux polynômes en Y suivants : $Y^5 - 4$ et $(X - Y)^5 - 8$ et .

Ce résultant est le déterminant de la matrice

$$\begin{pmatrix}
-4 & 0 & 0 & 0 & 0 & X^5-8 & 0 & 0 & 0 & 0 \\
0 & -4 & -0 & 0 & 0 & -5X^4 & X^5-8 & 0 & 0 & 0 \\
0 & 0 & -4 & 0 & 0 & 10X^3 & -5X^4 & X^5-8 & 0 & 0 \\
0 & 0 & 0 & -4 & 0 & -10X^2 & 10X^3 & -5X^4 & X^5-8 & 0 \\
0 & 0 & 0 & 0 & -4 & 5X & -10X^2 & 10X^3 & -5X^4 & X^5-8 \\
1 & 0 & 0 & 0 & 0 & -1 & 5X & -10X^2 & 10X^3 & -5X^4 \\
0 & 1 & 0 & 0 & 0 & 0 & -1 & 5X & -10X^2 & 10X^3 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 5X & -10X^2 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 5X \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1
\end{pmatrix},$$

soit (mapple) $R_1(X) = -X^{25} + 60X^{20} + 18\,560X^{15} + 737\,280X^{10} - 423\,680X^5 + 248\,832.$

Mais, toujours d'après le 4.1.1), les facteurs irréductibles de R_1 sont tous les polynômes minimaux possibles pour les $a+b$; or on vient de voir que $X^5 - 10X^3 + 20X - 12$ est un de ces polynômes minimaux (celui des $a+b$ avec $ab = 2$), donc il divise $-R_1$.

Le quotient de cette division est

$P(X) =$

$X^{20} + 10X^{18} + 80X^{16} - 48X^{15} + 600X^{14} - 360X^{13} + 4400X^{12} - 1680X^{11} + 12\,864X^{10}$

$-2400X^9 + 36\,320X^8 + 62\,400X^7 + 85\,760X^6 + 89\,088X^5 + 102\,400X^4 + 78\,720X^3 + 57\,600X^2$

$+34\,560X + 20\,736$

qui est donc un polynôme annulateur des vingt valeurs possibles de $a+b$ lorsque $ab \neq 2$.

Ce polynôme P est-il irréductible ?

Appliquons le 5) de l'annexe 1 pour montrer l'irréductibilité de $P(X)$.

Si z est une racine de P, $|z| \leq \sqrt[5]{4} + \sqrt[5]{8} = 2.83\ldots < 2.84 < k - \frac{1}{2}$ pour $k \geq 4$.

Comme $P(18) \neq 0$ et $P(19) = 38\,654\,067\,466\,104\,954\,195\,401\,291$ est un nombre premier (www.dcode.fr), P est irréductible sur Q.

Donc le polynôme minimal de chacune des 20 valeurs possibles de $a+b$ correspondantes à $ab \neq 2$ est ce polynôme P de degré 20.

Remarque : ici pour $k = 5, 7, 9, 11, 13, 15, 17,$ $P(k)$ n'est pas premier!

cas ab

ab prend les cinq valeurs $2\zeta^l$ pour $l = 0, 1, 2, 3, 4$ qui vérifient toutes $(ab)^5 = 32,$ donc $X^5 - 32 = X^5 - 2^5 = (X-2)(X^4 + 2X^3 + 4X^2 + 8X + 16)$ est un polynôme annulateur.

Pour $l = 0,$ $ab = 2$ et a pour polynôme minimal $X - 2$.

Les quatre autres valeurs de ab sont les racines de $X^4 + 2X^3 + 4X^2 + 8X + 16 = 16((\frac{X}{2})^4 + (\frac{X}{2})^3 + (\frac{X}{2})^2 + (\frac{X}{2}) + 1)$ qui est irréductible puisque on a vu au début de cet exemple que $X^4 + X^3 + X^2 + X + 1$ l'était : c'est donc le polynôme minimal des quatre valeurs de ab distinctes de 2.

On remarquera que dans ce cas ab est algébrique de degré 1 ou $4,$ qui sont bien des diviseurs du degré 4 de l'extension $Q(a,b)$ de Q (voir début de cet exemple).

exemple 6

$X^2 - 2$ et $X^2 + X + 1$ sont évidemment irréductibles.

cas $a+b$

$a+b$ prend les quatres valeurs $\pm\sqrt{2}+j$ et $\pm\sqrt{2}+j^2$, conjuguées 2 à 2 puisque j et j^2 sont conjugués.

$a+b$ est donc racine de $(X-(\sqrt{2}+j))(X-(\sqrt{2}+j^2))(X-(-\sqrt{2}+j))(X-(-\sqrt{2}+j)^2)$, soit $(X^2-(2\sqrt{2}-1)X+3-\sqrt{2})(X^2+(2\sqrt{2}+1)X+3+\sqrt{2})=X^4+2X^3-X^2-2X+7$ qui est irréductible d'après le 2.2 de l'annexe 1, et c'est donc le polynôme minimal des quatre valeurs prises par $a+b$.

Remarque 1 : autre façon d'obtenir le polynôme minimal de tout $a+b$.

$a+b\in Q(a,b)$ extension de Q de degré
$r=[Q(a)(b):Q]=[Q(a)(b):Q(a)][Q(a):Q]=2[Q(a)(b):Q(a)]$.
Mais b est racine de $X^2+X+1\in Q(a)[X]$, donc son degré sur $Q(a)$ est 1 ou 2, mais $\sqrt{3}\notin Q(\sqrt{2})=Q(a)$, donc $b\notin Q(a)$ et ainsi le degré de b sur $Q(a)$ est 2 et $r=4$: le degré de $a+b$ est donc un diviseur de 4, ce qu'on a constaté ci-dessus, son degré étant 4.

D'après le 2.3), $\{1,a,b,ab\}$ étant une base du Q –espace vectoriel $Q(a,b)$, si on veut utiliser la méthode des puissances pour retrouver le polynôme minimal on est amené à calculer les puissances suivantes :

$u^0=1$

$u=a+b$

$u^2=2ab-b+1$

$u^3=-3ab+6b-a+1$

$u^4=8ab-11b+4a-8$

Il faut trouver des $\lambda_i\in Q$ tels que $\sum_{i=0}^{4}\lambda_i u^i=0$, c'est-à-dire résoudre le systéme :

(1) $\lambda_0+\lambda_2+\lambda_3-8\lambda_4=0$

(2) $\lambda_1-\lambda_3+4\lambda_4=0$

(3) $\lambda_1-\lambda_2+6\lambda_3-11\lambda_4=0$

(4) $2\lambda_2-3\lambda_3+8\lambda_4=0$

La résolution peut se faire ici "à la main" :

de (2) on tire $\lambda_1=\lambda_3-4\lambda_4$ que l'on reporte dans (3), d'où $\lambda_2=7\lambda_3-15\lambda_4$, puis en reportant dans (4) on obtient $11\lambda_3-22\lambda_4=0$.

On peut donc prendre $\lambda_4=1,\lambda_3=2$, puis $\lambda_2=14-15=-1,\lambda_1=2-4=-2$ et $\lambda_0=1-2+8=7$ et on trouve comme polynôme annulateur de $a+b$, le polynôme $X^4+2X^3-X^2-2X+7$ qui est le polynôme minimal trouvé ci-dessus.

cas ab

ab prend les quatre valeurs $\sqrt{2}j,\sqrt{2}j^2,-\sqrt{2}j,-\sqrt{2}j^2$ et donc un polynôme annulateur est $(X-\sqrt{2}j)(X-\sqrt{2}j^2)(X+\sqrt{2}j)(X+\sqrt{2}j^2)=(X^2+\sqrt{2}X+2)(X^2-\sqrt{2}X+2)=X^4+2X^2+4$ qui est irréducitible sur Q d'après le 2.2) de l'annexe 1, et c'est donc le polynôme minimal de ab.

exemple 7

L'irréductibilité de $P_2(X)=X^8-X^4+1$ est évidente puisque c'est le polynôme cyclotomique Φ_{24}.

Deux autres façons de montrer l'irréductibilité :

en utilisant le 5) de l'annexe 1 :

les racines de $P_2(X)=X^8-X^4+1$ sont de module 1 (puisque ce sont les racines

24-ièmes de 1 primitives), il faut prendre $k > 1 + \frac{1}{2}$, soit $k \geq 2$, et comme $P_2(1) \neq 0$ et $P_2(2) = 241$ est un nombre premier, P_2 est irréductible

en utilisant le 2.1) de l'annexe 1 (beaucoup plus long) :

P_2 étant Φ_{24}, les huit racines de $X^8 - X^4 + 1$ sont les $\varphi(24) = 8$ racines 24-ièmes de 1 primitives, à savoir $e^{\frac{2\pi i}{24}m} = e^{\frac{\pi i}{12}m}$ avec m premier avec 24 et < 24, soit $m \in \{1;5;7;11;13;17;19;23\}$.

On peut les obtenir sans utiliser la notion de polynôme cyclotomique :

$X^{12} + 1 = (X^4)^3 + 1^3 = (X^4 + 1)(X^8 - X^4 + 1)$.

Les douze racines de $X^{12} + 1$ sont les racines douzièmes de -1, à savoir $v_k = e^{i\frac{\pi}{12}} \times e^{i\frac{2k\pi}{12}} = e^{i\frac{\pi}{12}(1+2k)}$, pour $k = 0, 1, 2, \ldots, 11$, qui sont évidemment opposées deux à deux ($v_{k+6} = -v_k$) et donc les douze racines de $X^{12} + 1$ sont $\pm v_0, \pm v_1, \pm v_2, \pm v_3, \pm v_4, \pm v_5$.

Notons aussi que $v_{11-k} = -v_{5-k}$ et v_k sont conjuguées.

D'après l'exemple 6 précédent $X^4 + 1$ est irréductible et ses racines sont $\frac{\sqrt{2}}{2}(\epsilon_2 + i\epsilon_3)$, soit $\pm v_1 = \pm\frac{\sqrt{2}}{2}(1 + i)$ et $\pm v_4 = \pm\frac{\sqrt{2}}{2}(-1 + i)$.

Les huit racines de $X^8 - X^4 + 1$, c'est-à-dire les huit valeurs possibles de b, sont donc $\pm v_0, \pm v_2, \pm v_3, \pm v_5$.

Le regroupement des racines conjuguées va permettre d'obtenir la décomposition de $X^8 - X^4 + 1$ en facteurs irréductibles dans R.

v_0 et $-v_5$ sont les racines de $X^2 - 2\cos(\frac{\pi}{12})X + 1$, $-v_0$ et v_5 sont les racines de $X^2 + 2\cos(\frac{\pi}{12})X + 1$

v_2 et $-v_3$ sont les racines de $X^2 - 2\cos(\frac{5\pi}{12})X + 1$, $-v_2$ et v_3 sont les racines de $X^2 + 2\cos(\frac{5\pi}{12})X + 1$

Donc $X^8 - X^4 + 1 =$

$(X^2 - 2\cos(\frac{\pi}{12})X + 1)(X^2 + 2\cos(\frac{\pi}{12})X + 1)(X^2 - 2\cos(\frac{5\pi}{12})X + 1)(X^2 + 2\cos(\frac{5\pi}{12})X + 1)$.

Le produit de trois de ces facteurs irréductibles dans R ne peut être dans $Q[X]$ (sinon d'après le 1) de l'annexe 1) le 4ième y serait, ce qui est faux, $\cos(\frac{\pi}{12})$ et $\cos(\frac{5\pi}{12})$ n'étant pas rationnels d'après l'annexe 3) et les formules $\cos p + \cos q = \ldots$ et $\cos p \cos q = \ldots$ permettent de voir que le produit quelconque de deux ces facteurs irréductibles dans R n'est pas dans $Q[X]$,: donc, d'après le 2.1) de l'annexe 1, $X^8 - X^4 + 1$ est irréductible sur Q, et ainsi c'est le polynôme minimal de ses huit racines.

Notons que puisque $b^{12} + 1 = 0$, $(b^3 + \frac{1}{b^3})^2 = \frac{b^{12} + 2b^6 + 1}{b^6} = 2 = a^2$, et donc $a = \pm(b^3 + \frac{1}{b^3})$, ce qui en fait est une conséquence de l'exemple 6 précédent puisque b^3 est une racine de $X^4 + 1$.

On peut préciser dans quels cas, on a + ou − : les valeurs de b étant $\pm v_0, \pm v_2, \pm v_3, \pm v_5$ et puisque $v_k^3 + \frac{1}{v_k^3} = e^{i\frac{(1+2k)\pi}{4}} + e^{-i\frac{(1+2k)\pi}{4}} = \sqrt{2}\,\mathrm{Re}((1+i)e^{i\frac{k\pi}{2}})$,

c'est que $v_0^3 + \frac{1}{v_0^3} = \sqrt{2}$, $v_2^3 + \frac{1}{v_2^3} = -\sqrt{2}$, $v_3^3 + \frac{1}{v_3^3} = \sqrt{2}$, $v_5^3 + \frac{1}{v_5^3} = -\sqrt{2}$.

Avant d'aller plus loin, cherchons tout de suite une base du Q –espace vectoriel $Q(a, b)$.

Puisque $a = \pm(b^3 + \frac{1}{b^3})$, $a \in Q(b)$ et $Q(a,b) = Q(b)$ et comme le polynôme minimal de b est $X^8 - X^4 + 1$, $[Q(b) : Q] = 8$ et donc une base de $Q(a,b) = Q(b)$ est $\{1, b, b^2, b^3, b^4, b^5, b^6, b^7\}$.
On peut déjà dire, d'après le 2.4), que le degré de tout $a+b$ et de tout ab est un diviseur de 8.

Cas $a+b$

Les seize couples (a,b) possibles donnent seize valeurs possibles pour $a+b$: les huit valeurs $\sqrt{2} \pm v_0, \sqrt{2} \pm v_2, \sqrt{2} \pm v_3, \sqrt{2} \pm v_5$ et leurs opposées.
Notons que puisque $b^8 = b^4 - 1$, on a aussi
$b^9 = b^5 - b, b^{10} = b^6 - b^2, b^{11} = b^7 - b^3, b^{12} = -1$
$\frac{1}{b} = b^3 - b^7, \frac{1}{b^2} = b^2 - b^6, \frac{1}{b^3} = b - b^5.$

si $a = -(b^3 + \frac{1}{b^3})$

alors $u = a + b = -(b^3 + b - b^5) + b = -b^3 + b^5$.
D'où (il suffit ici de de calculer les puissances paires de u jusqu'à u^8)
$u^2 = 2b^6 - 2b^4 - b^2 + 2$
$u^4 = 4b^6 - 7b^4 + 4b^2$ (carré du précédent)
$u^6 = -15b^6 + 30b^2 - 26$ (produit des deux précédents)
$u^8 = -112b^6 + 97b^4 + 56b^2 - 97.$
Les 3 premières égalités permettent d'obtenir b^2, b^4, b^6 en fonction de u (résolution d'un systéme)
$30b^2 = -4u^6 + 20u^4 - 70u^2 + 36$
$30b^4 = -8u^6 + 30u^4 - 120u^2 + 32$
$-3b^6 = u^6 - 4u^4 + 14u^2 - 2,$
et en reportant dans la dernière relation, on obtient, au pris de certains calculs...
$u^8 = 4u^6 - 15u^4 - 4u^2 + 1,$ cad un polynôme de $Q[X]$ annulateur de u est
$P(X) = X^8 - 4X^6 + 15X^4 - 4X^2 + 1.$

Pour montrer l'irréductibilité de P sur Q, on va utiliser le 2.1) de l'annexe 1.
En effet les racines de P sont connues, ce sont les huit valeurs possibles de $a+b$ lorsque $a = -(b^3 + \frac{1}{b^3})$, à savoir les huit valeurs de $-(b^3 + \frac{1}{b^3}) + b$ lorsque b décrit les huit racines de $X^8 - X^4 + 1$, soit $\pm v_0, \pm v_2, \pm v_3, \pm v_5$ (voir plus haut l'évaluation de $v_k^3 + \frac{1}{v_k^3}$ lorsque $k = 0, 2, 3, 5$) :
$\pm(\sqrt{2} - v_0), \pm(\sqrt{2} + v_2), \pm(\sqrt{2} - v_3), \pm(\sqrt{2} + v_5).$
Donc en regroupant les racines conjuguées, la décomposition en facteurs irréductibles dans $R[X]$ de P est
$P(X) = F_1(X)F_1(-X)F_2(X)F_2(-X)$ avec
$F_1(X) = (X + \sqrt{2} - e^{\frac{i\pi}{12}})(X + \sqrt{2} + e^{\frac{i11\pi}{12}}) = X^2 + \frac{\sqrt{2}}{2}(3 - \sqrt{3})X + 2 - \sqrt{3}$ (racines $-\sqrt{2} + v_0$ et $-\sqrt{2} - v_5$)
$F_2(X) = (X + \sqrt{2} + e^{\frac{i5\pi}{12}})(X + \sqrt{2} - e^{\frac{i7\pi}{12}}) = X^2 + \frac{\sqrt{2}}{2}(3 + \sqrt{3})X + 2 + \sqrt{3}$ (racines $-\sqrt{2} - v_2$ et $-\sqrt{2} + v_3$).
On vérifie que $F_1(X)F_1(-X) \notin Q[X]$ (le terme constant est $7 - 4\sqrt{3}$), $F_1(X)F_2(X) \notin Q[X]$ (le coefficient de X^3 est $3\sqrt{2}$) et $F_1(X)F_2(-X) \notin Q[X]$ (le coefficient de X^3 est $-\sqrt{6}$).

Comme d'après le 1) de l'annexe 1 (et le fait que $\cos(\frac{\pi}{12}),\cos(\frac{5\pi}{12}),\cos(\frac{7\pi}{12}),\cos(\frac{11\pi}{12})$ ne sont pas rationnels d'après l'annexe 3), le produit de $F_1(X)$ avec deux autres facteurs de $P(X)$ n'est pas dans $Q[X]$, le 2.1) de cette même annexe prouve que $P(X)$ est irréductible sur $Q[X]$:
donc $P(X) = X^8 - 4X^6 + 15X^4 - 4X^2 + 1$ est le polynôme minimal des huit valeurs de $a+b$ ci-dessus et leur degré étant 8, c'est bien un diviseur de 8.

Remarque 1 : l'irréductibilité de P peut se montrer à l'aide du 5) de l'annexe 1.
Toute racine de P a un module $< \sqrt{2}+1 < 2.42 < k - \frac{1}{2}$ pour $k \geq 3$, et comme $P(5) \neq 0$ et $P(6) = 1512289$ est un nombre premier, P est bien irréductible.

Remarque 2 : P étant symétrique c'est que l'inverse de toute racine de P est racine de P. Par exemple, en utilisant $\cos p - \cos q = -2\sin\frac{p+q}{2}\sin\frac{p-q}{2}$ et $\sin p - \sin q = 2\cos\frac{p+q}{2}\sin\frac{p-q}{2}$, on vérifie que $(\sqrt{2} - e^{\frac{i\pi}{12}})(\sqrt{2} + e^{\frac{i5\pi}{12}}) = 1$.

si $a = b^3 + \frac{1}{b^3}$
alors $u = a + b = b^3 + b - b^5 + b = 2b + b^3 - b^5$.
On en déduit (là aussi il suffit de calculer les puissances paires de u jusqu'à u^8)
$u^2 = -2x^6 + 2x^4 + 3x^2 + 2$
$u^4 = -4x^6 + 9x^4 + 20x^2 + 8$ (carré du précédent)
$u^6 = 17x^6 + 60x^4 + 90x^2 + 42$ (produit des deux précédents)
$u^8 = 224x^6 + 465x^4 + 392x^2 + 127$.
Les 3 premières égalités permettent d'obtenir x^2, x^4, x^6 en fonction de u (là j'ai utilisé un logiciel pour inverser la matrice 3×3 du systéme) et en reportant dans la dernière on obtient, au pris de certains calculs
$1001u^8 = 224(-30 \times 13(u^2 - 2) + 13(u^6 - 42))$
$+465(700(u^2 - 2) - 3 \times 77(u^4 - 8) + 28(u^6 - 42))$
$+392(-393(u^2 - 2) + 2 \times 77(u^4 - 8) - 10(u^6 - 42))$
$+127 \times 1001$
et ....
$u^8 = 12u^6 - 47u^4 - 84u^2 + 169$, cad un polynôme de $Q[X]$ annulateur de u est cette fois $P(X) = X^8 - 12X^6 + 47X^4 - 84X^2 + 169$.

Pour montrer l'irréductibilité de P sur Q, on va aussi utiliser l'annexe 1.
En effet les racines de P sont connues, ce sont les huit valeurs possibles de $a+b$ lorsque $a = b^3 + \frac{1}{b^3}$, à savoir (on change les $\sqrt{2}$ des huit valeurs du cas précédent en $-\sqrt{2}$) :
$\pm(\sqrt{2} + v_0), \pm(\sqrt{2} - v_2), \pm(\sqrt{2} + v_3), \pm(\sqrt{2} - v_5)$.
Donc en regroupant les racines conjuguées, la décomposition en facteurs irréductibles dans $R[X]$ de P est
$P(X) = F_1(X)F_1(-X)F_2(X)F_2(-X)$ avec
$F_1(X) = (X - \sqrt{2} - e^{\frac{i\pi}{12}})(X - \sqrt{2} + e^{\frac{i11\pi}{12}}) = X^2 - \frac{\sqrt{2}}{2}(5+\sqrt{3})X + 4 + \sqrt{3}$ (racines $\sqrt{2} + v_0$ et $\sqrt{2} - v_5$)
$F_2(X) = (X - \sqrt{2} + e^{\frac{i5\pi}{12}})(X - \sqrt{2} - e^{\frac{i7\pi}{12}}) = X^2 - \frac{\sqrt{2}}{2}(5-\sqrt{3})X + 4 - \sqrt{3}$ (racines $\sqrt{2} - v_2$ et $\sqrt{2} + v_3$).

On vérifie que $F_1(X)F_1(-X) \notin Q[X]$ (le terme constant est $19+8\sqrt{3}$), $F_1(X)F_2(X) \notin Q[X]$ (le coefficient de X^3 est $-5\sqrt{2}$) et $F_1(X)F_2(-X) \notin Q[X]$ (le coefficient de X^3 est $-\sqrt{6}$).
Comme d'après le 1) de l'annexe 1 (et le fait que $\cos(\frac{\pi}{12}),\cos(\frac{5\pi}{12}),\cos(\frac{7\pi}{12}),\cos(\frac{11\pi}{12})$ ne sont pas rationnels d'après l'annexe 3), le produit de $F_1(X)$ avec deux autres facteurs de $P(X)$ n'est pas dans $Q[X]$, le 2.1) de cette même annexe prouve que $P(X)$ est irréductible sur $Q[X]$:
donc $P(X)=X^8-12X^6+47X^4-84X^2+169$ est le polynôme minimal des huit valeurs de $a+b$ ci-dessus et leur degré étant 8, c'est bien un diviseur de 8.

Remarque 3: voir aussi en annexe 3 une vérification sur ces deux polynômes minimaux obtenus pour $a+b$.

Cas ab

Puisque $a=\pm\sqrt{2}$ et que les les huit valeurs de b sont $\pm v_0,\pm v_2,\pm v_3,\pm v_5$, les seize couples (a,b) ne donnent que huit valeurs distinctes pour ab : $\pm\sqrt{2}\,v_0,\pm\sqrt{2}\,v_2,\pm\sqrt{2}\,v_3,\pm\sqrt{2}\,v_5$, lesquelle vérifient $(ab)^8=16b^8=16(b^4-1)=16(\frac{(ab)^4}{4}-1)$ et donc ces huit valeurs sont racines de X^8-4X^4+16.
Ce polynôme est-il irréductible sur Q?
Comme pour X^8-X^4+1, les racines de X^8-4X^4+16 étant connues on peut le factoriser en irrédutibles de R en associant ses racines conjuguées deux à deux ($\sqrt{2}\,v_k$ et $-\sqrt{2}\,v_{5-k}$ sont conjuguées) :
$\sqrt{2}\,v_0=\sqrt{2}\,e^{i\frac{\pi}{12}}$ et $-\sqrt{2}\,v_5=-\sqrt{2}\,e^{i\frac{11\pi}{12}}=\sqrt{2}\,e^{-i\frac{\pi}{12}}$ sont racines de $X^2-2\sqrt{2}\cos(\frac{\pi}{12})X+2$
et donc $-\sqrt{2}\,v_0$ et $\sqrt{2}\,v_5$ sont racines de $X^2+2\sqrt{2}\cos(\frac{\pi}{12})X+2$
$\sqrt{2}\,v_2=\sqrt{2}\,e^{i\frac{5\pi}{12}}$ et $-\sqrt{2}\,v_3=-\sqrt{2}\,e^{i\frac{7\pi}{12}}=\sqrt{2}\,e^{-i\frac{5\pi}{12}}$ sont racines de $X^2-2\sqrt{2}\cos(\frac{5\pi}{12})X+2$
et donc $-\sqrt{2}\,v_2$ et $\sqrt{2}\,v_3$ sont racines de $X^2+2\sqrt{2}\cos(\frac{5\pi}{12})X+2$,
ce qui donne les quatre facteurs irréductibles dans $R[X]$ de X^8-4X^4+16.
Les formules $\cos p-\cos q=2\sin\frac{p+q}{2}\sin\frac{p-q}{2}$ et $\cos p\cos q=\frac{1}{2}(\cos(p+q)+\cos(p-q))$, permettent de voir que
$(X^2-2\sqrt{2}\cos(\frac{\pi}{12})X+2)(X^2+2\sqrt{2}\cos(\frac{5\pi}{12})X+2)=X^4-2X^3+2X^2-4X+4$, polynôme de $Q[X]$ qui est irréductible (voir 2.2 de l'annexe 1 et le fait que $\cos(\frac{\pi}{12})$ et $\cos(\frac{5\pi}{12})$ ne sont pas rationnels d'après l'annexe 3).
Et donc la décomposition, dans $Q[X]$, en facteurs irréductibles de X^8-4X^4+16 est $(X^4-2X^3+2X^2-4X+4)(X^4+2X^3+2X^2+4X+4)$ et ainsi
$\sqrt{2}\,v_0,-\sqrt{2}\,v_2,\sqrt{2}\,v_3,-\sqrt{2}\,v_5$ ont pour polynôme minimal $X^4-2X^3+2X^2-4X+4$
et $-\sqrt{2}\,v_0,\sqrt{2}\,v_2,-\sqrt{2}\,v_3,\sqrt{2}\,v_5$ ont pour polynôme minimal $X^4+2X^3+2X^2+4X+4$.

Autre façon d'obtenir ces polynômes minimaux : en procédant, comme pour $a+b$, par la méthode des puissances de ab, décomposées dans la base $\{1,b,b^2,b^3,b^4,b^5,b^6,b^7\}$ de $Q(a,b)$.
On a vu plus haut que $a=\pm(b^3+\frac{1}{b^3})$, d'où les deux cas

si $a=b^3+\frac{1}{b^3}$

$u=ab=b^4+b^{-2}=b^4+b^2-b^6$, car $1=b^4-b^8$

$u^2 = 2b^2$

$u^3 = 2ab^3 = 2(b^3 + \frac{1}{b^3})b^3 = 2b^6 + 2$

$u^4 = 4b^4$, et il est inutile de poursuivre le calcul des puissances car on remarque que $u^4 = 4(u - b^2 + b^6) = 4(u - \frac{u^2}{2} + \frac{u^3 - 2}{2})$, soit $u = ab$ racine de $X^4 - 2X^3 + 2X^2 - 4X + 4$,

si $a = -(b^3 + \frac{1}{b^3})$, cela revient à changer b en $-b$ et u en $-u$ par rapport à ce qui précéde et cette fois $u = ab$ est racine de $X^4 + 2X^3 + 2X^2 + 4X + 4$.

Reste évidemment à prouver l'irréductibilité de ces deux polynômes annulateurs (voir ci-dessus).

Cette méthode à l'avantage de donner un polynôme annulateur pour chacun des deux cas alors que précédemment on a d'abord obtenu $X^8 - 4X^4 + 16$ comme seul polynôme annulateur, polynôme qu'il a fallu ensuite décomposer en facteurs irréductibles.

exemple 8

$P_1(X) = X^6 - 4X^3 + 2$ est irréductible d'après Eisenstein (voir 3) de l'annexe 1)

Ses racines sont $r_1, jr_1, j^2r_1, r_2, jr_2, j^2r_2$ avec $r_1 = \sqrt[3]{2 + \sqrt{2}} \simeq 1,505\ldots$ et $r_2 = \sqrt[3]{2 - \sqrt{2}} \simeq 0,836\ldots$ (soit on pose $Y = X^3$, soit on remarque que $X^6 - 4X^3 + 2 = (X^3 - 2)^2 - 2$).

Cas $a + b$.

soit $a = b$ et le polynôme minimal de $a + b$ est évidemment $2^6 P_1(\frac{X}{2})$.

soit $a \neq b$:

soit a et b sont des racines troisièmes de $2 + \sqrt{2}$, auquel cas $a + b$ est une racine troisième de $-(2 + \sqrt{2})$, puisque $1 + j + j^2 = 0$, soit a et b sont des racines troisièmes de $2 - \sqrt{2}$, auquel cas $a + b$ est une racine troisième de $-(2 - \sqrt{2})$: ces six valeurs de $a + b$ sont évidemment racines de $P_1(-X)$ qui est donc leur polynôme minimal.

On notera que dans ce cas $(ab)^3 = (2 + \sqrt{2})^2 = 6 + 4\sqrt{2}$ ou $(2 - \sqrt{2})^2 = 6 - 4\sqrt{2}$.

soit a est une racine troisième de $2 + \sqrt{2}$ et b est une racine troisième de $2 - \sqrt{2}$, ou le contraire, ce qui donne dans les deux cas les mêmes neuf valeurs pour $a + b$: $j^k r_1 + j^{k'} r_2$ avec $j = 0, 1, 2$ et $j' = 0, 1, 2$.

Comme $(a + b)^3 = a^3 + b^3 + 3ab(a + b) = 2 + \sqrt{2} + 2 - \sqrt{2} + 3ab(a + b) = 4 + 3ab(a + b)$, et que $(ab)^3 = (2 + \sqrt{2})(2 - \sqrt{2}) = 2$, on a $((a + b)^3 - 4)^3 = 27 \times 2 \times (a + b)^3$ et ainsi un polynôme annulateur de $a + b$ est $P(X) = X^9 - 12X^6 - 6X^3 - 64$.

Pour toute racine z de P on a $|z| \leq r_1 + r_2 < 2,35 < k - \frac{1}{2}$ pour $k \geq 3$. Comme $P(2) \neq 0$ et $P(3) = 10709$ est un nombre premier, d'après le 5) de l'annexe 1, P est irréductible et c'est le polynôme minimal de ces neuf valeurs de $a + b$.

Cas ab

soit $a = b$ et alors $ab = a^2 \in \{r_1^2; j^2r_1^2; jr_1^2; r_2^2; j^2r_2^2; jr_2^2\}$ et $(ab)^3 = r_1^6 = (2 + \sqrt{2})^2 = 6 + 4\sqrt{2}$ ou $(ab)^3 = r_2^6 = 6 - 4\sqrt{2}$: pour ces six valeurs de ab, $((ab)^3 - 6)^2 = 32$ et ab a pour polynôme annulateur $P(X) = X^6 - 12X^3 + 4$.

Pour toute racine z de P on a $|z| \leq r_1^2 < 1,506^2 < 2,27 < k - \frac{1}{2}$ pour $k \geq 3$. Comme $P(6) \neq 0$ et $P(7) = 113537$ est un nombre premier, d'après le 5) de l'annexe 1, P est irréductible et c'est le polynôme minimal de ces six valeurs de ab.

soit $a \neq b$:

soit a et b sont des racines troisièmes de $2 + \sqrt{2}$, auquel cas $ab = r_1^2$ ou jr_1^2 ou

$j^2 r_1^2$, soit a et b sont des racines troisièmes de $2-\sqrt{2}$, auquel cas $ab = r_2^2$ ou jr_2^2 ou $j^2 r_2^2$ et ces six valeurs de ab sont les six valeurs précédentes

soit a est une racine troisième de $2+\sqrt{2}$ et b est une racine troisième de $2-\sqrt{2}$, ou le contraire, ce qui donne dans les deux cas les mêmes valeurs pour ab : $j^k r_1 j^{k'} r_2 = j^{k+k'}\sqrt[3]{2}$ avec $j = 0,1,2$ et $j' = 0,1,2$ et on obtient que trois valeurs distinctes pour ab : $\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}$.
Le polynôme minimal de ces trois valeurs est évidemment $X^3 - 2$.

7) Cas des deux polynômes $P_1(X) = X^{n_1} + \alpha_0$ et $P_2(X) = X^{n_2} + \beta_0$, irréductibles sur $\mathbb{Q}[X]$

On notera d =pgcd(n_1, n_2), $n_i' = \frac{n_i}{d}$ et $\varpi = (-1)^{n_1'+n_2'} \alpha_0^{n_2'} \beta_0^{n_1'}$.

7.1) Cas ab.

les valeurs prises par ab sont au nombre de $\frac{n_1 n_2}{d}$: ce sont sont les racines $\frac{n_1 n_2}{d}$-ièmes de ϖ (toutes distinctes évidemment, ϖ étant non nul), cad les racines de $X^{\frac{n_1 n_2}{d}} - \varpi \in \mathbb{Q}[X]$ et donc les polynômes minimaux des $\frac{n_1 n_2}{d}$ valeurs prises par ab sont les facteurs irréductibles de $X^{\frac{n_1 n_2}{d}} - \varpi$.

les $\frac{n_1 n_2}{d}$ valeurs prises par ab peuvent s'écrire $\xi a_0 b_0$ où a_0 est une racine de P_1 (cad une racine n_1 -ième de $-\alpha_0$), b_0 est une racine de P_2 (cad une racine n_2-ième de $-\beta_0$)et ξ décrit l'ensemble des racines $\frac{n_1 n_2}{d}$-ièmes de 1

ab prend $n_1 n_2$ valeurs si et seulement si $d = 1$.

$R_2(X) = (-1)^{n_1 n_2}(X^{\frac{n_1 n_2}{d}} - \varpi)^d$; résulte essentiuellemnet du fait que toute valeur prise par ab est atteinte par d couples (a,b).

En particulier, lorsque $n_1 = n_2$, $R_2(X) = (-1)^{n_1^2}(X^{n_1} - \alpha_0\beta_0)^{n_1}$ et les polynômes minimaux des valeurs prises par ab sont les facteurs irréductibles de $X^{n_1} - \alpha_0\beta_0$.

Ces formules correspondent évidemment aux résultats trouvés "directement" pour les exemples 1 et 2 du 5) et les exemples 1 à 5 du 6).

Voici un autre exemple mais avec un aspect général : $n_1 = n_2 = 3$ et α_0, β_0 rationnels quelconques (avec P_1 et P_2 irréductibles, donc α_0 et β_0 ne sont pas des cubes de rationnels)

Lorsque $P_1(X) = X^3 + \alpha_0$, $P_2(X) = X^3 + \beta_0$

si $\alpha_0\beta_0 = \theta^3$ avec $\theta \in \mathbb{Q}$, il y a deux polynômes minimaux pour ab

$X - \theta$ si $ab = \theta$

$X^2 + \theta X + \theta^2$ si $ab \neq \theta$

si $\alpha_0\beta_0$ n'est pas un cube, il y a un polynôme minimal pour tout ab

$X^3 - \alpha_0\beta_0$

Remarque : il est immédiat de vérifier que tout ab est racine de $X^{n_1 n_2} - (-1)^{n_1+n_2}\alpha_0^{n_1}\beta_0^{n_2}$, mais les racines de ce polynôme ne sont pas toutes des valeurs prises par ab : ce polynôme est $(X^{\frac{n_1 n_2}{d}} - \varpi)S(X)$ où $S \in \mathbb{Q}[X]$ et aucun ab n'est racine de S.

7.2) Cas $a + b$.

Ce cas est beaucoup plus difficile que le cas ab (chose déjà constatée sur les exemples du 5) et 6)), essentiellement à cause du fait que l'ensemble des racines n –ièmes de 1 n'est pas un groupe additif (voir annexe 5).
Je n'ai pas trouvé de formule générale pour R_1.

7.2.1) si $n_1 = 2,\ n_2 = 2, R_1(X) = (X^2 + \alpha_0 + \beta_0)^2 - 4\alpha_0\beta_0$

Lorsque $P_1(X) = X^2 + \alpha_0,\ P_2(X) = X^2 + \beta_0,\ \alpha_0 \neq \beta_0$

si $\alpha_0\beta_0 = \theta^2$ avec $\theta \in \mathbb{Q}$, il y a deux polynômes minimaux pour $a + b$

$$X^2 + \alpha_0 + \beta_0 - 2\theta$$

$$X^2 + \alpha_0 + \beta_0 + 2\theta$$

si $\alpha_0\beta_0$ n'est pas un carré, il y a un seul polynôme minimal pour tout $a + b$

$$R_1(X)$$

Lorsque $P_1(X) = X^2 + \alpha_0 = P_2(X)$

il y a deux polynômes minimaux pour $a + b$

$$X$$

$$X^2 + 4\alpha_0$$

7.2.2) si $n_1 = 2,\ n_2 = 4, R_1(X) = (X^4 + 2\alpha_0 X^2 + \alpha_0^2 + \beta_0)^2 - 16\alpha_0\beta_0 X^2$.

Remarque : le cas particulier $\alpha_0 = -2, \beta_0 = 1$ a été étudié à l'exemple 3 du 6).
Pour ces valeurs $\alpha_0 = -2, \beta_0 = 1,$ le R_1 ci-dessus devient
$X^8 - 8X^6 + 26X^4 - 8X^2 + 25 = X^8 - 8X^6 + 25X^4 + X^4 - 8X^2 + 25$ et donc
$R_1(X) = (X^4 + 1)(X^4 - 8X^2 + 5)$ et ainsi P_2 est un facteur de $R_1,$ cad un polynôme minimal de certaines valeurs de $a + b$ est P_2.
En fait, pour cas $n_1 = 2,\ n_2 = 4,\ P_2$ divise R_1 si et seulement si $\alpha_0^2 = 4\beta_0$ (rappel P_1 et P_2 doivent être irréductibles).

7.2.3) si $n_1 = 3,\ n_2 = 3, -R_1(X) = (X^3 + \alpha_0 + \beta_0)^3 - 27\alpha_0\beta_0 X^3$

En notant $u = \sqrt[3]{-\alpha_0}$ (c'est une racine de P_1), $v = \sqrt[3]{-\beta_0}$ (c'est une racine de P_2), donc $(uv)^3 = \alpha_0\beta_0,$ on a les résultats suivants :
(rappel : que ce soit pour $a + b$ ou pour $ab,$ la somme des degrés des polynômes minimaux obtenus est le nombre de valeurs prises par $a + b$ ou ab)

Note : les trois premiers cas correspondent à $(u + v)^3 \in \mathbb{Q},$ les deux derniers à $(u + v)^3 \notin \mathbb{Q},$ car $uv \in \mathbb{Q}$ et $(u + v)^3 \in \mathbb{Q}$ est impossible car sinon $u + v = \dfrac{(u + v)^3 - u^3 - v^3}{3uv} \in \mathbb{Q},$ donc u et v sont racines de $X^2 - (u + v)X + uv \in \mathbb{Q}[X]$ et ils sont algébriques de degré $\leq 2,$ alors qu'ils sont de degré 3 puisqu'ils sont racines de P_1 et P_2.

Lorsque $P_1(X) = X^3 + \alpha_0,\ P_2(X) = X^3 + \beta_0$

si $\alpha_0 = -\beta_0,$ il y a 2 polynômes minimaux pour $a + b$

$$X$$

$$X^6 + 27\alpha_0^2$$

si $\alpha_0 = \beta_0,$ il y a 2 polynômes minimaux pour $a + b$

$$X^3 + 8\alpha_0$$

$$X^3 - \alpha_0$$

si $(u + v)^3 \in \mathbb{Q}$ et $u \neq \pm v$, il y a 2 polynômes minimaux pour $a + b$

$$X^3 - (u + v)^3$$

$$X^6 + (2(\alpha_0 + \beta_0) + 3uv(u + v))X^3 + (u^2 + v^2 - uv)^3$$

si $\alpha_0\beta_0$ est un cube, cad si $uv \in \mathbb{Q},$ il y a 2 polynômes minimaux pour $a + b$

$$X^3 - 3uvX + \alpha_0 + \beta_0$$

$$X^6 + 3uvX^4 + 2(\alpha_0 + \beta_0)X^3 + 9(uv)^2X^2 + 3uv(\alpha_0 + \beta_0)X + (\alpha_0 + \beta_0)^3$$

si $(u + v)^3 \notin \mathbb{Q}$ et $uv \notin \mathbb{Q}$, il y a un seul polynôme minimal pour tout $a + b$

$$X^9 + 3(\alpha_0 + \beta_0)X^6 + 3(\alpha_0^2 + \beta_0^2 - 7\alpha_0\beta_0)X^3 + (\alpha_0 + \beta_0)^3 = -R_1(X)$$

7.2.4) si $n_1 = 4,\ n_2 = 4, R_1(X) = ((X^4 + \alpha_0 + \beta_0)^2 + 4\alpha_0\beta_0)^2 - 16\alpha_0\beta_0(3X^4 - (\alpha_0 + \beta_0))^2$

7.2.5) **On remarque que dans chacun des quatre cas précédents** $\pm R_1(X)$ s'écrit sous la forme $H(X)^2 - \mu\alpha_0\beta_0K(X)^2,\ \mu$ étant une constante indépendante des coefficients α_0 et β_0. Je ne sais si cette remarque est utile, car ce qui importe c'est une forme factorisée dans $\mathbb{Q}[X]$ de R_1 ; cependant c'est une écriture qui semble générale pour R_1.

7.3) **Cas** $a + b$ **avec** $P_1 = P_2 = X^{n_1} + \alpha_0$.

Si on note $r_1, r_2, \ldots, r_{n_1}$ les racines de $P_1 = P_2,$ cad les racines n_1 –ièmes de $-\alpha_0,$ les valeurs prises par a et b sont les r_i.

Le cas $P_1(X) = P_2(X) = X^2 + \alpha_0$ ayant été traité au 7.2.1, **on supposera ici** $n_1 \geq 3$.

7.3.1)

Si n_1 est impair

le nombre de valeurs prises par $a + b$ est $\frac{n_1(n_1 + 1)}{2},$ qui se répartissent en

n_1 valeurs correspondants aux couples (a, b) avec $a = b,$ chacune ayant pour multiplicité 1 dans R_1 et toutes ont pour polynôme minimal $2^{n_1}P_1(\frac{X}{2})$

$\frac{n_1(n_1 - 1)}{2}$ valeurs correspondants aux couples (a, b) avec $a \neq b,$ chacune ayant pour multiplicité 2 dans R_1

$R_1(X) = -2^{n_1}P_1(\frac{X}{2})T^2(X)$ avec $T \in \mathbb{Q}[X]$ **le** polynôme unitaire de degré $\frac{n_1(n_1 - 1)}{2}$ et dont les racines sont les $\frac{n_1(n_1 - 1)}{2}$ valeurs $a + b$ correspondants aux couples (a, b) avec $a \neq b$; les facteurs irréductibles de T donneront les polynômes minimaux des valeurs $a + b$ pour $a \neq b$

Si n_1 est pair

le nombre de valeurs prises par $a+b$ est $\frac{n_1^2+2}{2}$, qui se répartissent en

n_1 valeurs correspondants aux couples (a,b) avec $a=b$, chacune ayant pour multiplicité 1 dans R_1 et toutes ont pour polynôme minimal $2^{n_1}P_1(\frac{X}{2})$

la valeur 0 correspondant aux n_1 couples $(a,-a)$, de multiplicité n_1 dans R_1, cette valeur 0 de $a+b$ ayant évidemment comme polynôme minimal X

$\frac{n_1(n_1-2)}{2}(\neq 0$ car $n_1 \geq 3)$ valeurs correspondants aux couples (a,b) avec $a \neq \pm b$, chacune ayant pour multiplicité 2 dans R_1

$R_1(X)=X^{n_1}(2^{n_1}P_1(\frac{X}{2}))T^2(X)$ avec $T \in \mathbb{Q}[X]$ **le** polynôme unitaire de degré $\frac{n_1(n_1-2)}{2}$ et dont les racines sont les $\frac{n_1(n_1-2)}{2}$ valeurs $a+b$ correspondants aux couples (a,b) avec $a \neq b$; les facteurs irréductibles de T donneront les polynômes minimaux des valeurs $a+b$ pour $a \neq \pm b$.

Evidemment, que ce soit dans le cas n_1 impair (resp pair), un polynôme unitaire, de degré $\frac{n_1(n_1-1)}{2}$ (resp $\frac{n_1(n_1-2)}{2}$) et annulateur des $\frac{n_1(n_1-1)}{2}$ (resp $\frac{n_1(n_1-2)}{2}$) valeurs correspondants aux couples (a,b) avec $a \neq \pm b$ est obligatoirement T.
On précisera au 7.3.2) une méthode pour justement trouver T sans passer par le déterminant de Sylvester : on montrera alors que T est aussi (comme les autres facteurs de R_1 déjà trouvés) un polynôme en X^{n_1} **et donc pour** $n_1 \geq 2$, R_1 **est un polynôme en** X^{n_1} (pour $n_1=2$, voir 7.2.1)).

.

7.3.2)

Voici une méthode pour trouver le polynôme T défini au 7.3.1) en cherchant un polynôme annulateur de $1+\tau$ où τ est une racine n_1 –ième de 1.

Il s'agit de trouver un polynôme annulateur des $a+b$ avec $a \neq \pm b$.
$a+b=b(1+\tau)$ avec $\tau=\frac{a}{b}$ qui est une racine n_1 –ième de 1 (puisque $a^{n_1}=b^{n_1}=-\alpha_0$).

On va appliquer la méthode du 2.4) mais en l'adaptant au cas ci-dessus en remarquant que $(1+\tau)^{kn_1}$ s'écrit forme de $\mathbb{Q}$ –combinaison linéaire de 1 et des $\tau^j+\tau^{n_1-j}$ (pour $1 \leq j < \frac{n_1}{2}$), cela pour $k=1,2,\ldots,N$ (N sera précisé plus loin), ce qui permettra de trouver un polynôme unitaire $R \in \mathbb{Q}[X]$, de degré Nn_1, en X^{n_1}, et annulateur de $1+\tau$.
Ainsi $R(\frac{a+b}{b})=R(1+\tau)=0$ et puisque $(\frac{X}{b})^{kn_1}=\frac{X^{kn_1}}{(-\alpha_0)^k}$, le polynôme $(-\alpha_0)^N R(\frac{X}{b})$ est dans $\mathbb{Q}[X]$, unitaire et annulateur de tous les $a+b$ avec $a \neq \pm b$.

Bien entendu $1+\tau \in \mathbb{Q}[\xi]$ où ξ est une racine n_1 –ième de 1 primitive et donc $1+\tau$ est algébrique de degré un diviseur de $\varphi(n_1)=[\mathbb{Q}(\xi);\mathbb{Q}]$.
Par exemple si $n_1=5$, $\varphi(n_1)=4$ et donc le degré du polynôme minimal de $1+\tau$ est 2 ou 4 (car $\tau \neq \pm 1$) ; en fait, cf le 3.1, ce polynôme minimal est
$\phi_5(X-1)=X^4-3X^3+4X^2-2X+1$.
Or la méthode ci-dessus va donner un polynôme annulateur de $1+\tau$ qui sera au moins de degré 5 (puisque c'est un polynôme en X^5) : c'est $X^{10}+11X^5-1$!
En fait le but ici n'est pas de trouver un polynôme annulateur de $1+\tau$, mais un polynôme annulateur de $1+\tau$ qui permette d'en déduire un polynôme annulateur de

$a+b$.
Et $X^{10}+11X^5-1$ donne $X^{10}-11\alpha_0 X^5-\alpha_0^2$ comme polynôme annulateur de tous les $a+b$ ($a \neq \pm -b$) ; il est irréductible pour $\alpha_0 = -4$.
Note : le lecteur peut vérifier que $X^{10}+11X^5-1$ est effectivement un multiple de $\phi_5(X-1)$.

si n_1 impair

$$(1+\tau)^{kn_1} = \lambda_{k,0}+\lambda_{k,1}(\tau+\tau^{n_1-1})+\ldots+\lambda_{k,\frac{n_1-1}{2}}(\tau^{\frac{n_1-1}{2}}+\tau^{\frac{n_1+1}{2}})$$

Il y a $N=\frac{n_1-1}{2}$ termes de la forme $\tau^j+\tau^{n_1-j}$.

si n_1 pair, $(1+\tau)^{kn_1} = \lambda_{k,0}+\lambda_{k,1}(\tau+\tau^{n_1-1})+\ldots+\lambda_{k,\frac{n_1}{2}-1}(\tau^{\frac{n_1}{2}-1}+\tau^{\frac{n_1}{2}+1})$; $\tau^{\frac{n_1}{2}}$ n'apparaît pas, car il est incorporé dans $\lambda_{k,0}$ puisque $\tau^{\frac{n_1}{2}} = \pm 1$ (son carré est 1).
Il y a $N=\frac{n_1}{2}-1$ termes de la forme $\tau^j+\tau^{n_1-j}$.

En fait pour $n_1=4$, $\tau=\pm i$ (puisque $\tau \neq \pm 1$) et donc $\tau^{\frac{n_1}{2}} = \tau^2 = -1$, mais si $n_1 \geq 6$, alors $\tau^{\frac{n_1}{2}} = (\frac{a}{b})^{\frac{n_1}{2}}$ pourra prendre soit la valeur -1, soit la valeur 1 : il y aura deux valeurs possibles pour $\lambda_{k,0}$, donc on va alors trouver deux polynômes annulateurs pour $1+\tau$, l'un, R_1, pour les valeurs de τ telles que $\tau^{\frac{n_1}{2}} = 1$, l'autre R_2, pour les valeurs de τ telles que $\tau^{\frac{n_1}{2}} = -1$.

On remarquera que 1 et les $\tau^j+\tau^{n_1-j}$ ne sont pas Q –linéairement indépendant car $1+\tau+\tau^2+\ldots+\tau^{n_1-1} = 0$ (puisque $\tau \neq 1$), d'où

si n_1 est impair $1+(\tau+\tau^{n_1-1})+\ldots+(\tau^{\frac{n_1-1}{2}}+\tau^{\frac{n_1+1}{2}}) = 0$

si n_1 est pair $\tau^{\frac{n_1}{2}} \times 1+(\tau+\tau^{n_1-1})+\ldots+(\tau^{\frac{n_1}{2}-1}+\tau^{\frac{n_1}{2}+1}) = 0.$; en outre dans ce cas on a $\tau+\tau^{n_1-1}$ et $\tau^{\frac{n_1}{2}-1}+\tau^{\frac{n_1}{2}+1}$ qui sont égaux si $\tau^{\frac{n_1}{2}} = 1$, et opposés si $\tau^{\frac{n_1}{2}} = -1$. En outre si τ peut prendre la valeur $\pm i$ ($\Leftrightarrow n_1 = 4p$), alors $\tau = -\tau^{-1}$ et $\tau+\tau^{n_1-1} = \tau^{\frac{n_1}{2}-1}+\tau^{\frac{n_1}{2}+1} = 0$.
Mais, vu le but cherché, cela n'est pas gênant, au contraire dans cd cas n_1 pair, cela pourra alléger les calculs.

Passons à la détermination effective d'un polynôme annulateur R de $1+\tau$.
On obtient R (ou R_1 et R_2) en cherchant les **rationnels** $\mu_1, \mu_2, \ldots, \mu_{N-1}$ tels que dans l'expression $\sum_{k=1}^{N-1}\mu_k(1+\tau)^{kn_1}+(1+\tau)^{Nn_1}$ les coefficients des $\tau^j+\tau^{n_1-j}$ soient égaux : cela fait $N-1$ inconnues et $N-1$ équations (lorsque n_1 est pair, il y a un seul systéme à résoudre, car seul le terme constant $\lambda_{k,0}$ change lorsque $\tau^{\frac{n_1}{2}}$ passe de 1 à -1).
Dans tous les exemples faits, il n'y a pas de problème de résolution....
Les coefficients des $\tau^j+\tau^{n_1-j}$ étant égauxdans $\sum_{k=1}^{N-1}\mu_k(1+\tau)^{kn_1}+(1+\tau)^{Nn_1}$, c'est que, puisque $1+\tau+\tau^2+\ldots+\tau^{n_1-1} = 0$, $\sum_{k=1}^{N-1}\mu_k(1+\tau)^{kn_1}+(1+\tau)^{Nn_1} \in \mathbb{Q}$, ce qui donne un polynôme R unitaire, dans $\mathbb{Q}[X]$, annulateur de $1+\tau$

Dans le cas n_1 impair, on obtient un seul polynôme annulateur (unitaire et dans $\mathbb{Q}[X]$) de tous les $a+b$ avec $a \neq \pm b$: $(-\alpha_0)^N R(\frac{X}{b})$. Si ce polynôme a pour degré $\frac{n_1(n_1-1)}{2}$, c'est le polynôme T défini au 7.3.1.

Dans le cas n_1 pair, on obtient deux polynômes annulateurs R_1 et R_2 de $1+\tau$, qui vont donner deux polynômes annulateurs de tous les $a+b$ avec $a \neq \pm b$:
$T_1(X) = (-\alpha_0)^N R_1(\frac{X}{b})$ pour $(\frac{a}{b})^{\frac{n_1}{2}} = (\tau)^{\frac{n_1}{2}} = 1$ et $T_2(X) = (-\alpha_0)^N R_2(\frac{X}{b})$ pour $(\frac{a}{b})^{\frac{n_1}{2}} = (\tau)^{\frac{n_1}{2}} = -1$.
Mais ces deux polynômes n'ont aucune racine commune de type $a+b$ avec $a \neq \pm b$ car d'après le 4) de l'annexe 5), $a+b = a'+b' \neq 0$ implique $\{a;b\} = \{a';b'\}$, donc $(\frac{a}{b})^{\frac{n_1}{2}}$ serait égal à $(\frac{a'}{b'})^{\frac{n_1}{2}}$ ce qui est exclu.
D'où si la somme des degrés de T_1 et T_2 est $\frac{n_1(n_1-2)}{2}$, alors nécessairement T_1T_2 est le polynôme T défini au 7.3.1).
Note : T_1 et T_2 ne sont pas forcément du même degré : voir exemple ci-dessous $n_1 = 8$.

On notera que puisque T est un polynôme en X^{n_1}, alors R_1 est aussi un polynôme en X^{n_1}.

Une dernière remarque : dans le cas n_1 pair, pour les exemple traités ci-dessous ($n_1 \leq 8$), il y a toujours des simplifications sur les $\tau^j + \tau^{n_1-j}$, simplifications qui permettent de conclure sans avoir à résoudre le moindre systéme!
A noter aussi, que si n_1 est un multiple de 4, $\pm i$ est une valeur possible de τ ($(\pm i)^{4p} = 1$) et $X^{n_1} + (-1)^{\frac{n_1}{4}} 2^{\frac{n_1}{2}} \alpha_0$ est un polynôme annulateur des $a+b$ avec $\frac{a}{b} = \pm i$ (il suffit de simplifier $(a+b)^{n_1}$).

Applications :

$n_1 = 3 : R_1(X) = -(X^3 + 8\alpha_0)(X^3 - \alpha_0)^2$: on retrouve le résultat donné au 7.2.3) mais cette forme factorisée de R_1 n'est pas si facile que cela à obtenir à partir du cas général. Rappelons qu'au 7.2.3) les deux polyômes minimaux pour $a+b$ sont donnés (voir le cas $\alpha_0 = \beta_0$).

$n_1 = 4 : R_1(X) = X^4(X^4 + 16\alpha_0)(X^4 - 4\alpha_0)^2$: cette forme factorisée de R_1 n'est pas si facile que cela à obtenir à partir du cas général vu au 7.2.4).

$n_1 = 5 : R_1(X) = -(X^5 + 32\alpha_0)(X^{10} - 11\alpha_0 X^5 - \alpha_0^2)^2$: le cas particulier $\alpha_0 = -4$ a été vu à l'exemple 4 du 6).

$n_1 = 6 : R_1(X) = X^6(X^6 + 64\alpha_0)(X^6 + \alpha_0)^2(X^6 - 27\alpha_0)^2$: on remarquera que P_1^2 divise R_1.

$n_1 = 7 : R_1(X) = -(X^7 + 128\alpha_0)(X^{21} - 57\alpha_0 X^{14} - 289\alpha_0^2 X^7 + \alpha_0^3)^2$:
$X^{21} - 57\alpha_0 X^{14} - 289\alpha_0^2 X^7 + \alpha_0^3$ est irréductible pour $\alpha_0 = 2$ (via site decode)

$n_1 = 8 : R_1(X) = X^8(X^8 + 256\alpha_0)(X^8 + 16\alpha_0)^2(X^{16} + 136\alpha_0 X^8 - 1848\alpha_0)^2$:
$X^{16} + 136\alpha_0 X^8 - 1848\alpha_0$ est irréductible pour $\alpha_0 = 3$ (via site decode)

preuves :

preuve 7.1)

Prouvons que les valeurs prises par ab sont les racines $\frac{n_1 n_2}{d}$ -ièmes de ϖ.

$(ab)^{\frac{n_1 n_2}{d}} = (a^{n_1})^{\frac{n_2}{d}} (b^{n_2})^{\frac{n_1}{d}} = \varpi$.

Réciproquement, soit r une racine $\frac{n_1 n_2}{d}$ -ième de ϖ : $r = e^{\frac{2ikd\pi}{n_1 n_2}} a_0 b_0$ où a_0 est une valeur prise par a et b_0 une valeur prise par b.

n_1' et n_2' étant premiers entre eux, il existe deux entiers u et v tels que $un_1' + vn_2' = 1$, soit $un_1 + vn_2 = d$ et ainsi

$r = e^{2ik(\frac{u}{n_2} + \frac{v}{n_1})\pi} a_0 b_0 = e^{\frac{2iv\pi}{n_1}} a_0 e^{\frac{2iu\pi}{n_2}} b_0$ qui est une valeur prise par ab, car $e^{\frac{2iv\pi}{n_1}} a_0$ est une racine de P_1 et $e^{\frac{2iu\pi}{n_2}} b_0$ est une racine de P_2.

Prouvons que $R_2(X) = (-1)^{n_1 n_2}(X^{\frac{n_1 n_2}{d}} - \varpi)^d$.

Notons $r_1, r_2, \ldots, r_{\frac{n_1 n_2}{d}}$ les racines de $\widehat{R_2}(X) = X^{\frac{n_1 n_2}{d}} - \varpi$.

Ces racines étant toutes les valeurs prises par ab, cf le 4.1.2

$R_2(X) = (-1)^{n_1 n_2} \prod_{k=1,2,\ldots,\frac{n_1 n_2}{d}} (X - r_k)^{m_k}$ où m_k est le nombre de couples (a,b) tels que $ab = r_k$.

Or $a = a_0\xi$ avec ξ une racine n_1 –ième de 1 et a_0 une racine n_1 –ième de $-\alpha_0$ (cad une valeur possible pour a) et $b = b_0\eta$ avec η une racine n_2 –ième de 1 et b_0 une racine n_2 –ième de $-\beta_0$; donc $ab = r_k \Leftrightarrow \xi\eta = e^{\frac{2ikd\pi}{n_1 n_2}}$, et d'après l'annexe 5, il y a exactement d couples (ξ,η) possibles donc, pour tout k, $m_k = d$ et ainsi

$R_2(X) = (-1)^{n_1 n_2} \prod_{k=1,2,\ldots,\frac{n_1 n_2}{d}} (X - r_k)^d = (-1)^{n_1 n_2} \widehat{R_2}(X)^d$.

L'exemple $P_1(X) = X^3 + \alpha_0$, $P_2(X) = X^3 + \beta_0$ est laissé au lecteur.

Preuve de la remarque :

$\widetilde{R}_2(X) = X^{n_1 n_2} - (-1)^{n_1+n_2}\alpha_0^{n_1}\beta_0^{n_2} = (X^{\frac{n_1 n_2}{d}})^d - (\varpi)^d$.

Donc les racines de $\widetilde{R}_2$ sont les racines de $X^{\frac{n_1 n_2}{d}} - \delta\varpi$ où δ est une racine d –ième quelconque de 1 :

si $\delta = 1$ on obtient les racines de R_2 (rappel : les racines de R_2 sont uniquement toutes les valeurs prises par ab)

si $\delta \neq 1$ on obtient d'autres racines que celles de R_2.

Quant à la factorisation annoncée de $\widetilde{R}_2$ dans $\mathbb{Q}[X]$, elle vient du fait que dans tout anneau commutatif $A^n - B^n = (A-B)(A^{n-1}B + A^{n-2}B^2 + \ldots + AB^{n-2} + B^{n-1})$. □

preuve 7.2)

preuve 7.2.1 $P_1(X) = X^2 + \alpha_0$, $P_2(X) = X^2 + \beta_0$.

$R_1(X) = (X^2 + \alpha_0 + \beta_0)^2 - 4\alpha_0\beta_0$ se détermine facilement à l'aide du déterminant 4×4 de Sylvester ; cependant un polynôme annulateur de tout $a + b$ se trouve sans déterminant en remarquant que $(a+b)^2 + \alpha_0 + \beta_0 = 2ab$, relation qui élevée au carré donne $((a+b)^2 + \alpha_0 + \beta_0)^2 = 4\alpha_0\beta_0$ et on retrouve R_1 comme polynôme annulateur.

Cas $\alpha_0 \neq \beta_0$

si $\alpha_0\beta_0 = \theta^2$ avec $\theta \in \mathbb{Q}$, $R_1(X) = (X^2 + \alpha_0 + \beta_0 + 2\theta)(X^2 + \alpha_0 + \beta_0 - 2\theta)$ est réductible dans $\mathbb{Q}[X]$.

$X^2 + \alpha_0 + \beta_0 + 2\theta$ sera réductible dans $\mathbb{Q} \Leftrightarrow -(\alpha_0 + \beta_0 + 2\theta)$ est un carré dans $\mathbb{Q}$; or $-(\alpha_0 + \beta_0 + 2\theta) = -(\alpha_0 + \frac{\theta^2}{\alpha_0} + 2\theta) = -\frac{(\alpha_0 + \theta)^2}{\alpha_0}$ qui n'est pas un carré, puisque $-\alpha_0$ n'est pas un carré et $\alpha_0 + \theta \neq 0$ (sinon, $\alpha_0\beta_0 = \theta^2$ implique $\alpha_0 = \beta_0$ ce qui est exclu ici).

Donc $X^2 + \alpha_0 + \beta_0 + 2\theta$ est irréductible sur $\mathbb{Q}$, de même pour $X^2 + \alpha_0 + \beta_0 - 2\theta$: ces deux polynômes sont donc les polynômes minimaux cherchés.

si $\alpha_0\beta_0 = \theta^2$ avec $\theta \notin \mathbb{Q}$, alors R_1 n'a pas de racine dans $\mathbb{Q}$ et si R_1 est réductible dans $\mathbb{Q}[X]$ ce sera sous la forme $(X^2 + uX + v)(X^2 + u'X + v')$.

R_1 étant pair $u + u' = 0$ et $uv' + u'v = 0$.

Si $u = -u' = 0$, alors $R_1(X) = X^4 + 2(\alpha_0 + \beta_0)X^2 + (\alpha_0 - \beta_0)^2 = (X^2 + v)(X^2 + v')$ et $v + v' = 2(\alpha_0 + \beta_0)$ et $vv' = (\alpha_0 - \beta_0)^2$.

Donc v et v' sont racines de $X^2 - 2(\alpha_0 + \beta_0)X + (\alpha_0 - \beta_0)^2$ dont le discriminant est $16\alpha_0\beta_0$ qui n'est pas un carré, donc on ne peut avoir $u = -u' \neq 0$.

Puisque $u = -u' \neq 0$, on a $v = v'$ et $R_1(X) = (X^2 + uX + v)(X^2 - uX + v)$.

Ainsi $2v - u^2 = 2(\alpha_0 + \beta_0)$ et $v^2 = (\alpha_0 - \beta_0)^2$, donc

soit $v = \alpha_0 - \beta_0$ et $u^2 = -4\beta_0$, ce qui est impossible car P_2 est irréductible, donc $-\beta_0$ n'est pas un carré

soit $v = -\alpha_0 + \beta_0$ et $u^2 = -4\alpha_0$, ce qui est impossible car P_1 est irréductible, donc $-\alpha_0$ n'est pas un carré.

Finalement R_1 est irréductible sur $\mathbb{Q}$, donc c'est le polynôme minimal de tout $a + b$.

Cas $\alpha_0 = \beta_0$

Dans ce cas $R_1(X) = (X^2 + 2\alpha_0)^2 - 4\alpha_0^2 = X^2(X^2 + 4\alpha_0)$ et les deux polynômes minimaux pour $a + b$ sont X (lorsque $a = -b$) et $X^2 + 4\alpha_0$ qui est bien irréductible car $-\alpha_0$ n'est pas un carré, donc $--4\alpha_0$ aussi ($X^2 + 4\alpha_0$ est le polynôme minimal des deux valeurs de $a + b$ lorsque $a = b$). □

preuve 7.2.2 $P_1(X) = X^2 + \alpha_0$, $P_2(X) = X^4 + \beta_0$.

J'ai trouvé $R_1(X) = X^8 + 4\alpha_0X^6 + (6\alpha_0^2 + 2\beta_0)X^4 + (4\alpha_0^3 - 12\alpha_0\beta_0)X^2 + (\alpha_0^2 + \beta_0)^2$ via le déterminant de Sylvester et un logiciel.

On peut trouver la forme $(X^4 + 2\alpha_0X^2 + \alpha_0^2 + \beta_0)^2 - 16\alpha_0\beta_0X^2$ en recherchant directement un polynôme annulateur.

$(a + b)^2 = -\alpha_0 + 2ab + b^2$.

$(a + b)^4 = \alpha_0^2 - \beta_0 + 4ab(a^2 + b^2) + 6a^2b^2 = \alpha_0^2 - \beta_0 + 2((a + b)^2 + \alpha_0 - b^2)(-\alpha_0 + b^2) - 6\alpha_0b^2$

$(a + b)^4 = \alpha_0^2 - \beta_0 - 2\alpha_0(a + b)^2 - 2\alpha_0^2 + 2\alpha_0b^2 + 2b^2(a + b)^2 + 2\alpha_0b^2 + 2\beta_0 - 6\alpha_0b^2$

$(a + b)^4 + 2\alpha_0(a + b)^2 + \alpha_0^2 - \beta_0 = 2b^2(-\alpha_0 + (a + b)^2)$

En élevant au carré et en faisant passer tout à droite, on voit que $a + b$ est racine de

$U(X) = (X^4 + 2\alpha_0X^2 + \alpha_0^2 - \beta_0)^2 + 4\beta_0(-\alpha_0 + X^2)^2$

$U(X) =$

$X^8 + 4\alpha_0^2X^4 + (\alpha_0^2 - \beta_0)^2 + 4\alpha_0X^6 + 2(\alpha_0^2 - \beta_0)X^4 + 4\alpha_0(\alpha_0^2 - \beta_0)X^2 + 4\alpha_0^2\beta_0 + 4\beta_0X^4 - 8\alpha_0\beta_0X^2$

On remarque alors que

$(\alpha_0^2 - \beta_0)^2 + 4\alpha_0^2\beta_0 = (\alpha_0^2 + \beta_0)^2$, $2(\alpha_0^2 - \beta_0)X^4 + 4\beta_0X^4 = 2(\alpha_0^2 + \beta_0)X^4$

et $4\alpha_0(\alpha_0^2 - \beta_0)X^2 - 8\alpha_0\beta_0X^2 = 4\alpha_0(\alpha_0^2 + \beta_0)X^2 - 16\alpha_0\beta_0X^2$, ce qui donne

$U(X) = (X^4 + 2\alpha_0X^2 + \alpha_0^2 + \beta_0)^2 - 16\alpha_0\beta_0X^2$ qui redonne bien R_1 en développant le carré.

Preuve de la remarque : puisque $R_1(X) = (P_2(X) + 2\alpha_0X^2 + \alpha_0^2)^2 - 16\alpha_0\beta_0X^2$, P_2 divise R_1

équivaut à $P_2(X)$ divise $(2\alpha_0X^2+\alpha_0^2)^2-16\alpha_0\beta_0X^2=4\alpha_0^2X^4+(4\alpha_0^3-16\alpha_0\beta_0)X^2+\alpha_0^4$.
Donc il est nécessaire que $4\alpha_0^3-16\alpha_0\beta_0=0$, soit $\alpha_0^2=4\beta_0$ (puisque $\alpha_0\neq 0$).
Réciproquement, $P_2=X^4+\beta_0$ divise effectivement
$4\alpha_0^2X^4+(4\alpha_0^3-16\alpha_0\beta_0)X^2+\alpha_0^4=16\beta_0(X^4+\beta_0)$. □

preuve 7.2.3 $P_1(X)=X^3+\alpha_0,\ P_2(X)=X^3+\beta_0$.
Là aussi, comme pour le cas $n_1=n_2=2$, un polynôme annulateur est facile à trouver car $(a+b)^3+\alpha_0+\beta_0=3ab(a+b)$ et en élevant à la puissance 3, on retrouve
$-R_1=(X^3+\alpha_0+\beta_0)^2-27\alpha_0\beta_0X^3$ comme polynôme annulateur.
Ensuite ...travail laissé au lecteur... □.

preuve 7.2.4 $P_1(X)=X^4+\alpha_0,\ P_2(X)=X^4+\beta_0$.
Par le déterminant de Sylvester, à l'aide un logiciel, j'ai obtenu
$R_1(X)=X^{16}+4(\alpha_0+\beta_0)X^{12}+(6\alpha_0^2-124\alpha_0\beta_0+6\beta_0^2)X^8+(4\alpha_0^3+124\alpha_0^2\beta_0+124\alpha_0\beta_0^2+4\beta_0^3)X$
Il n'est pas facile d'en trouver une écriture de la forme $H(X)^2-\mu\alpha_0\beta_0K(X)^2$ comme celles obtenues pour les trois cas précédents, mais on la trouve aussi en cherchant directement un polynôme annulateur :
$(a+b)^4+\alpha_0+\beta_0=4ab(a^2+b^2)+6a^2b^2=2ab(2(a+b)^2-ab)$
$\frac{(a+b)^4+\alpha_0+\beta_0}{2ab}+ab=2(a+b)^2$, égalité que l'on élève au carré,
$\frac{((a+b)^4+\alpha_0+\beta_0)^2}{4a^2b^2}+a^2b^2+(a+b)^4+\alpha_0+\beta_0=4(a+b)^4$
$\frac{1}{a^2b^2}(\frac{((a+b)^4+\alpha_0+\beta_0)^2}{4}+\alpha_0\beta_0)=3(a+b)^3-\alpha_0-\beta_0$, et enfin
$\frac{1}{\alpha_0\beta_0}(\frac{((a+b)^4+\alpha_0+\beta_0)^4}{16}+\alpha_0^2\beta_0^2+\frac{\alpha_0\beta_0((a+b)^4+\alpha_0+\beta_0)^2}{2})=(3(a+b)^3-\alpha_0-\beta_0)^2$
et on obtient comme polynôme annulateur
$(X^4+\alpha_0+\beta_0)^4+16\alpha_0^2\beta_0^2+8\alpha_0\beta_0(X^4+\alpha_0+\beta_0)^2-16\alpha_0\beta_0(3X^4-(\alpha_0+\beta_0))^2$
ou $((X^4+\alpha_0+\beta_0)^2+4\alpha_0\beta_0)^2-16\alpha_0\beta_0(3X^4-(\alpha_0+\beta_0))^2=R_1(X)$,
puisque dans le membre de gauche
le coeffcient de X^{16} est 1
le coefficient de X^{12} est $4(\alpha_0+\beta_0)$
le coefficient de X^8 est $6(\alpha_0+\beta_0)^2+8\alpha_0\beta_0-16\times 9\times\alpha_0\beta_0=6\alpha_0^2-124\alpha_0\beta_0+6\beta_0^2$
le coefficient de X^4 est
$4(\alpha_0+\beta_0)^3+16\alpha_0\beta_0(\alpha_0+\beta_0)+16\times 6\alpha_0\beta_0(\alpha_0+\beta_0)=4\alpha_0^3+124\alpha_0^2\beta_0+124\alpha_0\beta_0^2+4\beta_0^3$
le terme constant est
$(\alpha_0+\beta_0)^4+16\alpha_0^2\beta_0^2+8\alpha_0\beta_0(\alpha_0+\beta_0)^2-16\alpha_0\beta_0(\alpha_0+\beta_0)^2=((\alpha_0+\beta_0)^2-4\alpha_0\beta_0)^2=(\alpha_0-\beta$

preuve 7.3.1)
Cas n_1 impair.
Pour un couple (a,b) avec a et b racines de $P_1=P_2$ (rappel on note $r_1,r_2,\ldots,r_{n_1}$ les racines de P_1)
soit $a=b$ et $(a,a)=(r_i,r_i)$ pour $i=1,2,\ldots,n_1$, donc n_1 valeurs possibles $2r_1,2r_2,\ldots,2r_{n_1}$ qui ont évidemment $2^{n_1}P_1(\frac{X}{2})$ comme polynôme minimal ; chacune de ces valeurs $2r_i$ est atteinte une seule fois par le couple (r_i,r_i), cela d'après le 4) de l'annexe 5, et donc sa multiplicité dans R_1 est 1 (voir 4.1.1))
soit $a\neq b$, ce qui donne $n_1(n_1-1)$ couples (a,b) possibles et cf le 4) de l'annexe 5, on obtient $\frac{n_1(n_1-1)}{2}$ valeurs distinctes pour $a+b$ atteintes chacune deux fois.

L'égalité $R_1(X) = 2^{n_1}P_1(\frac{X}{2})T^2(X)$ résulte du 4.1.1).

Cas n_1 pair.

En notant $n_1 = 2p,$ on supposera que les racines de P_1 sont $r_1, r_2, \ldots, r_p$ et $-r_1, -r_2, \ldots, -r_p$

Pour un couple (a,b) avec a et b racines de $P_1 = P_2$

soit $a = b$ et $(a,a) = (r_i, r_i)$ pour $i = 1, 2, \ldots, n_1,$ donc n_1 valeurs possibles $2r_1, 2r_2, \ldots, 2r_p$ et $-2r_1, -2r_2, \ldots, -2r_p$ pour $a+b,$ valeurs qui ont évidemment $2^{n_1}P_1(\frac{X}{2})$ comme polynôme minimal ; chacune de ces valeurs r_i est atteinte une seule fois par le couple $(r_i, r_i),$ cela d'après le 4) de l'annexe 5, et donc sa multiplicité dans R_1 est 1 (voir 4.1.1))

soit $a = -b$ et $(a,a) = (r_i, -r_i)$ pour $i = 1, 2, \ldots, p$ ou $(-r_i, r_i)$ pour $i = 1, 2, \ldots, p,$ donc une seule valeur possible pour $a+b$ qui est $0,$ atteinte exactement par les n_1 couples $(r_i, -r_i)$ et $(-r_i, r_i),$ cela cela d'après le 4) de l'annexe 5, et donc sa multiplicité dans R_1 est n_1 (voir 4.1.1))

soit $a \neq \pm b$, ce qui donne $n_1(n_1-2)$ couples (a,b) possibles (a étant choisi, b doit être différent de a et $-a$) et cf le 4) de l'annexe 5, on obtient $\frac{n_1(n_1-2)}{2}$ valeurs distinctes pour $a+b$ atteintes chacune deux fois.

L'égalité $R_1(X) = X^{n_1}(2^{n_1}P_1(\frac{X}{2}))T^2(X)$ résulte du 4.1.1). □

preuve 7.3.2)

Cas $n_1 = 3$

$R_1(X) = -2^3P_1(\frac{X}{2})T^2 = -(X^3 + 8\alpha_0)T^2.$

τ étant $\frac{a}{b} \neq \pm 1,$ et $\tau^3 = 1,$

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

Comme $\tau = j$ ou $j^2,$ $\tau + \tau^2 = -1$ et $1+\tau$ est racine de $X^3 - 1,$ donc un polynôme annulateur de tout $a+b,$ avec $a \neq \pm b,$ est $(-\alpha_0)((\frac{X}{b})^3 - 1) = X^3 - \alpha_0.$

Comme le degré de ce polynôme unitaire est $3 = \frac{n_1(n_1-1)}{2},$ c'est $T,$ donc

$R_1(X) = -(X^3 + 8\alpha_0)(X^3 - \alpha_0)^2.$ □

Cas $n_1 = 4$

$R_1(X) = X^4(2^4P_1(\frac{X}{2}))T^2 = X^4(X^4 + 16\alpha_0)T^2.$

τ étant $\frac{a}{b} \neq \pm 1,$ et $\tau^4 = 1,$

$(1+\tau)^4 = 2 + 6\tau^2 + 4\tau(1+\tau^2).$

Comme $\tau^2 = \pm 1$ et $\tau \neq \pm 1,$ c'est que $\tau = \pm i,$ donc $\tau^2 = -1$ et ainsi $(1+\tau)^4 = -4$ et $1+\tau$ est racine de $X^4 + 4.$

Donc $(-\alpha_0)((\frac{X}{b})^4 + 4) = X^4 - 4\alpha_0$ est annulateur de tout $a+b$ avec $a \neq \pm b$ et comme il est de degré $4 = \frac{n_1(n_1-2)}{2},$ c'est T et $R_1(X) = X^4(X^4 + 16\alpha_0)(X^4 - 4\alpha_0)^2.$ □

Cas $n_1 = 5$

$R_1(X) = -2^5P_1(\frac{X}{2})T^2 = -(X^5 + 32\alpha_0)T^2.$

τ étant $\frac{a}{b} \neq \pm 1,$ et $\tau^5 = 1,$

$(1+\tau)^5 = 2 + 5(\tau + \tau^4) + 10(\tau^2 + \tau^3)$

$(1+\tau)^{10} = 254 + 220(\tau+\tau^4) + 165(\tau^2+\tau^3)$
$(1+\tau)^{10} + \mu_1(1+\tau)^5 = 254 + 2\mu_1 + (220+5\mu_1)(\tau+\tau^4) + (165+10\mu_1)(\tau^2+\tau^3)$ et on choisit μ_1 tel que $220+5\mu_1 = 165+10\mu_1$, soit $\mu_1 = 11$.
Avec ce choix, $(1+\tau)^{10} + \mu_1(1+\tau)^5 = 254 + 22 + 275 \times (\tau+\tau^2+\tau^3+\tau^4)$ et $1+\tau$ est racine de $X^{10}+11X^5-1$ puisque $\tau+\tau^2+\tau^3+\tau^4 = -1$.
Donc $(-\alpha_0)^2((\frac{X}{b})^{10} + 11(\frac{X}{b})^5 - 1) = X^{10} - 11\alpha_0 X^5 - \alpha_0^2$ est annulateur de tout $a+b$ avec $a \neq \pm b$ et comme il est de degré $10 = \frac{n_1(n_1-1)}{2}$, c'est T et
$R_1(X) = -(X^5+32\alpha_0)(X^{10}-11\alpha_0 X^5 - \alpha_0^2)^2$. □

Cas $n_1 = 6$
$R_1(X) = X^6(2^6 P_1(\frac{X}{2}))T^2 = X^6(X^6+64\alpha_0)T^2$.
$\tau = \frac{a}{b} \neq \pm 1$; $\tau^6 = 1$.
Dans ce cas particulier on n'a pas besoin de passer à $(1+\tau)^{12}$, l'égalité $(1+\tau)^6 = 2 + 20\tau^3 + 6(\tau+\tau^5) + 15(\tau^2+\tau^4)$ suffisant.
En effet,

soit $\tau^3 = 1$ et alors $\tau^5 = \tau^2$ et $\tau^4 = \tau$, d'où $(1+\tau)^6 = 22 + 21(\tau+\tau^2) = 1$, car puisque $\tau \neq 1$, $\tau = j$ ou j^2 et $\tau+\tau^2 = -1$.
Donc $1+\tau$ racine de X^6-1 et $T_1(X) = (-\alpha_0)((\frac{X}{b})^6 - 1) = X^6 + \alpha_0$ est annulateur de tout $a+b$ avec $a \neq \pm b$ et $(\frac{a}{b})^3 = 1$.

soit $\tau^3 = -1$ alors $\tau^5 = -\tau^2$ et $\tau^4 = -\tau$, d'où $(1+\tau)^6 = -18 - 9(\tau-\tau^2) = -27$, car puisque $\tau \neq -1$, $\tau = -j$ ou $-j^2$ et $\tau - \tau^2 = 1$.
Donc $1+\tau$ racine de X^6+27 et $T_2(X) = (-\alpha_0)((\frac{X}{b})^4 + 27) = X^6 - 27\alpha_0$ est annulateur de tout $a+b$ avec $a \neq \pm b$ et $(\frac{a}{b})^3 = -1$.

Puisque la somme des degrés de T_1 et T_2 est $12 = \frac{n_1(n_1-2)}{2}$, c'est que $T_1 T_2 = T$ et
$R_1(X) = X^6(X^6+64\alpha_0)(X^6+\alpha_0)^2(X^6-27\alpha_0)^2$. □

Cas $n_1 = 7$
$R_1(X) = -(2^7 P_1(\frac{X}{2}))T^2 = -(X^7+128\alpha_0)T^2$.
$\tau = \frac{a}{b} \neq \pm 1$; $\tau^7 = 1$.
$(1+\tau)^7 = 2 + 7(\tau+\tau^6) + 21(\tau^2+\tau^5) + 35(\tau^3+\tau^4)$
$(1+\tau)^{14} = 3434 + 3017(\tau+\tau^6) + 2093(\tau^2+\tau^5) + 1365(\tau^3+\tau^4)$
$(1+\tau)^{21} = 232562 + 257775(\tau+\tau^6) + 314489(\tau^2+\tau^5) + 360031(\tau^3+\tau^4)$
$(1+\tau)^{21} + \mu_1(1+\tau)^7 + \mu_2(1+\tau)^{14} = p + q(\tau+\tau^6) + r(\tau^2+\tau^5) + s(\tau^3+\tau^4)$
avec
$p = 232562 + 2\mu_1 + 3434\mu_2$
$q = 257775 + 7\mu_1 + 3017\mu_2$
$r = 314489 + 21\mu_1 + 2093\mu_2$
$s = 360031 + 35\mu_1 + 1365\mu_2$.
Le systéme $q = r = s$ donne $\mu_1 = -289$ et $\mu_2 = 57$ et dans ce cas $p = 427722$ et $q = 427721$, ce qui donne
$(1+\tau)^{21} - 289(1+\tau)^7 + 57(1+\tau)^{14} = 427722 + 427721(\tau+\tau^6+\tau^2+\tau^5+\tau^3+\tau^4) = 1$.
Donc $X^{21} + 57X^{14} - 289X^7 - 1$ est annulateur de $1+\tau$ et
$(-\alpha_0)^3((\frac{X}{b})^{21} + 57(\frac{X}{b})^{14} - 289(\frac{X}{b})^7 - 1) = X^{21} - 57\alpha_0 X^{14} - 289\alpha_0^2 X^7 + \alpha_0^3$ est annulateur de

tout $a+b$ avec $a \neq \pm -b$, et comme il est de degré $\frac{n_1(n_1-1)}{2} = 21$, c'est le polynôme T et $R_1(X) = -(X^7 + 128\alpha_0)^2(X^{21} - 57\alpha_0 X^{14} - 289\alpha_0^2 X^7 + \alpha_0^3)^2$. □

Cas $n_1 = 8$

$R_1(X) = X^8(2^8 P_1(\frac{X}{2}))T^2 = X^8(X^8 + 256\alpha_0)T^2$.

$\tau = \frac{a}{b} \neq \pm 1$; $\tau^8 = 1$.

$(1+\tau)^8 = 2 + 8(\tau + \tau^7) + 28(\tau^2 + \tau^6) + 56(\tau^3 + \tau^5) + 70\tau^4$

$(1+\tau)^{16} = 12872 + 11456(\tau + \tau^7) + 8128(\tau^2 + \tau^6) + 4928(\tau^3 + \tau^5) + 3640\tau^4$.

Mais $\tau^4 = \pm 1$, donc

soit $\tau^4 = 1$, et $\tau^2 = -1 \Leftrightarrow \tau = \pm i$ (puisque ± 1 est exclu), et alors $\tau + \tau^7 = \tau^3 + \tau^5 = 0$ et $\tau^2 + \tau^6 = -2$, donc on obtient tout de suite $(1+\tau)^8 = 16$ et un polynôme annulateur de $1+\tau$ est $X^8 - 16$, donc un polynôme annulateur de tout $a+b$ avec $a \neq \pm b$ et $(\frac{a}{b})^4 = 1$ est $T_1(X) = (-\alpha_0)((\frac{X}{b})^8 - 16) = X^8 + 16\alpha_0$

soit $\tau^4 = -1$, et cette fois $\tau^2 + \tau^6 = 0$ et $\tau + \tau^7 = \tau - \tau^3 = -(\tau^3 + \tau^5)$ et ainsi $(1+\tau)^8 = -68 + 48(\tau^3 - \tau)$ et $(1+\tau)^{16} = 9232 + 6528(\tau^3 - \tau)$.

Il n'y a pas de systéme à résoudre : on élimine $\tau^3 - \tau$ entre les deux égalités et $(6528 = 136 \times 48)$ on obtient $X^{16} - 136X^8 - 18480$ comme polynôme annulateur de $1+\tau$.

Un polynôme annulateur de tout $a+b$ avec $a \neq \pm b$ et $(\frac{a}{b})^4 = -1$ est

$T_2(X) = (-\alpha_0)^2((\frac{X}{b})^{16} - 136(\frac{X}{b})^8 - 18480) = X^{16} + 136\alpha_0 X^8 - 18480\alpha_0^2$.

Comme la somme des degrés de T_1 et T_2 est $\frac{n_1(n_1-2)}{2} = 24$, c'est que $T_1 T_2 = T$ et $R_1(X) = X^8(X^8 + 256\alpha_0)(X^8 + 16\alpha_0)^2(X^{16} + 136\alpha_0 X^8 - 18480\alpha_0^2)^2$. □

Annexe 1

Critères d'irréductibilité dans $Q[X]$

1) K étant un corps dont une extension est L, si A et B (non nuls) sont dans $K[X]$, avec $A = BC$ et C dans $L[X]$, alors C est dans $K[X]$.

preuve :

Par division euclidienne dans $K[X]$, $A = BU + V$ avec $V = 0$ ou $d^\circ V < d^\circ B$.

On en déduit $B(C - U) = V$ et $V \neq 0$ implique $C - U \neq 0$ et $d^\circ V \geq d^\circ B$ d'où contradiction : V est obligatoirement nul, donc $C = U$ est dans $K[X]$.

Autre façon : la division euclidienne dans $K[X]$ ci-dessus est évidemment une division euclidienne dans $L[X]$, or l'égalité $A = BC$ est aussi une division euclidienne dans $L[X]$, et par unicité de cette division, $U = C$ et $V = 0$. □

2)

2.1) Soit P un polynôme de $Q[X]$ dont la décomposition en facteurs irréductibles dans $R[X]$ est $\prod_i F_i^{n_i}$: si P est réductible sur $Q[X]$ alors on peut partitionner les F_i en deux groupes tels que les deux produits des F_i les constituant soient des polynômes de $Q[X]$ non constants.

preuve : si $P = UV$ avec U, V deux polynômes de $Q[X]$ de degré ≥ 1, on décompose U et V en facteurs irréductibles de $R[X]$ et l'unicité de la décomposition en facteurs irréductibles de $R[X]$ permet de conclure. □

2.2) Si $P = (X^2 + aX + b)(X^2 + a'X + b')$ est un élément de $Q[X]$ avec $a^2 - 4b < 0$, $a'^2 - 4b' < 0$, et $X^2 + aX + b$ et $X^2 + a'X + b'$ pas dans $Q[X]$, alors P est irréductible sur $Q[X]$.

preuve : P ne peut être réductible cf le 2.1. □

Exemple 1 : $X^4 + 1 = (X^2 + \sqrt{2}\,X + 1)(X^2 - \sqrt{2}\,X + 1)$ est irréductible dans $Q[X]$, d'après 2.2

Exemple 2 :

$X^4 - X^2 + 1 = (X^2 - \sqrt{3}\,X + 1)(X^2 + \sqrt{3}\,X + 1)$ est irréductible dans $Q[X]$, d'après 2.2

Exemple 3 :

$X^4 - 2 = (X^4 - \sqrt[4]{2})(X + \sqrt[4]{2})(X^2 + \sqrt{2})$ est irréductible dans $Q[X]$, d'après 2.1, car le regroupement de deux des facteurs laissera subsister le troisième qui n'est pas dans $Q[X]$ (exemple du livre de Jean-Claude Carrega, Théorie des corps).

Bien entendu, le critère d'Eisenstein (voir ci-dessous) donne aussi la réponse.

3) Critère d'Eisenstein.

Pour tout entier $n \geq 2$, soit $P(X) = c_n X^n + c_{n-1} X^{n-1} + \ldots + c_1 X + c_0 \in Z[X]$:

s'il existe un nombre p premier tel que

- p divise tous les coefficients de P, excepté c_n
- p^2 ne divise pas c_0

alors P est irréductible dans $Q[X]$.

Exemple 1 : $P(X) = X^6 - 3X^3 + 12X - 3$ est irréductible dans $Q[X]$ (prendre $p = 3$).

Exemple 2 : si n est un entier ≥ 1, p un nombre premier, alors $X^n \pm p$ est irréductible

dans $Q[X]$

4) Soit K un sous-corps de C :

si p est un nombre premier et k dans K, alors
$X^p - k$ irréductible sur $K \Leftrightarrow X^p - k$ n'a pas de racine dans K

si n est un entier ≥ 1, p est un nombre premier impair et k dans K, alors
$X^{p^n} - k$ irréductible sur $K \Leftrightarrow X^p - k$ n'a pas de racine dans K

si n est un entier ≥ 2, $k \in K$, alors
$X^{2^n} - k$ irréducitible sur $K \Leftrightarrow X^2 - k$ et $4X^2 + k$ n'ont pas de racine dans K.

Par exemple $X^{2^n} + 2$ est irréductible sur $\mathbb{Q}$, $X^2 + 2$ et $4X^2 - 2$ n'ayant pas de racine rationnelle.
Note : ces trois résultats sont prouvés dans le livre Exercices d'algèbre (Ellipse) de Pascal Ortiz.

5) Un critère moins courant qui nécessite de connaître un majorant des parties réelles de toutes les racines du polynôme :
Soit $P \in Z[X]$ et $k \in Z$ tel que pour toute racine $z \in C$ de P on a $\mathrm{Re}(z) < k - \frac{1}{2}$ (inégalité vérifiée si $|z| < k - \frac{1}{2}$) :
si $P(k-1) \neq 0$ et si $|P(k)|$ est un nombre premier ou $P(k) = \pm 1$ alors P est irréducible sur $Q[X]$.

Evidemment si $|P(k)|$ n'est pas un nombre premier et si $P(k) \neq \pm 1$, on regarde ce qui se passe pour $P(k+1)$, puisque pour toute racine z de P on a aussi $\mathrm{Re}(z) < k + 1 - \frac{1}{2}$.
Etc.
Remarque 1 : par exemple le site www.decode.fr peut s'avérer très utile pour tester la primalité de grands entiers.
Remarque 2 : dans cette étude j'ai utilisé ce critère environ une dizaine de fois. Une seule fois je n'ai pas pu conclure car de $k = 3$ à $k = 37$, $P(k)$ n'était pas premier (exemple 3 du 5)).

preuve :
montrons d'abord que $\forall t > 0,\ |P(k - \frac{1}{2} - t)| < |P(k - \frac{1}{2} + t)|$:
soit $z = a + ib$ une racine de P
et $d = |k - \frac{1}{2} - t - z|^2 - |k - \frac{1}{2} + t - z|^2 = -2t(2k - 1 - 2a) < 0$, puisque $t > 0$ et $a < k - \frac{1}{2}$.
Donc $|k - \frac{1}{2} - t - z| < |k - \frac{1}{2} + t - z|$ pour toute racine z de P et par multiplication membre à membre de toutes les inégalités correspondantes on a $|P(k - \frac{1}{2} - t)| < |P(k - \frac{1}{2} + t)|$.
Supposons $P=UV$ avec U et V dans $Z[X]$ avec U et V non constants.
En faisant $t = \frac{1}{2}$ dans le résultat précédent (qui s'applique à U, puisque les racines de U sont racines de P), on obtient $|U(k-1)| < |U(k)|$.
Comme $U(k-1) \neq 0$, $|U(k-1)| \geq 1$, donc $|U(k)| > 1$ et $|U(k)| \geq 2$.
De même, $|V(k)| \geq 2$, or $|P(k)| = |U(k)||V(k)|$ et $|P(k)|$ est premier ou égal à 1 : ceci est

impossible et donc P n'est pas le produit de deux polynômes non constants de $Z[X]$, donc P est irréductible sur $Q[X]$. □

Annexe 2

Quelques précisions sur le résultant de deux polynômes de $Q[X]$ de degrés ≥ 1
(à partir d'un exemple)

Définition :

Soient $P(X) = \alpha_3 X^3 + \alpha_2 X^2 + \alpha_1 X + \alpha_{.0} \in Q[X]$ de degré $p = 3$ et
$Q(X) = \beta_5 X^5 + \beta_4 X^4 + \beta_3 X^3 + \beta_2 X^2 + \beta_1 X + \beta_0 \in Q[X]$ de degré $q = 5$.
Je prends comme résultant de P et Q, noté $res(P,Q)$ le déterminant de la matrice $(p+q) \times (p+q) = 8 \times 8$ suivante :

$$\begin{pmatrix} \alpha_0 & 0 & 0 & 0 & 0 & \beta_0 & 0 & 0 \\ \alpha_1 & \alpha_0 & 0 & 0 & 0 & \beta_1 & \beta_0 & 0 \\ \alpha_2 & \alpha_1 & \alpha_0 & 0 & 0 & \beta_2 & \beta_1 & \beta_0 \\ \alpha_3 & \alpha_2 & \alpha_1 & \alpha_0 & 0 & \beta_3 & \beta_2 & \beta_1 \\ 0 & \alpha_3 & \alpha_2 & \alpha_1 & \alpha_0 & \beta_4 & \beta_3 & \beta_2 \\ 0 & 0 & \alpha_3 & \alpha_2 & \alpha_1 & \beta_5 & \beta_4 & \beta_3 \\ 0 & 0 & 0 & \alpha_3 & \alpha_2 & 0 & \beta_5 & \beta_4 \\ 0 & 0 & 0 & 0 & \alpha_3 & 0 & 0 & \beta_5 \end{pmatrix}$$

C'est le déterminant de Sylvester : P apparaît dans les q premières colonnes et Q apparaît dans les p colonnes suivantes.
Evidemment ce déterminant appartient à l'anneau contenant les coefficients α_i et β_i, à savoir ici Q.

R0 P et Q étant deux éléments de $Q[X]$ de degrés respectifs p et q, de coefficients de tête respectifs α_p et β_q,
de racines respectives (dans $\mathbb{C}$), $x_1, x_2, \ldots, x_p$ et $y_1, y_2, \ldots, y_q$, on a

$$res(P,Q) = \alpha_p^q \beta_q^p \prod_{\substack{i=1,2,\ldots,p \\ j=1,2,\ldots,q}} (y_j - x_i) = (-1)^{pq} \prod_{\substack{i=1,2,\ldots,p \\ j=1,2,\ldots,q}} (x_i - y_j)$$

$$res(P,Q) = \beta_q^p \prod_{j=1,2,\ldots,q} P(y_j) = (-1)^{pq} \alpha_p^q \prod_{i=1,2,\ldots,p} Q(x_i).$$

R1 P et Q étant deux éléments de $Q[X]$ de degrés ≥ 1, $res(P,Q)$ est nul si et seulement si les deux polynômes ont, dans C, une racine commune.

C'est évident à partir de R0. Vérifions le à partir du déterminant de Sylvester sur un exemple.
Prenons $P(X) = X + \alpha_0$ et $Q(X) = \beta_3 X^3 + \beta_2 X^2 + \beta_1 X + \beta_0$ avec α_0, β_i dans Q.
$res(P,Q)$ est le déterminant de

$$\begin{pmatrix} \alpha_0 & 0 & 0 & \beta_0 \\ 1 & \alpha_0 & 0 & \beta_1 \\ 0 & 1 & \alpha_0 & \beta_2 \\ 0 & 0 & 1 & \beta_3 \end{pmatrix}$$

et en développant par rapport à la première ligne, on obtient
$res(P,Q) = \alpha_0(\alpha_0^2\beta_3 + \beta_1 - \alpha_0\beta_2) - \beta_0 = -Q(-\alpha_0)$ et donc $res(P,Q) = 0 \Leftrightarrow -\alpha_0$ est racine de $Q \Leftrightarrow P$ et Q ont une racine commune.

R2 $res(Q,P) = (-1)^{pq} res(P,Q)$: si l'un des polynômes a un degré pair les deux résultats sont égaux.

R3 La définition du résultant de deux polynômes de degrés ≥ 1, peut être étendue au cas où un seul des polynôme est constant, cad de degré 0.
Par exemple si $P = \alpha_0,$ et $q \geq 1$, Q n'apparaît pas dans le déterminant de Sylvester (il est de dimension $q \times q$), seul P apparaît q fois, et la matrice étant $\alpha_0 I_8$, $res(P,Q) = \alpha_0^q$.

On remarque que $res(Q,P)$ va être aussi α_0^q et ainsi R2 est vérifié puisqu'ici $pq = 0$.
Mais R1 est aussi vérifié car $res(P,Q) = 0 \Leftrightarrow \alpha_0 = 0 \Leftrightarrow P$ et Q ont une racine commune (puisque si $\alpha_0 = 0$ toutes les racines de Q sont racines de P, et si $\alpha_0 \neq 0,$ ils ne peuvent avoir de racines communes,P n'en ayant pas).

Bien entendu, si les deux polynômes P et Q étaient constants, la matrice ci-dessus ne serait pas définie.

R4 P_1 et P_2 étant maintenant deux polynômes de $Q[X]$ unitaires **non constants** et P_2 de terme constant non nul, on considère les deux résultants suivants (voir le 2.5) : ici je n'ai pas besoin de supposer P_1 et P_2 irréductibles) :

$R_1(X) = res_Y(P_1(Y), P_2(X-Y))$ et $R_2(X) = res_Y(P_1(Y), Y^{n_2}P_2(\frac{X}{Y}))$.

Le terme constant de P_2 est supposé non nul pour que $Y^{n_2}P_2(\frac{X}{Y})$ soit toujours de degré (en Y) ≥ 1 (si $P_2(X) = X$ ce n'est plus le cas car alors $Y^{n_2}P_2(\frac{X}{Y}) = X$).
Alors,
1) R_1 et $R_2 \in \mathbb{Q}[X]$ et sont de degré $n_1 n_2$ et de coefficient de tête $\pm 1 = (-1)^{n_1 n_2}$.

2) Cas particuliers :
2.1) si $P_1(X) = X,$ alors $R_2(X) = (-1)^{n_2}X^{n_2}$

2.2) si $P_2(X) = X + \beta_0$ avec $\beta_0 \neq 0$ alors $R_2(X) = \beta_0^{n_1}P_1(-\frac{1}{\beta_0}X),$ donc de terme de plus haut degré $(-1)^{n_1}X^{n_1},$ ce qui est cohérent avec le 1).

2.3) si $P_1(X) = X^3 + \alpha_0$ et $P_2(X) = X^3 + \beta_0$ (avec $\beta_0 \neq 0$) alors
$-R_1(X) = (X^3 + \alpha_0 + \beta_0)^3 - 27\alpha_0\beta_0X^3$
$-R_2(X) = (X^3 - \alpha_0\beta_0)^3$

R5 Lorsque P_1 est de degré $1,$ les polynômes minimaux de $a+b$ et ab ont été déterminés au 3.1) sans utiliser la notion de résultant. On va montrer ici que ces polynômes minimaux sont respectivement $(-1)^{n_1n_2}R_1$ et si $\alpha_0 \neq 0,$ $(-1)^{n_1n_2}R_2,$ par contre pour α_0 le polynôme minimal de tout ab est $X,$ seul facteur irréductible de R_2.

preuves :

preuve R0 : admis. □

preuve R1 :

c'est évidemment trivial en appliquant le résultat précédent, mais comme je ne donne pas la preuve de R0, je propose une preuve à partir de la définition du résultant comme déterminant de Sylvester.

Elle se fait en deux étapes.

P et Q ont une racine commune si et seulement si "leur pgcd" est de degré ≥ 1 (note le pgcd est défini à une constante multiplicative près) :

en effet, si P et Q sont premiers entre eux, Bezout montre qu'ils n'ont pas de racine commune, donc si P et Q ont une racine commune, ils ne sont pas premiers entre eux, cad leur pgcd n'est pas une constante ; réciproquement si leur pgcd est de degré ≥ 1, il a une racine dans C, racine qui est commune à P et Q.

le pgcd de P et Q est de degré ≥ 1 si et seulement si il existe deux polynômes non nuls U et $V \in Q[X]$ tels que $UP + VQ = 0$ avec $d°U < d°Q$ et $d°V < P$.

en effet, si le pgcd D de P et Q est de degré ≥ 1, on prend $U = \frac{Q}{D} \in Q[X]^*$ et $V = \frac{-P}{D} \in Q[X]^*$; réciproquement si $UP + VQ = 0$ avec U, V dans $Q[X]$ et $d°U < d°Q$ et $d°V < P$, alors P et Q ne peuvent être premiers entre eux, car sinon, Q divisant UP, Q diviserait U, et on n'aurait pas $d°U < d°Q$.

P et Q ont une racine commune si et seulement si les $n_1 + n_2$ polynômes X^iP pour $0 \leq i \leq q-1$ et X^jQ pour $0 \leq j \leq p-1$ forment une partie liée de l'espace vectoriel des polynômes, à coefficients dans C, de degré au plus égal à $p + q - 1$, cad la matrice de leurs coefficients dans la base canonique $1, X, X^2, \ldots, X^{p+q-1}$ de cet espace vectoriel est non inversible, donc si et seulement si le déterminant de Sylvester de P et Q est nul. □

preuve R2 :

là aussi le résultat est immédiat à partir de $R0$, mais on peut le démontrer facilement à partir du déterminant de Sylvester.

En effet, si on échange deux colonnes d'un déterminant, celui-ci change de signe.

Notons $res(P,Q) = \det(c_1, c_2, \ldots c_p, c_{p+1}, \ldots, c_{p+q})$ où c_i est la ième colonne de $res(P,Q)$.

Pour obtenir $res(Q,P)$ il faut que les q dernières colonnes (leur ordre étant conservé) de $res(P,Q)$ deviennent les q premières colonnes, les p premières (leur ordre étant conservé) devenant les p dernières.

En échangeant c_{p+1} et c_p, puis c_{p+1} et c_{p-1},..., puis c_{p+1} avec c_1, on obtient $\det(c_{p+1}, c_1, c_2, \ldots c_p, c_{p+2}, \ldots, c_{p+q})$, cela avec p échanges.

On répéte la même chose avec c_{p+2} et on obtient $\det(c_{p+1}, c_{p+2}, c_1, c_2, \ldots c_p, c_{p+3}, \ldots, c_{p+q})$ avec encore p échanges

Etc : à partir de $res(P,Q)$, avec pq échanges on obtient donc $\det(c_{p+1}, c_{p+2}, \ldots, c_{p+q}, c_1, c_2, \ldots c_p) = res(Q,P)$. □

preuve R4 :

1) $P_1(Y)$, $P_2(X-Y))$, $Y^{n_2}P_2(\frac{X}{Y})$ sont des polynômes en Y dont les coefficients sont dans l'anneau $Q[X]$, donc R_1 et R_2 sont dans $Q[X]$.

Pour déterminer leur degré et coefficient de tête, remarquons que le déterminant de Sylvester de l'exemple donné à la définition ci-dessus est (comme tout déterminant) la somme (algébrique) de $8!$ produits de 8 coefficients de la matrice, ces 8 coefficients appartenant tous à des lignes différentes et à des colonnes différentes.

On voit alors qu'il y a un seul produit (formellement non nul) contenant β_0^3 : c'est, au

signe près, $\alpha_3^5\beta_0^3$:
en effet, les coefficients autres que β_0 doivent être pris dans la sous-matrice 5×5 située en bas et à gauche, et évidemment en prenant un seul par ligne et par colonne, donc dans la première colonne de cette sous-matrice, on doit prendre α_3, sinon on est obligé de prendre 0, etc

Appliquons cette remarque :
d'après la formule de Taylor pour les polynômes,
$P_2(X-Y)=P_2(X)-P_2^{'}(X)Y+\frac{1}{2}P_2^{''}(X)Y^2+\ldots+\frac{(-1)^{n_2-1}}{(n_2-1)!}P_2^{(n_2-1)}(X)Y^{n_2-1}+(-1)^{n_2}Y^{n_2}$
donc, parmi les $8!$ termes du résultant R_1 (polynôme en X) celui de degré le plus élevè est, au signe près, $\alpha_{n_1}^{n_2}\beta_0^{n_1}=1^{n_2}\times(P_2(X))^{n_1}$: donc R_1 est de degré n_1n_2 et de coefficient de tête ± 1.
En fait, en mettant les colonnes correspondants à P_2 au début de la matrice et en utilisant le raisonnement fait à la preuve de R2, on voit que le coefficient de tête de R_1 est $(-1)^{n_1n_2}$.
Et pour R_2, comme $Y^{n_2}P_2(\frac{X}{Y})=X^{n_2}+\beta_{n_2-1}X^{n_2-1}Y+\ldots+\beta_1XY^{n_2-1}+\beta_0Y^{n_2}$ est un polynôme en Y de degré n_2 (car $\beta_0\neq 0$) et a pour terme constant X^{n_2}, parmi les $8!$ termes du résultant R_2 (polynôme en X) celui de degré le plus élevè est, au signe près, $1^{n_2\times}(X^{n_2})^{n_1}$: donc R_2 est de degré n_1n_2 et de coefficient de tête ± 1, qui est en fait $(-1)^{n_1n_2}$ (même raisonnement que ci-dessu pour R_1).

2) Illustrons par des exemples : le lecteur en déduira la preuve générale.
2.1) si $P_1(X)=X$, $P_2(X)=X^3+\beta_2X^2+\beta_1X+\beta_0$ (par exemple) :
$R_2(X)$ est (puisque $Y^2P_2(\frac{X}{Y})=X^3+\beta_2X^2Y+\beta_1XY^2+\beta_0Y^3$, avec $\beta_0\neq 0$) le déterminant de
$\begin{pmatrix} 0 & 0 & 0 & X^3 \\ 1 & 0 & 0 & \beta_2X^2 \\ 0 & 1 & 0 & \beta_1X \\ 0 & 0 & 1 & \beta_0 \end{pmatrix}$, soit en développant par rapport à la première ligne
$-X^3=(-1)^{n_1n_2}X^{n_2}$

2.2) si $P_1(X)=X^3+\alpha_2X^2+\alpha_1X+\alpha_0$ (par exemple) , $P_2(X)=X+\beta_0$
$R_2(X)$ est (puisque $YP_2(\frac{X}{Y})=X+\beta_0Y$) le déterminant de
$\begin{pmatrix} \alpha_0 & X & 0 & 0 \\ \alpha_1 & \beta_0 & X & 0 \\ \alpha_2 & 0 & \beta_0 & X \\ 1 & 0 & 0 & \beta_0 \end{pmatrix}$, soit en développant par rapport à la première colonne (on obtient que des déterminants triangulaires)$-X^3+\alpha_2\beta_0X^2-\alpha_1\beta_0^2X+\alpha_0\beta_0^3$, ce qui est, pour $\beta_0\neq 0$, $\beta_0^3P_1(-\frac{1}{\beta_0}X)$.

2.3) si $P_1(X)=X^3+\alpha_0$ et $P_2(X)=X^3+\beta_0$ (avec $\beta_0\neq 0$) alors

$R_1(X)$ est le résultant de $P_1(Y)=Y^3+\alpha_0$ et $P_2(X-Y)=(X-Y)^3+\beta_0$, cad le déterminant de

$$\begin{pmatrix} \alpha_0 & 0 & 0 & X^3+\beta_0 & 0 & 0 \\ 0 & \alpha_0 & 0 & -3X^2 & X^3+\beta_0 & 0 \\ 0 & 0 & \alpha_0 & 3X & -3X^2 & X^3+\beta_0 \\ 1 & 0 & 0 & -1 & 3X & -3X^2 \\ 0 & 1 & 0 & 0 & -1 & 3X \\ 0 & 0 & 1 & 0 & 0 & -1 \end{pmatrix}$$

soit, en ajoutant, respectivement, les trois premières colonnnes aux trois dernières

$$\begin{pmatrix} \alpha_0 & 0 & 0 & X^3+\alpha_0+\beta_0 & 0 & 0 \\ 0 & \alpha_0 & 0 & -3X^2 & X^3+\alpha_0+\beta_0 & 0 \\ 0 & 0 & \alpha_0 & 3X & -3X^2 & X^3+\alpha_0+\beta_0 \\ 1 & 0 & 0 & 0 & 3X & -3X^2 \\ 0 & 1 & 0 & 0 & 0 & 3X \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

puis en développant par rapport à la dernière ligne, et en notant $S = X^3 + \alpha_0 + \beta_0$

$$-\begin{pmatrix} \alpha_0 & 0 & S & 0 & 0 \\ 0 & \alpha_0 & -3X^2 & S & 0 \\ 0 & 0 & 3X & -3X^2 & S \\ 1 & 0 & 0 & 3X & -3X^2 \\ 0 & 1 & 0 & 0 & 3X \end{pmatrix}$$

puis en développant par rapport à la dernière ligne

$$\begin{pmatrix} \alpha_0 & S & 0 & 0 \\ 0 & -3X^2 & S & 0 \\ 0 & 3X & -3X^2 & S \\ 1 & 0 & 3X & -3X^2 \end{pmatrix} - 3X\begin{pmatrix} \alpha_0 & 0 & S & 0 \\ 0 & \alpha_0 & -3X^2 & S \\ 0 & 0 & 3X & -3X^2 \\ 1 & 0 & 0 & 3X \end{pmatrix}$$

et on développe chacun des deux déterminants 4×4 par rapport à leur première colonne

$$\alpha_0\begin{pmatrix} -3X^2 & S & 0 \\ 3X & -3X^2 & S \\ 0 & 3X & -3X^2 \end{pmatrix} - S^3 - 27\alpha_0^2X^3 + 3X\begin{pmatrix} 0 & S & 0 \\ \alpha_0 & -3X^2 & S \\ 0 & 3X & -3X^2 \end{pmatrix}$$

Et par deux Sarrus, on obtient

$R_1(X) = \alpha_0(-27X^6 + 18X^3S) - S^3 - 27\alpha_0^2X^3 + 9\alpha_0SX^3 =$

$R_1(X) = -S^3 - 27\alpha_0(X^6 - X^3S + \alpha_0X^3) = -(X^3 + \alpha_0 + \beta_0)^3 + 27\alpha_0\beta_0X^3$

Quant à R_2, c'est le résultant de $P_1(Y)$ et de $Y^3P_2(\frac{X}{Y}) = X^3 + \beta_0Y^3$, soit le déterminant de

$$\begin{pmatrix} \alpha_0 & 0 & 0 & X^3 & 0 & 0 \\ 0 & \alpha_0 & 0 & 0 & X^3 & 0 \\ 0 & 0 & \alpha_0 & 0 & 0 & X^3 \\ 1 & 0 & 0 & \beta_0 & 0 & 0 \\ 0 & 1 & 0 & 0 & \beta_0 & 0 \\ 0 & 0 & 1 & 0 & 0 & \beta_0 \end{pmatrix}$$

On soustrait les trois dernières colonnes aux (respectivement) trois premières colonnes multipliées par β_0, et on est ramené (rappel : on a supposé $\beta_0 \neq 0$) au déterminant de

$$\frac{1}{\beta_0^3}\begin{pmatrix} \alpha_0\beta_0 - X^3 & 0 & 0 & X^3 & 0 & 0 \\ 0 & \alpha_0\beta_0 - X^3 & 0 & 0 & X^3 & 0 \\ 0 & 0 & \alpha_0\beta_0 - X^3 & 0 & 0 & X^3 \\ 0 & 0 & 0 & \beta_0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \beta_0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \beta_0 \end{pmatrix}$$

La matrice est triangulaire et donc

$R_2(X) = \frac{1}{\beta_0^3}(\alpha_0\beta_0 - X^3)^3\beta_0^3 = (\alpha_0\beta_0 - X^3)^3$.

Remarque : par continuité de $R_2(X)$ par rapport à β_0, le résultat est encore vrai pour $\beta_0 = 0$. □

preuve R5 :

comme $P_1(X) = X + \alpha_0$, a prend une seule valeur $-\alpha_0$.

Cas $a + b$

Il a été vu au 3.1) que tout $a + b = -\alpha_0 + b$ a pour polynôme minimal $P_2(X + \alpha_0)$

Vérifions dans le cas $n_2 = 4$ (généralisation laissée au lecteur) que ce polynôme minimal est $(-1)^{n_1 n_2} R_1(X)$.

Puisque $P_2(X - Y) = P_2(X) - P_2'(X)Y + \frac{1}{2}P''(X)Y^2 - \frac{1}{6}P_2'''(X)Y^3 + Y^4$, $R_1(X)$ est le déterminant de

$$\begin{pmatrix} \alpha_0 & 0 & 0 & 0 & P_2(X) \\ 1 & \alpha_0 & 0 & 0 & -P_2'(X) \\ 0 & 1 & \alpha_0 & 0 & \frac{P_2''(X)}{2} \\ 0 & 0 & 1 & \alpha_0 & -\frac{P_2'''(X)}{6} \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

En développant par rapport à la dernière colonne, on obtient

$R_1(X) = \alpha_0^4 + \frac{1}{6}P_2'''(X)\alpha_0^3 + \frac{1}{2}P_2''(X)\alpha_0^2 + P_2'(X)\alpha_0 + P_2(X) = P_2(X + \alpha_0)$

Cas ab

On a aussi vu au 3.1) que

tout ab étant $-\alpha_0 b$,

si $\alpha_0 = 0$, tout ab a pour valeur 0, de polynôme minimal X

si $\alpha_0 \neq 0$, tout ab a pour polynôme minimal $(-\alpha_0)^{n_2} P(\frac{X}{-\alpha_0})$.

Vérifions dans le cas $n_2 = 4$ (généralisation laissée au lecteur) que si $\alpha_0 \neq 0$, $(-1)^{n_1 n_2} R_2 = R_2$ est égal à $(-\alpha_0)^{n_2} P(\frac{X}{-\alpha_0})$.

$R_2(X)$ est le déterminant de

$$\begin{pmatrix} \alpha_0 & 0 & 0 & 0 & X^4 \\ 1 & \alpha_0 & 0 & 0 & \beta_3 X^3 \\ 0 & 1 & \alpha_0 & 0 & \beta_2 X^2 \\ 0 & 0 & 1 & \alpha_0 & \beta_1 X \\ 0 & 0 & 0 & 1 & \beta_0 \end{pmatrix}$$

soit en développant par rapport à la dernière colonne
$R_2(X) = X^4 - \beta_3 X^3 \alpha_0 + \beta_2 X^2 \alpha_0^2 - \beta_1 X \alpha_0^3 + \beta_0 \alpha_0^4$.

Donc si $\alpha_0 \neq 0$, $R_2(X) = (-\alpha_0)^4 P(\frac{X}{-\alpha_0})$ qui est le polynôme minimal de tout ab trouvé au 3.1.

Mais si $\alpha_0 = 0$, $R_2(X) = X^4$ et le seul facteur irréductible de R_2 est X, ce qui signifie (voir 4.1.2)) que ab prend une seule valeur 0 de polynôme minimal X, résultat trouvé au 3.1.

□

Annexe 3

Deux compléments sur l'exemple 7 du 6).

1) Une preuve que $\cos(\frac{\pi}{12}), \cos(\frac{5\pi}{12}), \cos(\frac{7\pi}{12}), \cos(\frac{11\pi}{12})$ ne sont pas rationnels.

Pour cela j'utilise le théorème suivant :
si n est un entier ≥ 3 et si ζ est une racine n-ième de 1 primitive alors $\zeta + \frac{1}{\zeta}$ est algébrique sur Q de degré $\frac{\varphi(n)}{2}$.

Application au cas $n = 24$:
$\frac{\varphi(24)}{2} = \frac{\varphi(2^3)\varphi(3)}{2} = \frac{(2^3 - 2^2)(3-1)}{2} = 4 \neq 1,$ donc pour les $\varphi(24) = 8$ racines 24-ième de 1 primitives $\zeta,\ \zeta + \frac{1}{\zeta}$ n'est pas rationnel.

Or ces huit racines 24-ième de 1 primitives sont $e^{\frac{2\pi i}{24}k}$ avec $k \leq 24$ et premier avec 24, soit $k \in \{1;5;7;11;13;17;19;23\}$.
Comme $e^{\frac{2\pi i}{24}k} + \frac{1}{e^{\frac{2\pi i}{24}k}} = 2\cos\frac{\pi i}{12}k$, on obtient le résultat annoncé. □

2) Une vérification sur les deux polynômes minimaux possibles pour chacune des 16 valeurs de $a + b$.
Ces deux polynômes sont
$X^8 - 4X^6 + 15X^4 - 4X^2 + 1$ de racines $\sqrt{2} - v_0,\ -\sqrt{2} + v_0,\ \sqrt{2} + v_2,\ -\sqrt{2} - v_2,\ \sqrt{2} - v_3,\ -\sqrt{2} + v_3,\ \sqrt{2} + v_5,\ -\sqrt{2} - v_5$
et
$X^8 - 12X^6 + 47X^4 - 84X^2 + 169$ de racines $-\sqrt{2} - v_0,\ \sqrt{2} + v_0,\ -\sqrt{2} + v_2,\ \sqrt{2} - v_2,\ -\sqrt{2} - v_3,\ \sqrt{2} + v_3,\ -\sqrt{2} + v_5,\ \sqrt{2} - v_5$.
Le produit p_v de ces 16 racines doit être $1 \times 169 = 169$: vérifons le.

$p_v = (-1)^8(\prod_{i=0,2,3,5}(\sqrt{2} + v_i)\prod_{i=0,2,3,5}(\sqrt{2} - v_i))^2 = \prod_{i=0,2,3,5}\theta_i$ avec $\theta_i = v_i^4 - 4v_i^2 + 4$.

$v_0^2 = e^{\frac{i\pi}{6}}$, $v_0^4 = e^{\frac{i\pi}{3}}$, $\theta_0 = \frac{9}{2} - 2\sqrt{3} + i(-2 + \frac{\sqrt{3}}{2})$

$v_2^2 = e^{\frac{i5\pi}{6}}$, $v_2^4 = e^{\frac{i5\pi}{3}}$, $\theta_2 = \frac{9}{2} + 2\sqrt{3} + i(-2 - \frac{\sqrt{3}}{2})$

$v_3^2 = e^{\frac{i7\pi}{6}}$, $v_3^4 = e^{\frac{i7\pi}{3}}$, donc θ_3 et θ_2 sont conjugués (si $\theta' + \theta = 2k\pi,\ e^{i\theta'}$ et $e^{i\theta}$ sont conjugués)

$v_5^2 = e^{\frac{i11\pi}{6}}$, $v_5^4 = e^{\frac{i11\pi}{3}}$, donc θ_5 et θ_0 sont conjugués.

D'où $p_v = |\theta_0|^2|\theta_2|^2 = ((\frac{9}{2} - 2\sqrt{3})^2 + (-2 + \frac{\sqrt{3}}{2})^2) \times ((\frac{9}{2} + 2\sqrt{3})^2 + (2 + \frac{\sqrt{3}}{2})^2)$

$p_v = (37 - 20\sqrt{3}) \times (37 + 20\sqrt{3}) = 169.$ □

annexe 4

Un complément sur les exemple 6 et 7 du 6) : polynôme minimal des racines de X^4+1 et des racines de X^8-X^4+1 sur $Q(\sqrt{2})$.

Rappelons que X^4+1 est le polynôme minimal sur Q de $\pm v_1$ et $\pm v_4$, et que X^8-X^4+1 est le polynôme minimal sur Q de $\pm v_0$, $\pm v_2$, $\pm v_3$, $\pm v_5$, les $\pm v_i$ étant les racines de $X^{12}+1$.

Cas des racines de $X^4+1=(X^2-\sqrt{2}X+1)(X^2+\sqrt{2}X+1)$:

les deux facteurs $X^2-\sqrt{2}X+1$ et $X^2+\sqrt{2}X+1$ sont irréductibles sur $Q(\sqrt{2})$ puisqu'ils n'ont pas de racine dans $Q(\sqrt{2})$:

donc $X^2-\sqrt{2}X+1$ est le polynôme minimal sur $Q(\sqrt{2})$ de v_1 et $-v_4$

et $X^2+\sqrt{2}X+1$ est le polynôme minimal sur $Q(\sqrt{2})$ de $-v_1$ et v_4

donc le degré sur $Q(\sqrt{2})$ des racines de X^4+1 est 2.

Cas des racines de X^8-X^4+1 :

$X^8-X^4+1=F_1(X)F_1(-X)F_2(X)F_2(-X)$ avec $F_1(X)=X^2-2\cos(\frac{\pi}{12})X+1$ (ses racines sont v_0 et $-v_5$) et $F_2(X)=X^2-2\cos(\frac{5\pi}{12})X+1$ (ses racines sont v_2 et $-v_3$).

C'est la décomposition , dans R, en 4 facteurs irréductibles de X^8-X^4+1.

X^8-X^4+1 est-il réductible dans $Q(\sqrt{2})[X]$? Puisque $\cos\frac{\pi}{12}=\frac{\sqrt{2+\sqrt{3}}}{2}$, $\cos\frac{5\pi}{12}=\frac{\sqrt{2-\sqrt{3}}}{2}$), aucun des $F_i[X]$ est dans $Q(\sqrt{2})[X]$, il faut essayer de regrouper ces F_i deux par deux.

$F_1(X)F_1(-X)=(X^2+1)^2-4\cos^2(\frac{\pi}{12})X^2=(X^2+1)^2-(2+\sqrt{3})X^2$ et le coefficient de X^3 de $F_1(X)F_2(X)$ est $\sqrt{6}$, donc ces deux produits ne sont pas dans $Q(\sqrt{2})[X]$.

Reste $F_1(X)F_2(-X)$.

Compte-tenu des formules $\cos p+\cos q=2\cos\frac{p+q}{2}\cos\frac{p-q}{2}$,

$\cos p-\cos q=-2\sin\frac{p+q}{2}\sin\frac{p-q}{2}$ et $\cos p\cos q=\frac{1}{2}(\cos(p+q)+\cos(p-q))$,

$F_1(X)F_2(-X)=X^4+\sqrt{2}X^3+X^2+\sqrt{2}X+1$, produit qui est dans $Q(\sqrt{2})[X]$.

Donc, X^8-X^4+1 est réductible dans $Q(\sqrt{2})[X]$, en $(X^4+\sqrt{2}X^3+X^2+\sqrt{2}X+1)(X^4-\sqrt{2}X^3+X^2-\sqrt{2}X+1)$: ces deux facteurs sont-ils eux irréductibles dans $Q(\sqrt{2})[X]$?

Comme $X^4+\sqrt{2}X^3+X^2+\sqrt{2}X+1=F_1(X)F_2(-X)$ et que $F_1(X)$ et $F_2(-X)$ ne sont pas dans $Q(\sqrt{2})[X]$, d'après le 2.1 et 2.2 (en remplacant Q par le corps de réels $Q(\sqrt{2})$), $X^4+\sqrt{2}X^3+X^2+\sqrt{2}X+1$ est irréductible sur $Q(\sqrt{2})$ et donc $X^4-\sqrt{2}X^3+X^2-\sqrt{2}X+1$ aussi (X en $-X$).

Finalement $X^4+\sqrt{2}X^3+X^2+\sqrt{2}X+1$ est le polynôme minimal sur $Q(\sqrt{2})[X]$ de v_0, $-v_5$, $-v_2$, v_3

et $X^4-\sqrt{2}X^3+X^2-\sqrt{2}X+1$ est le polynôme minimal sur $Q(\sqrt{2})[X]$ de $-v_0$, v_5, v_2, $-v_3$.

Donc le degré sur $Q(\sqrt{2})$ des racines de X^8-X^4+1 est 4.

Remarque :

de la factorisation de $X^4+1=(X^2-\sqrt{2}X+1)(X^2+\sqrt{2}X+1)$ on déduit que $X^{12}+1=(X^6-\sqrt{2}X^3+1)(X^6+\sqrt{2}X^3+1)$ et donc puisque $X^{12}+1=(X^4+1)(X^8-X^4+1)$ toute racine de X^4+1 ou de X^8-X^4+1 est racine de $X^6-\sqrt{2}X^3+1$ ou de $X^6+\sqrt{2}X^3+1$.

De cette factorisation on déduit uniquement que le degré de toute racine de $X^{12}+1$ sur

$Q(\sqrt{2})$ est ≤ 6.

Mais ces deux facteurs ne peuvent être irréductibles sur $Q(\sqrt{2})$ puisque le degré de toute racine de $X^{12}+1$ sur $Q(\sqrt{2})$ est 2 ou 4, donc pas 6 : ils doivent être factorisable, dans $Q(\sqrt{2})$, par un second degré.

Effectivement, en s'inspirant des résultats ci-dessus on vérifie que
$X^6-\sqrt{2}X^3+1=(X^2+\sqrt{2}X+1)\left(X^4-\sqrt{2}X^3+X^2-\sqrt{2}X+1\right)$.

annexe 5

Quatre choses sur les racines $n-$ *ièmes* de 1

On note, pour $n \geq 2$, U_n l'ensemble des racines n –ièmes de 1 (groupe cyclique multiplicatif).
Soient n_1 et n_2 deux entiers ≥ 2, d leur pgcd et $n_i' = \frac{n_i}{d}$ et f l'application f de $U_{n_1} \times U_{n_2}$ dans $U_{\frac{n_1 n_2}{d}}$ définie par $f(\xi, \eta) = \xi\eta$.

On a alors les deux résultats suivants :
1) f est surjective et tout élément de $U_{\frac{n_1 n_2}{d}}$ a exactement d antécédents.

2) Si U_n est un groupe multiplicatif,ce n'est pas le cas du point de vue additif :
la somme $\xi_1 + \xi_2$ de deux racines n –ièmes de 1 est une racine $n-$ ième de $1 \Leftrightarrow$ n est un multiple de 6 et $\frac{\xi_1}{\xi_2} = j$ ou j^2.

3) Si n est pair il existe exactement n couples de racines n_ièmes de 1 dont la somme des éléments du couple est 0.

4) Soient quatre racines n –ièmes de 1 : $\xi_1, \xi_2, \xi_3, \xi_4$.
si n est impair, $\xi_1 + \xi_2 = \xi_3 + \xi_4 \Leftrightarrow \{\xi_1; \xi_2\} = \{\xi_3; \xi_4\}$
si n est pair, $\xi_1 + \xi_2 = \xi_3 + \xi_4 \neq 0 \Leftrightarrow \{\xi_1; \xi_2\} = \{\xi_3; \xi_4\}$.

preuve :

preuve 1) f est bien définie car $(\xi\eta)^{\frac{n_1 n_2}{d}} = (\xi^{n_1})^{n_2'}(\eta^{n_2})^{n_1'} = 1 \times 1 = 1$.
Déterminons maintenant le nombre de couples $(\xi, \eta) \in U_{n_1} \times U_{n_2}$ tels que $\xi\eta = 1$.
On a $\xi = e^{\frac{2ik_1\pi}{n_1}}$ et $\eta = e^{\frac{2ik_2\pi}{n_2}}$ avec $k_1 \in \{0; 1; 2; \ldots; n_1 - 1\}$ et $k_2 \in \{0; 1; 2; \ldots; n_2 - 1\}$.
$\xi\eta = 1 \Leftrightarrow \frac{2ik_1\pi}{n_1} + \frac{2ik_2\pi}{n2} = 2iK\pi \Leftrightarrow k_1 n_2 + k_2 n_1 = K n_1 n_2$.
Comme $0 \leq k_1 n_2 + k_2 n_1 < 2n_1 n_2$, c'est que $K = 0$ ou 1.
Si $K = 0$, la seule possibilité est $(k_1, k_2) = (0, 0)$
Si $K = 1$, $k_1 n_2 + k_2 n_1 = K n_1 n_2 \Leftrightarrow k_1 n_1' + k_2 n_1' = d n_1' n_2'$: donc n_i' divise k_i, cad $k_i = \rho_i n_i'$ et ainsi $k_1 n_2 + k_2 n_1 = K n_1 n_2 \Leftrightarrow \rho_1 + \rho_2 = d$.
Mais comme $0 \leq k_i < n_i$, on a $0 \leq \rho_i < d$ et il y a exactement $d - 1$ couples (ρ_1, ρ_2) possibles : $(i, d - i)$ pour $i = 1, 2, \ldots, d - 1$, ce qui donne, pour $K = 1$, exactement $d - 1$ couples (k_1, k_2), soit $d - 1$ couples (ξ, η) tels que $\xi\eta = 1$.
Avec le couple $(\xi, \eta) = (1, 1)$ correspondant à $K = 0$, 1 a donc exactement d antécédents par f.

Cherchons maintenant le nombre d'antécédents par f d'un élément quelconque de $U_{\frac{n_1 n_2}{d}}$.
Un élément quelconque de $U_{\frac{n_1 n_2}{d}}$ est $e^{\frac{2i\lambda d\pi}{n_1 n_2}}$ avec $\lambda \in \{0; 1; \ldots; \frac{n_1 n_2}{d} - 1\}$.
Comme n_1' et n_2' sont premiers entre eux, il existe u et v tels que $u n_1' + v n_2' = 1$, soit $\lambda u n_1 + \lambda v n_2 = \lambda d$.
Ainsi pour $\xi = e^{\frac{2ik_1\pi}{n_1}} \in U_{n_1}$ et $\eta = e^{\frac{2ik_2\pi}{n_2}} \in U_{n_2}$, $\xi\eta = e^{\frac{2i\lambda\pi}{n_1 n_2}} \Leftrightarrow \xi'\eta' = 1$ avec

$\xi' = e^{\frac{2i(k_1-\lambda v)\pi}{n_1}} \in U_{n_1}$ et $\eta' = e^{\frac{2i(k_2-\lambda u)\pi}{n_2}} \in U_{n_2}$.
Et d'après le raisonnement précédent, il y a exatement d couples (ξ', η') possibles, donc 1 a d antécédents (ξ, η) par f. □

preuve 2) Si $n = 6k$ et $\frac{\xi_1}{\xi_2} = j$, $\xi_1 + \xi_2 = \xi_2(1+j) = -\xi_2 j^2$ et $(\xi_1+\xi_2)^{6k} = 1$; même chose si $\frac{\xi_1}{\xi_2} = j^2$ puisque $1 + j^2 = -j$.
Réciproquement, si $\xi_i = e^{i\theta_i}$ sont des racines n –ièmes de 1 telles que $\xi_1 + \xi_2 = \xi_3$, alors $|1 + e^{i(\theta_2-\theta_1)}| = |e^{i(\theta_3-\theta_1)}) = 1$ et $(1+\cos(\theta_2-\theta_1))^2 + (\sin(\theta_2-\theta_1))^2 = 1$, soit $\cos(\theta_2-\theta_1) = -\frac{1}{2} \Leftrightarrow \theta_2 - \theta_1 = \pm\frac{2\pi}{3} + 2K\pi$ et ainsi $e^{i(\theta_2-\theta_1)} = j$ ou j^2.□

preuve 3) Si on note $\xi_1, -\xi_1, \xi_2, -\xi_2, \ldots, \xi_p, -\xi_p$ les $2p$ racines $2p$ –ièmes de 1, il est clair que les couples dont la somme des éléments est 0 ne peuvent être $(\xi_i, -\xi_i)$ ou $(-\xi_i, \xi_i)$. □

preuve 4) Montrons le sens gauche ⇒ droite, l'autre sens étant trivial.
En multipliant l'égalité $\xi_1 + \xi_2 = \xi_3 + \xi_4$ par ξ_1^{-1}, on obtient $1 + \xi_2' = \xi_3' + \xi_4'$ avec $\xi' = e^{i\theta_i'}$.
Or $1 + \xi_2' = 2\cos\frac{\theta_2'}{2} e^{\frac{i\theta_2'}{2}}$ et donc $2\cos\frac{\theta_2'}{2} = s + t$ avec $s = e^{i(\theta_3' - \frac{\theta_2'}{2})}$ et $t = e^{i(\theta_4' - \frac{\theta_2'}{2})}$.
s et t étant de modules 1 et de parties imaginaires opposées ils sont opposés ou conjugués.
Mais $s = -t$ implique $\xi_3' + \xi_4' = 0$, ce qui est exclu par hypothèse dans le cas n pair et est impossible si n est impair ($\xi_3' + \xi_4' = 0$ implique $(-1)^n = 1$).
Donc s et t ont leurs parties réelles égales, soit $2\cos\frac{\theta_2'}{2} = 2\cos(\theta_3' - \frac{\theta_2'}{2})$, d'où

soit $\frac{\theta_2'}{2} = \theta_3' - \frac{\theta_2'}{2} + 2k\pi$ et $\theta_2' = \theta_3' + 2k\pi$ donc $\xi_2' = \xi_3'$, puis $1 = \xi_4'$

soit $\frac{\theta_2'}{2} = -\theta_3' + \frac{\theta_2'}{2} + 2k\pi$ et $\theta_3' = 2k\pi$ donc $1 = \xi_4'$, puis $\xi_2' = \xi_3'$.

Dans les deux cas on a bien $\{\xi_1; \xi_2\} = \{\xi_3; \xi_4\}$. □