Exercice 1. Soit A anneau intègre et soit $f, g \in A[X]$ non constants, avec $\deg(f) = n$, $\deg(g) = m$.

1. Trouver $u, v \in A[X]$, tels que $uf - vg = \mathrm{Res}(f, g)$ et $\deg(u) < m$, $\deg(v) < n$.
2. Soit A factoriel. Montrer que $\mathrm{Res}(f, g) = 0$ ssi f, g possèdent un diviseur commun non constant dans $A[X]$.

Solution 1. Soit $f = a_n X^n + \cdots + a_0$ et $g = b_m X^m + \cdots + b_0$. On commence par rappeler la définition de la matrice M de Sylvester. Soit :

$$\varphi : A[X]_{m-1} \times A[X]_{n-1} \to A[X]_{n+m-1}$$

définie par $\varphi(u, v) = uf + vg$.

Soit K le corps des fractions de A. L'application φ donne lieu à une application K-linéaire

$$\psi : K[X]_{m-1} \times K[X]_{n-1} \to K[X]_{n+m-1}$$

définie aussi par $\psi(u, v) = uf + vg$. On a $\mathrm{Res}(f, g) = \det(\psi)$.

Plus précisément, la matrice M de Sylvester est la matrice de ψ en les bases $(X^{n+m-1}, \ldots, 1)$ et $((X^{m-1}, 0), \ldots, (1, 0), (0, X^{n-1}), \ldots, (0, 1))$.

$$M = (M_{i,j})_{1 \le i,j \le n+m} = \begin{pmatrix} a_n & 0 & & & b_m & 0 & \\ a_{n-1} & a_n & & & \vdots & \ddots & \\ \vdots & & \ddots & & \vdots & & b_m \\ \vdots & & & a_n & \vdots & & \vdots \\ \vdots & & & a_{n-1} & \vdots & & \vdots \\ a_0 & & & \vdots & \vdots & & \vdots \\ & a_0 & & \vdots & b_0 & & \vdots \\ & & \ddots & \vdots & & \ddots & \vdots \\ & & & a_0 & & & b_0 \end{pmatrix}$$

Dans la pratique, on doit écrire en colonne les coefficients de f, puis se déplacer vers la droite et recopier cette même colonne, décalée d'un cran vers le bas, ceci autant de fois que le degré de g. Puis recommencer avec g jouant le rôle de f.

1. Si $\mathrm{Res}(f, g) = 0$, alors $u = v = 0$ conviennent.

   Supposons désormais $\mathrm{Res}(f, g) \neq 0$. Cherchons en $u, v \in A[X]$ dont les coefficients sont fonctions polynomiales des coefficients de f et g, tels que $uf + vg = \mathrm{Res}(f, g)$ et $\deg(u) < m$, $\deg(v) < n$.

   Comme $\mathrm{Res}(f, g) = \det(\psi) \neq 0$, l'application ψ est bijective, donc u, v seront en plus uniques dans $K[X]$ et à fortiori dans $A[X]$.

   Travaillons pour le moment dans $K[X]$. Soit $u = u_{m-1} X^{m-1} + \cdots + u_0$ et $v = v_{n-1} X^{n-1} + \cdots + v_0$ avec u_i et v_j dans K. La condition $\varphi(u, v) = \mathrm{Res}(f, g)$ équivaut à :

$$M \begin{pmatrix} u_{m-1} \\ \vdots \\ u_0 \\ v_{n-1} \\ \vdots \\ v_0 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \mathrm{Res}(f, g) \end{pmatrix}$$

Ceci s'écrit, en coordonnées en la base $(X^{n+m-1},\dots,1)$ de $K[X]_{n+m-1} \simeq K^{n+m}$, sous la forme $M(u,v)^t = \det(M)(0,\dots,0,1)^t$. Comme M est inversible, on a :

$$(u,v)^t = \det(M)M^{-1}(0,\dots,0,1)^t.$$

Or $M^{-1} = \det(M)^{-1}\mathrm{Co}(M)^t$, où $\mathrm{Co}(M)$ est la comatrice de M. Donc on a :

$$\begin{aligned}(u,v)^t &= \det(M)M^{-1}(0,\dots,0,1)^t = \\ &= \det(M)^{-1}\det(M)\mathrm{Co}(M)^t(0,\dots,0,1)^t = \\ &= \mathrm{Co}(M)^t(0,\dots,0,1)^t.\end{aligned}$$

En définitive, $(u,v)^t$ s'obtient comme dernière colonne de la comatrice $\mathrm{Co}(M)^t$. En particulier, les coefficients de la comatrice étant dans A, on a bien $u,v \in A[X]$. Aussi, les coefficients de la comatrice $\mathrm{Co}(M)$ sont fonctions polynomiales de ceux de M, donc des coefficients de f et g, ainsi les coefficients de u,v sont polynomiaux en f,g.

2. Soit A factoriel. Alors $A[X]$ est factoriel. Posons $h = \mathrm{pgcd}(f,g)$ dans $A[X]$.

   Si $\deg(h) > 0$, $u = g/h$ et $v = f/g$ sont éléments de $A[X] \subset K[X]$ et $\deg(u) < m$, $\deg(v) < n$. On a alors $(u,-v) \in \ker(\psi) \setminus \{0\}$. Donc ψ n'est pas injective et $\mathrm{Res}(f,g) = \det(\psi) = 0$.

   Réciproquement il suffit de montrer que, si $\deg(h) = 0$, alors $\mathrm{Res}(f,g) \neq 0$. Supposons pas l'absurde $\mathrm{Res}(f,g) = 0$ et $\deg(h) = 0$. Soit k le ppcm de f et g dans $A[X]$. On a donc $\deg(k) = n+m$, car $\deg(h) = 0$. Comme $\mathrm{Res}(f,g) = \det(\psi) = 0$, il existe $(U,-V) \in \ker(\psi) \setminus \{0\}$ donc $U,V \in K[X]$ non nuls, $\deg(U) < m$, $\deg(V) < n$ et $Uf = gV$. En multipliant U et V par le ppcm c des coefficients non nuls de U et V on obtient $u = cU$ et $v = cV$, polynômes dans $A[X]$. On a $uf = gv$ et ce polynôme est un multiple de f et g donc $k \mid uf$. Ainsi, $\deg(uf) = \deg(u) + n = \deg(U) + n \geq n+m$. Mais $\deg(U) < m$: c'est absurde.

Exercice 2. Soient $A = \mathbb{Z}[a_0,a_1,\dots,a_n,b_0,b_1,\dots,b_m]$ et posons :

$$\begin{aligned}f &= a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0,\\ g &= b_mX^m + b_{m-1}X^{m-1} + \cdots + b_0.\end{aligned}$$

Montrer que $\mathrm{Res}(f,g) \in A$ est un polynôme homogène de degré $n+m$ en $a_0,\dots,a_n,b_0,\dots,b_m$.

Solution 2. On adoptera la convention suivante : le polynôme nul est homogène de degré a, pour tout $a \in \mathbb{N}$. On développe d'abord la notion de matrice homogène.

Soit B un anneau intègre et $C = B[X_1,\dots,X_N]$. Pour une matrice carrée $M = (M_{i,j})$ de taille ℓ avec $M_{i,j} \in C$ pour tout i,j, on a :

$$\det(M) = \sum_{\sigma\in\mathfrak{S}_\ell} \epsilon(\sigma)M_{\sigma(1),1}\cdots M_{\sigma(\ell),\ell},$$

Pour e et d dans $\mathbb{Z}^\ell$, on dit que M est *homogène* de multidegrés (e,d) si $M_{i,j}$ est un polynôme homogène de degré $d_i - e_j$ en les variables $X = (X_1,\dots,X_p)$. Si M est homogène de multidegrés (e,d) alors $\det(M)$ est homogène de degré $|d| - |e| = \sum_{i=1}^{\ell}(d_i - e_i)$. En effet, pour chaque $\sigma \in \mathfrak{S}_n$ le polynôme $M_{\sigma(1),1}\cdots M_{\sigma(\ell),\ell}$ est homogène (en tant que produit de polynômes homogènes) de degré :

$$\deg(M_{\sigma(1),1}\cdots M_{\sigma(\ell),\ell}) = \sum_{i=1}^{\ell}(d_{\sigma(i)} - e_i) = \sum_{i=1}^{\ell} d_{\sigma(i)} - \sum_{i=1}^{\ell} e_i = |d| - |e|.$$

On sait que, si M est la matrice de Sylvester associée à f et g, alors $\mathrm{Res}(f,g) = \det(M)$. Dans ce cas M est homogène de multidegrés (e,d) en les variables $(a,b) = (a_0,\dots,a_n,b_0,\dots,b_n)$ avec $d = (1,\dots,1)$ et $e = (0,\dots,0)$. Donc $\mathrm{Res}(f,g)$ est homogène de degré $m+n$.

De plus, $\mathrm{Res}(f,g)$ n'est pas le polynôme nul. En effet, pour $n,m>0$ on a $\mathrm{Res}((X-1)^n,X^m)\neq 0$ (en fait $\mathrm{Res}((X-1)^n,X^m)=1$). En effet, la matrice de Sylvester de ces deux polynômes s'écrit :

$$M=\begin{pmatrix} 1 & 0 & & & 1 & 0 & \\ -n & 1 & & & 0 & \ddots & \\ \binom{n}{2} & & \ddots & & \vdots & & 1 \\ \vdots & & & 1 & \vdots & & 0 \\ \vdots & & & -n & \vdots & & \vdots \\ (-1)^n & & & \vdots & \vdots & & \vdots \\ & (-1)^n & & \vdots & 0 & & \vdots \\ & & \ddots & \vdots & & \ddots & \vdots \\ & & & (-1)^n & & & 0 \end{pmatrix}$$

Ainsi, à un signe près, $\mathrm{Res}((X-1)^n,X^m)=\det(M)$ est le déterminant de la sous matrice triangulaire M ci-dessus ayant $(-1)^n$ sur la diagonale : ce déterminant vaut $(-1)^{nm}$. On peut conclure que $\mathrm{Res}((X-1)^n,X^m)=1$, on peut calculer le signe de la même permutation que dans la solution de l'exercice 4 ou alors on peut utiliser l'énoncé de l'exercice 4.

Exercice 3. Soit $A=\mathbb{Z}[\alpha_1,\dots,\alpha_n,\beta_1,\dots,\beta_m,u,v]$ et $B=A[X]$. Posons :

$$f(X)=u(X-\alpha_1)\cdots(X-\alpha_n);$$
$$g(X)=v(X-\beta_1)\cdots(X-\beta_m).$$

Montrer que la partie homogène de plus haut degré en les $\beta_1,\dots,\beta_m$ de $\mathrm{Res}(f,g)$ vaut :

$$u^m v^n(-1)^{nm}(\beta_1\beta_2\cdots\beta_m)^n.$$

Solution 3. Soit $f(X)=\sum_{i=1}^n a_iX^i$ et $g(X)=\sum_{j=1}^m b_jX^j$. On a donc :

$$f(X)=a_nX^n+\cdots+a_0=u(X^n-s_1(\alpha)X^{n-1}+\cdots+(-1)^n s_n(\alpha))$$

Autrement dit, $a_i=u(-1)^{n-i}s_{n-i}(\alpha)$ et $b_j=v(-1)^{m-j}s_{m-j}(\beta)$, on aura posé $s_0=1$.

La matrice de Sylvester prend la forme :

$$M=\begin{pmatrix} u & 0 & & & & v & 0 & \\ -us_1(\alpha) & u & & & & \vdots & \ddots & \\ \vdots & & \ddots & & & \vdots & & v \\ \vdots & & & u & & \vdots & & \vdots \\ \vdots & & & -us_1(\alpha) & & \vdots & & \vdots \\ u(-1)^n s_n(\alpha) & & & \vdots & & \vdots & & \vdots \\ & u(-1)^n s_n(\alpha) & & \vdots & v(-1)^m s_m(\beta) & & & \vdots \\ & & \ddots & \vdots & & & \ddots & \vdots \\ & & & u(-1)^n s_n(\alpha) & & & & v(-1)^m s_m(\beta) \end{pmatrix}$$

Cette matrice est homogène en (α,β) de multidegrés (e,d) où $d=(1,2,\dots,n+m)$ et $e=(1,\dots,m,1,\dots,n)$, donc $d_i=i$, $e_j=j$ si $j\leq m$ et $e_j=j-m$ si $j\geq m+1$. En effet, on a $M_{i,j}$ homogène de degré d_i-e_j. Par exemple comme $e_{m+1}=1$ et $d_1=1$ on a bien que $M_{1,m+1}=v$ est de degré 0 en (α,β).

Maintenant, un terme contribuant à la somme qui exprime le déterminant, développé selon une quelconque ligne, est, si on ignore le signe dû aux inversions, de la forme :

$$u^m(-1)^{i_1+\cdots+i_m}s_{i_1}(\alpha)\cdots s_{i_m}(\alpha)v^n(-1)^{j_1+\cdots+j_n}s_{j_1}(\beta)\cdots s_{j_n}(\beta)$$

avec tous les $i_k\in[\![0,n]\!]$ et $j_\ell\in[\![0,m]\!]$.

Pour avoir degré maximum en (β), i.e. $\sum j_\ell$ maximum, on doit avoir degré minimum en (α), i.e. $\sum i_k=0$. Donc $j_\ell=m$ pour tout ℓ et $i_k=0$ pour tout k.

Le terme en question est donc, si on ignore le signe dû aux inversions :

$$(-1)^{nm}u^m v^n s_m(\beta)^n=(-1)^{nm}u^m v^n(\beta_1\cdots\beta_m)^n.$$

En fait ce terme s'obtient comme produit des coefficients de M apparaissant sur la diagonale principale : il n'y a donc pas d'inversion à prendre en compte. On obtient ainsi le coefficient cherché.

Exercice 4. Soit A anneau intègre, $B = A[\alpha_1, \dots, \alpha_n, u]$ et $g \in A[X]$ de degré $m \geq 1$.

1. Posons $f = u\prod_{i=1}^{n}(X - \alpha_i) \in B[X]$. Montrer que
$$\mathrm{Res}(f, g) = u^m \prod_{i=1}^{n} g(\alpha_i)\,.$$
2. Soit de plus $g = v\prod_{j=1}^{m}(X - \beta_j)$ pour certains $v, \beta_1, \dots, \beta_n \in A$. Montrer que
$$\mathrm{Res}(f, g) = u^m v^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j)\,.$$

Solution 4. Développons une réflexion sur les coefficients dominants de f et g. D'abord, on peut supposer sans restriction $u = 1$ car il est clair que la matrice de Sylvester de (f, g) s'obtient à partir de la matrice de Sylvester de $(\prod(X - \alpha_i), g)$ en multipliant par u les premières m colonnes.

Pour la même raison, on peut supposer g primitif, i.e. de contenu 1 (autrement dit, le pgcd des coefficients de g est 1). En effet, autrement on écrit $g = cg_0$ où g_0 est primitif et c est le contenu de g, et on raisonne sur g_0, sachant que $\mathrm{Res}(f, cg_0) = c^n\mathrm{Res}(f, g_0)$.

Supposons désormais $u = 1$ et g primitif, de sorte qu'aucun facteur irréductible de g n'est constant.

Une autre méthode pour ne pas devoir soucier du terme dominant de g est de remarquer qu'il est suffisant de montrer l'égalité cherchée pour g unitaire. En effet, si $g = b_m X^m + \cdots + b_0$ avec $b_m \neq 0$ alors on peut considérer $G = B_m X^m + \cdots + B_0$ où $B_i = b_i/b_m \in K$, K étant le corps des fractions de A. Les matrices de Sylvester associées à (f, g) et (f, G), définies dans K, différent en ce que les n colonnes contenant les coefficients B_i multipliées par b_0 donnent les n colonnes contenant les b_i. Ainsi, $\mathrm{Res}(f, g) = (b_0)^n\mathrm{Res}(f, G)$.

Donc, si l'égalité est valide pour G unitaire, on a (à priori dans K mais en fait dans A) :
$$\mathrm{Res}(f, g) = (b_0)^n\mathrm{Res}(f, G) = u^m(b_0)^n\prod_{i=1}^{n} G(\alpha_i) = u^m(b_0)^n\prod_{i=1}^{n}\frac{1}{b_0}g(\alpha_i) = u^m\prod_{i=1}^{n} g(\alpha_i).$$

Passons aux questions.

1. Soit $R = \mathrm{Res}(f, g)$. D'après l'exercice 1, il existe $u, v \in A[X]$ tels que $R = uf + vg$. Donc $R = R(\alpha_i) = v(\alpha_i)g(\alpha_i)$ pour tout $i \in [\![1, n]\!]$. Ainsi, $g(\alpha_i) \mid R$ pour toit $i \in [\![1, n]\!]$.

   Soit $i \neq j \in [\![1, n]\!]$. On a $g(\alpha_i) \in A[\alpha_i]$, $g(\alpha_j) \in A[\alpha_j]$ et $A[\alpha_i] \cap A[\alpha_j] = A$, donc aucun facteur irréductible non constant de $g(\alpha_i)$ n'est conjugué à un facteur irréductible non constant de $g(\alpha_j)$. Ainsi, comme g est primitif, les facteurs irréductibles de $g(\alpha_i)$ et $g(\alpha_j)$ sont tous non conjugués (ou plus simplement car g est unitaire si on a fait cette hypothèse, licite d'après ce qui précède). Par factorialité de A on a donc que $\prod_{i=1}^{n} g(\alpha_i)$ divise R.

   Maintenant on montre que $\prod_{i=1}^{n} g(\alpha_i) = R$ car ces polynômes ont tous deux degré nm en (α) et degré n en (b), le premier divise le deuxième, et le coefficient de plus haut degré en les (α) est le même, à savoir :
$$b_m^n s_n(\alpha)^m.$$

   En effet, pour trouver ce terme, on a deux méthodes. Soit on utilise l'exercice 3 puis l'exercice 5 pour intervertir f et g. Soit on calcule directement avec la matrice de Sylvester par la même méthode que l'exercice 3, ce qui donne comme coefficient :
$$\epsilon(\sigma)b_m^n(-1)^{nm}s_n(\alpha)^m,$$
   où σ est la permutation correspondante au produit :
$$M_{n+1,1}M_{n+2,2}\cdots M_{n+m,m}M_{1,m+1}M_{2,m+2}\cdots M_{n,m+n}.$$

Donc $\sigma(i) = n + i$ si $i \in [\![1, m]\!]$ et $\sigma(i) = i - m$ si $i \in [\![m+1, m+n]\!]$. Autrement dit σ est :

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & m & m+1 & m+2 & \cdots & m+n \\ n+1 & n+2 & \cdots & m+n & 1 & 2 & \cdots & n \end{pmatrix}.$$

Si on compte le nombre de désordres dans la deuxième ligne, on obtient nm, car les m termes à gauche sont ordonnés aussi bien que les n termes à droite, et chaque fois que $i \in [\![1, m]\!]$ et $j \in [\![1, n]\!]$ on a $\sigma(i) > \sigma(j + m)$. On a donc $\epsilon(\sigma) = (-1)^{nm}$, comme on voulait.

Une autre façon de déterminer le signe est de calculer le résultant sur des polynômes faciles, par exemple $f = X^n$ et $g = (X-1)^m$.

2. De nouveau, on peut supposer sans perte de généralité que $u = v = 1$. On travaille dans $D = A[\alpha_1, \ldots, \alpha_n, Y_1, \ldots, Y_m]$. On pose $G = \prod_{j=1}^{m}(X - Y_j)$ dans $D[X]$. On souhaite montrer :

$$\mathrm{Res}(f, G) = \prod_{i \in [\![1,n]\!]} \prod_{j \in [\![1,m]\!]} (\alpha_i - Y_j).$$

Cela est suffisant pour répondre à la question, quitte à utiliser la spécialisation $D \to B$ qui envoie, pour tout $j \in [\![1, m]\!]$, la variable Y_j sur β_j (c'est possible, car ce faisant les termes dominants de ces polynômes ne changent pas).

Fixons $i \in [\![1, n]\!]$. On définit $C = A[\alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_n, Y_1, \ldots, Y_m]$, de sorte que $D = C[\alpha_i]$. Soit $R \in \mathrm{Res}(f, G)$. On a $R \in D$. Comme $\alpha_i - Y_j$ est unitaire dans $C[\alpha_i]$, on peut faire la division euclidienne de R par $\alpha_i - Y_j$, ce qui donne (comme $\alpha_i - Y_j$ est de degré 1 en α_i) deux éléments $U \in D = C[\alpha_i]$ et $V \in C$ tels que :

$$R = (\alpha_i - Y_j)U + V.$$

Ici, $R \in D = C[\alpha_i]$ est un polynôme en α_i. On considère, pour $j \in [\![1, m]\!]$ fixé, le morphisme d'évaluation $D \to C$ qui envoie α_i sur Y_j. L'image de R par ce morphisme est $R(Y_j)$ et par spécialisation du résultant ceci coïncide avec $\mathrm{Res}(f_j, G)$ où :

$$f_j(X) = (X - Y_j) \prod_{i \in [\![1,n]\!] \setminus \{j\}} (X - \alpha_i).$$

Maintenant, f_j et G on un facteur commun non constant, à savoir $X - Y_j$, donc $\mathrm{Res}(f_j, G) = 0$. Ainsi $R(Y_j) = 0$. Donc $V = 0$. Nous avons montré que $(\alpha_i - Y_j)$ divise R. En utilisant l'argument déjà évoqué, comme quoi $(\alpha_i - Y_j)$ sont irréductibles pour tout (i, j) et non conjugués si $(i, j) \neq (i', j')$, on obtient que $\prod_{i \in [\![1,n]\!]} \prod_{j \in [\![1,m]\!]} (\alpha_i - Y_j)$ divise R.

Nous savons par ce qui précède que ces polynômes sont de même degré et possèdent même coefficient dominant en les (α), à savoir $s_n(\alpha)^m$. On déduit qu'ils sont égaux.

Exercice 5. Soit A anneau intègre.

1. Soit $f, g \in A[X]$ de degré $n \geq 1$ et $m \geq 1$. Montrer

$$\mathrm{Res}(f, g) = (-1)^{nm}\mathrm{Res}(g, f).$$

2. Soient $f, g_1, g_2 \in A[X]$ non constants. Montrer

$$\mathrm{Res}(f, g_1 g_2) = \mathrm{Res}(f, g_1)\mathrm{Res}(f, g_2).$$

Solution 5. On écrit de nouveau la matrice de Sylvester apparaissant dans le calcul de $\mathrm{Res}(f,g)$, pour $f = a_nX^n + \cdots + a_0$ et $g = b_mX^m + \cdots + b_0$:

$$M = (M_{i,j})_{1\le i,j\le n+m} = \begin{pmatrix} a_n & 0 & & & b_m & 0 & \\ a_{n-1} & a_n & & & \vdots & \ddots & \\ \vdots & & \ddots & & \vdots & & b_m \\ \vdots & & & a_n & \vdots & & \vdots \\ \vdots & & & a_{n-1} & \vdots & & \vdots \\ a_0 & & & \vdots & \vdots & & \vdots \\ & a_0 & & \vdots & b_0 & & \vdots \\ & & \ddots & \vdots & & \ddots & \vdots \\ & & & a_0 & & & b_0 \end{pmatrix}$$

Pour calculer on écrit :

$$M' = (M'_{i,j})_{1\le i,j\le n+m} = \begin{pmatrix} b_m & 0 & & & a_n & 0 & \\ b_{n-1} & b_m & & & \vdots & \ddots & \\ \vdots & & \ddots & & \vdots & & a_n \\ \vdots & & & b_m & \vdots & & \vdots \\ \vdots & & & b_{n-1} & \vdots & & \vdots \\ b_0 & & & \vdots & \vdots & & \vdots \\ & b_0 & & \vdots & a_0 & & \vdots \\ & & \ddots & \vdots & & \ddots & \vdots \\ & & & b_0 & & & a_0 \end{pmatrix}$$

On passe la colonne $(a_m, \ldots, a_0, 0, \ldots, 0)^t$ à gauche par rapport à $(0, \ldots, 0, b_m, \ldots, b_0)^t$, moyennant un changement de signe du déterminant. De même pour les colonnes suivantes, il y en a n au total, lues de la droite vers la gauche. On obtient un signe $(-1)^n$. Cette opération doit être répétée pour les colonnes suivantes contenant des a_i, il y en a m au total. On obtient un signe $((-1)^n)^m = (-1)^{nm}$, comme demandé.

Pour la question suivante, considérons une autre approche au résultant. Soit K le corps des fractions de A. Posons $B = K[X]/(g)$. Il s'agit d'un K-espace vectoriel (en fait d'une K-algèbre) de dimension m, dont une base est $\mathcal{B} = (X^{m-1}, \ldots, 1)$, où on abuse légèrement de la notation en oubliant de noter que nous considérons des classes d'équivalence dans B. Définissons l'application de multiplication par f dans B :

$$\Psi_f : B \to B, \qquad u \mapsto uf.$$

Nous allons montrer que, si g est unitaire, alors $\det(\Psi_f) = \mathrm{Res}(f,g)$. Fixons $j \in [\![1, m]\!]$. La j-ième colonne de la matrice de Sylvester M associée au couple (f,g) est constituée des coefficients de $X^{m-j}f$ en la base $(X^{n+m-1}, \ldots, 1)$. Par division euclidienne de $X^{m-j}f$ par g, il existe Q_j et R_j dans $K[X]$, avec $\deg(R_j) \le m-1$, tels que :

$$X^{m-j}f = Q_jg + R_j.$$

Comme $j \le m-1$ et $\deg(f) = n$, on a $\deg(Q_j) \le n-1$. Ainsi $Q_j = \sum_{k=1}^{n} q_{k,j}X^{n-k}$. Donc la colonne des coefficients de Q_jg en la base $(X^{n+m-1}, \ldots, 1)$ s'écrit comme combinaison linéaire des colonnes de $m+1$ à $m+n$ de M, car ces colonnes sont les coordonnées en la base $(X^{n+m-1}, \ldots, 1)$ de X^ig, pour $i \in [\![0, n-1]\!]$.

On en déduit que $\det(M)$ ne change pas si on remplace la $(j+1)$-ième colonne M_j de M par les coordonnées de $R_j = X^{m-j}f - Q_jg$ en la base $(X^{n+m-1}, \ldots, 1)$. Comme $\deg(R_j) \le m-1$, il existe $r_{1,j}, \ldots, r_{m,j} \in K$ tels que $R_j = \sum_{i=1}^{m} r_{i,j}X^{m-i}$. La matrice M' qu'on obtient en faisant ce remplacement pour tout $j \in [\![1, m]\!]$ prend la forme :

$$M' = \left(\begin{array}{c|c} 0 & N' \\ \hline N & N'' \end{array}\right)$$

avec $N = (r_{i,j})$ et pour certaines matrices N', N'' où N' est triangulaire inférieure avec 1 sur la diagonale. Ainsi,

$$\mathrm{Res}(f,g) = \det(N) = \det\begin{pmatrix} r_{1,1} & r_{1,1} & \cdots & r_{1,m} \\ \vdots & & & \vdots \\ r_{m,1} & r_{m,1} & \cdots & r_{m,m} \end{pmatrix}.$$

Maintenant on remarque que, dans l'algèbre B, on a $\Psi_f(X^j) = R_j = \sum_{i=1}^{m} r_{i,j} X^{m-i}$, donc $N = \mathrm{Mat}_{\mathcal{B}}(\Psi_f)$. Conclusion : $\mathrm{Res}(f,g) = \det(N) = \det(\Psi_f)$.

Pour $f_1, f_2 \in A[X]$ on a $\Psi_{f_1 f_2} = \Psi_{f_2} \circ \Psi_{f_1}$. Par conséquent $\mathrm{Res}(f_1 f_2, g) = \mathrm{Res}(f_1, g)\mathrm{Res}(f_2, g)$.

On obtient le même résultat si on échange les rôles de f et g. Ceci montre que $\mathrm{Res}(f, g_1 g_2) = \mathrm{Res}(f, g_1)\mathrm{Res}(f, g_2)$ si f est unitaire. Par les observations faites précédemment sur l'effet du coefficient dominant de f sur le résultant, on a $\mathrm{Res}(f, g_1 g_2) = \mathrm{Res}(f, g_1)\mathrm{Res}(f, g_2)$ pour tout f.

Exercice 6. On identifie l'ensemble des polynômes unitaires de degré n à coefficients dans $\mathbb{R}$ à l'espace $\mathbb{R}^n$ au moyen de la bijection $X^n + a_1 X^{n-1} + \cdots + a_n \mapsto (a_1, \ldots, a_n)$. Moyennant cette identification, on note $\mu : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^{n+m}$ l'application qui aux polynômes unitaires f et g de degrés respectivement n et m fait correspondre leur produit fg. Comparer le déterminant jacobien de μ au point (f,g) avec le résultant $\mathrm{Res}(f,g)$. En déduire le résultat suivant : si f et g sont premiers entre eux, il existe des voisinages U de f dans $\mathbb{R}^n$, V de g dans $\mathbb{R}^m$ et W de fg dans $\mathbb{R}^{n+m}$ tels que μ induise un difféomorphisme de $U \times V$ sur W. En particulier, pour tout h dans W il existe un unique couple (f,g) dans $U \times V$ tel que $h = fg$.

Solution 6. On écrit les coordonnées $x = (a_1, \ldots, a_n, b_1, \ldots, b_m)$ de $\mathbb{R}^n$. Les coordonnées dans $\mathbb{R}^{n+m}$ du $\mu(f,g)$ prennent la forme :

$$\mu(f,g) = (a_1 + b_1, a_2 + a_1 b_1 + b_2, \ldots, a_k + a_{k-1} b_1 + \cdots + a_1 b_{k-1} + b_k, \cdots, a_n b_m),$$

où $\mu_k = a_k + a_{k-1} b_1 + \cdots + a_1 b_{k-1} + b_k$ est la k-ième coordonnée de μ.

Donc la matrice jacobienne s'écrit :

$$J(\mu)|_{f,g} = \frac{\partial \mu_i}{\partial x_j}(f,g) = \begin{pmatrix} 1 & 0 & & & 1 & 0 & \\ b_1 & 1 & & & a_1 & \ddots & \\ \vdots & & \ddots & & \vdots & & 1 \\ \vdots & & & 1 & \vdots & & a_1 \\ \vdots & & & b_1 & \vdots & & \vdots \\ b_m & & & \vdots & \vdots & & \vdots \\ & b_m & & \vdots & a_n & & \vdots \\ & & \ddots & \vdots & & \ddots & \vdots \\ & & & b_m & & & a_n \end{pmatrix}$$

On retrouve la matrice de Sylvester associée au couple (g,f), donc :

$$\det(J(\mu|_{(f,g)})) = (-1)^{(n+1)(m+1)} \mathrm{Res}(f,g).$$

Maintenant, si f et g sont premiers entre eux alors $\mathrm{Res}(f,g) \neq 0$, donc, comme μ est indéfiniment dérivable en tant que fonction polynomiale, la conclusion se déduit du théorème d'inversion locale.

Exercice 7. On travaille sur $\mathbb{R}[X]$.

1. Calculer le discriminant de $f = X^3 + aX + b$.
2. Soit f un polynôme unitaire à coefficients réels de degré n. Montrer que, si $\mathrm{Discr}(f) > 0$, alors le nombre de racines réelles de f est congru à n modulo 4, et que, si $\mathrm{Discr}(f) < 0$, alors le nombre de racines réelles de f est congru à $n-2$ modulo 4.
3. Discuter le nombre de racines réelles de $f = X^3 + aX + b$ selon les valeurs de a et b.

Solution 7. On a $f'(X) = 3X^2 + a$ donc R le résultat de f et f' vaut :

$$R = \begin{vmatrix} b & 0 & a & 0 & 0 \\ a & b & 0 & a & 0 \\ 0 & a & 3 & 0 & a \\ 1 & 0 & 0 & 3 & 0 \\ 0 & 1 & 0 & 0 & 3 \end{vmatrix} = 27b^2 + 4a^3.$$

Pour la question suivante, on écrit $n = r + 2s$, r étant le nombre de racines réelles :

$$f(X) = \prod_{i=1}^{r}(X - \alpha_i) \prod_{i=1}^{s}(X - \beta_i)(X - \bar{\beta}_i).$$

avec $\alpha_i \in \mathbb{R}$ et $\beta_i \in \mathbb{C} \setminus \mathbb{R}$. Le discriminant D de f s'écrit :

$$D = \prod_{1 \le i < j \le r} (\alpha_i - \alpha_j)^2 \prod_{i \in [\![1,r]\!], k \in [\![1,s]\!]} (\alpha_i - \beta_k)^2 (\alpha_i - \bar{\beta}_k)^2 \prod_{1 \le i < j \le s} (\beta_i - \beta_j)^2 (\bar{\beta}_i - \bar{\beta}_j)^2 \prod_{1 \le i,k \le s} (\beta_i - \bar{\beta}_k)^2.$$

Maintenant, supposons que le discriminant de f soit non nul, donc $(\alpha_i - \alpha_j)^2 > 0$ et $(\alpha_i - \beta_j)^2 (\alpha_i - \bar{\beta}_j)^2 > 0$ car cette expression vaut $|\alpha_i - \beta_j|^4$ étant donné que $\alpha_i = \bar{\alpha}_i$. De même $(\beta_i - \beta_j)^2 (\bar{\beta}_i - \bar{\beta}_j)^2 > 0$. Aussi $(\beta_i - \bar{\beta}_k)^2 (\beta_k - \bar{\beta}_i)^2 > 0$ dès lors que $i \neq k$. En revanche $(\beta_i - \bar{\beta}_i)^2 < 0$. Le signe de D est donc déterminé par le nombre de termes de la forme $(\beta_i - \bar{\beta}_i)^2 < 0$, c'est-à-dire par s dans le sens que ce signe vaut $(-1)^s$.

Pour résumer, en supposant $D \neq 0$, on a $r \equiv n - 2$ modulo 4 ssi s impair ssi $D > 0$ et $4 \mid 2s = n - r$ ssi s pair ssi $D < 0$.

Pour la dernière question, c'est juste une application du résultat précédent. On a :

- Si $a^3 > 27b^2/4$, alors trois racines réelles.
- Si $a^3 < 27b^2/4$, alors une racine réelle.
- Si $a^3 = 27b^2/4$, alors 2 racines réelles ou une. Mais si f n'a qu'une racine α il s'écrit $(X - \alpha)^3$ (car f unitaire) or f n'ayant pas de terme carré on doit avoir $\alpha = 0$. Ceci arrive uniquement pour $a = b = 0$.

Exercice 8. Soit $A = \mathbb{C}[T]$. Soit $p, q, r, s \in A$ avec $q \neq 0 \neq s$ et $\operatorname{pgcd}(p, q) = \operatorname{pgcd}(r, s) = 1$. Considérons le plan affine $\mathbb{C}^2$ et la courbe paramétrée $C \subset \mathbb{C}^2$ définie par :

$$C = \left\{ \left(\frac{p(t)}{q(t)}, \frac{r(t)}{s(t)} \right) \mid t \in \mathbb{C}, q(t) \neq 0 \neq s(t) \right\}.$$

1. Établir une relation entre C et
$$D = \{(x, y) \in \mathbb{C}^2 \mid xq(t) - p(t) = ys(t) - r(t) = 0, \exists t \in \mathbb{C}\}.$$
2. Soit $B = \mathbb{C}[X, Y]$, $f = Xq - p$ et $g = Ys - r$ dans $B[T]$ et posons $R = \operatorname{Res}(f, g) \in B$. Montrer que $(x, y) \in D$ implique $R(x, y) = 0$, sauf pour un nombre fini de valeurs de x et y.
3. Trouver une équation de D lorsque $p = T^2 - 1$, $q = s = T^2 + 1$, $r = 2T$.
4. Soit $\mathbb{P}^2$ le complété projectif de $\mathbb{C}^2$. Trouver l'équation d'une courbe $\hat{D} \subset \mathbb{P}^2$ dont la partie affine est D puis décrire une paramétrisation $\mathbb{P}^1 \to \hat{D}$.

Solution 8. On utilise le résultant pour donner une idée de la théorie de l'élimination.

1. Soit $(x, y) \in C$. Il existe alors $t \in \mathbb{C}$ tel que $q(t) \neq 0 \neq s(t)$ et $x = p(t)/q(t)$, $y = r(t)/s(t)$. Donc $xq(t) = p(t)$ et $ys(t) = r(t)$. Ainsi, $(x, y) \in D$. Nous avons montré $C \subset D$.

   Soit $(x, y) \in D$. Il existe alors $t \in \mathbb{C}$ tel que $xq(t) = p(t)$ et $ys(t) = r(t)$. Remarquons que, si $q(t) = 0$, alors $0 = xq(t) = p(t)$ donc p et q ont une racine commune, à savoir t. Mais ceci est exclu car $\operatorname{pgcd}(p, q) = 1$. Donc $q(t) \neq 0$. De même, on a $s(t) \neq 0$. Donc $(x, y) \in C$. Autrement dit $D \subset C$, ce qui montre finalement $C = D$.

2. Soit $n = \deg_T(f)$ et $m = \deg_T(g)$. On écrit $f = a_n T^n + \cdots + a_0$ avec $a_i \in \mathbb{C}[X]$ pour tout $i \in [\![0, n]\!]$ et $a_n \neq 0$. De même $g = b_m T^m + \cdots + b_0$ avec $b_i \in \mathbb{C}[Y]$ pour tout $i \in [\![0, m]\!]$ et $b_m \neq 0$. Notons $x_1, \ldots, x_n \in \mathbb{C}$ les racines de f_n et $y_1, \ldots, y_m \in \mathbb{C}$ les racines de g_m dans $\mathbb{C}$.

   Pour $x, y \in \mathbb{C}$, $f_x = xq - p$ et $g_y = ys - r$, polynômes dans $\mathbb{C}[T]$. Pour $x \in \mathbb{C} \setminus \{x_1, \ldots, x_n\}$ et $y \in \mathbb{C} \setminus \{y_1, \ldots, y_m\}$ on peut appliquer la spécialisation du résultant et obtenir $R(x, y) = \mathrm{Res}(f_x, g_y)$.

   Maintenant, soit $(x, y) \in D$, avec $x \in \mathbb{C} \setminus \{x_1, \ldots, x_n\}$ et $y \in \mathbb{C} \setminus \{y_1, \ldots, y_m\}$. Il existe alors $t \in \mathbb{C}$ tel que $xq(t) = p(t)$ et $ys(t) = r(t)$, i.e. tel que $f_x(t) = 0$ et $g_y(t) = 0$. Donc $\mathrm{Res}(f_x, g_y) = 0$. Par ce qui précède, on conclut $R(x, y) = 0$. Notons $E = \{(x, y) \in \mathbb{C}^2 \mid R(x, y) = 0\}$. On a montré que, si $x \in \mathbb{C} \setminus \{x_1, \ldots, x_n\}$ et $y \in \mathbb{C} \setminus \{y_1, \ldots, y_m\}$, alors $(x, y) \in D$ implique $(x, y) \in E$.

   On peut argumenter aussi que, si $(x, y) \in \mathbb{C}^2$, avec $x \in \mathbb{C} \setminus \{x_1, \ldots, x_n\}$ et $y \in \mathbb{C} \setminus \{y_1, \ldots, y_m\}$, alors $(x, y) \in E$ implique $(x, y) \in D$. En effet, si $R(x, y) = R(f_x, g_y) = 0$ alors f_x et g_y ont un facteur commun non constant. Donc f_x et g_y admettent une racine commune t, car $\mathbb{C}$ est algébriquement clos. Donc il existe $t \in \mathbb{C}$ tel que $xq(t) = p(t)$ et $ys(t) = r(t)$, ainsi $(x, y) \in D$.

3. On écrit $f = X(T^2 + 1) - T^2 + 1 = T^2(X - 1) + X + 1$ et $g = Y(T^2 + 1) - 2T = YT^2 - 2T + Y$.

$$\mathrm{Res}(f, g) = \det \begin{pmatrix} X-1 & 0 & Y & 0 \\ 0 & X-1 & -2 & Y \\ X+1 & 0 & Y & -2 \\ 0 & X+1 & 0 & Y \end{pmatrix} = 4(X^2 + Y^2 - 1).$$

   On trouve $E = \{(x, y) \in \mathbb{C}^2 \mid x^2 + y^2 = 1\}$. Analysons quel lien existe entre E et D.

   — Soit $(x, y) \in \mathbb{C}^2$. Nous avons montré que, si $x \neq 1$ et $y \neq 0$ alors $(x, y) \in C = D$ ssi $(x, y) \in E$.

   — Soit $x = 1$. Alors $(1, y)$ appartient à E ssi $y = 0$. Par contre, $(1, y)$ n'appartient à D pour aucune valeur de y (car $t^2 - 1 \neq t^2 + 1$ quelque soit $t \in \mathbb{C}$).

   — Soit $y = 0$. Alors $(x, 0)$ appartient à E ssi $x = \pm 1$. Aussi, $(x, 0)$ appartient à D ssi $x = -1$ car $y = 0$ implique $t = 0$ donc $x = -1$.

   — En conclusion, E et D coïncident sur tout $\mathbb{C}^2$ hormis pour le point $(1, 0)$ qui appartient à E mais pas à D.

4. On peut homogénéiser l'équation pour trouver le complété dans $\mathbb{P}^2$, donc :

$$\hat{D} = \{(X : Y : Z) \mid X^2 + Y^2 - Z^2 = 0\}.$$

   En effet, $\mathbb{C}^2 = \mathbb{P}^2 \setminus H_\infty$ où $H_\infty = \{(X : Y : Z) \mid Z = 0\}$, cet ouvert affine étant constitué des points de la forme $(X : Y : 1)$. On voit, en posant $Z = 1$, que $\hat{D} \cap \mathbb{C}^2 = D$.

   Pour $q(t) \neq 0 \neq s(t)$ on a, pour $k = \mathrm{ppcm}(q, s)$ et $u = k/q$, $v = k/s$, on a :

$$\left(\frac{p(t)}{q(t)} : \frac{r(t)}{s(t)} : 1 \right) = \left(p(t)u(t) : r(t)v(t) : k(t) \right).$$

   Pour décrire la paramétrisation, on peut homogénéiser la paramétrisation donnée ci-dessus, donc on obtient :

$$\hat{D} = \{(T^2 - S^2 : T^2 + S^2 : 2TS) \mid (T : S) \in \mathbb{P}^1\}$$

Exercice 9. Soit K un corps et $A = K[\alpha_1, \dots, \alpha_n]$, notons L le corps des fractions de A. Soit $M \in \mathrm{M}_n(L)$ la matrice $M = (M_{i,j})_{1 \leq i,j \leq n}$ définie par $M_{i,j} = \alpha_i^{j-1}$ donc :

$$\begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{pmatrix}.$$

1. En raisonnant sur le système linéaire associé à M, montrer que $\det(M) = 0$ ssi $\alpha_i = \alpha_j$ pour un couple $i \neq j$ de $[\![1, n]\!]$.
2. Montrer que $\det(M) = \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i)$.
3. Montrer que, si $P = \prod_{1 \leq i \leq n} (X - \alpha_i) \in L[X]$, le discriminant de P vaut $\det(M)^2$.
4. Soit $S_k = \sum_{i=1}^n \alpha_i^k$. Montrer que le discriminant de P vaut :

$$\det \begin{pmatrix} S_0 & S_1 & S_2 & \cdots & S_{n-1} \\ S_1 & S_2 & \ddots & \cdots & S_n \\ S_2 & \ddots & \ddots & \cdots & S_{n+1} \\ \vdots & & & & \vdots \\ S_{n-1} & \ddots & \ddots & \ddots & S_{2n-2} \end{pmatrix}.$$

Solution 9. Nous allons travailler dans L puis montrer que certaines égalités ont lieu dans A.

1. Soit $\det(M) = 0$. Alors il existe $(a_0, \dots, a_{n-1}) \in L^n \setminus \{0\}$ solution du système :

$$\begin{cases} a_0 + a_1\alpha_1 + \cdots + a_{n-1}\alpha_1^{n-1} = 0 \\ \vdots \\ a_0 + a_1\alpha_n + \cdots + a_{n-1}\alpha_n^{n-1} = 0 \end{cases}$$

   Ainsi, $\alpha_1, \dots, \alpha_n$ sont racines du polynôme $a_{n-1}X^{n-1} + \cdots + a_0 \in L[X]$. Comme ce polynôme est non nul et de degré au plus $n-1$, il ne peut admettre plus que $n-1$ racines distinctes, donc $\alpha_i = \alpha_j$ pour au moins un couple $(i, j) \in [\![1, n]\!] \times [\![1, n]\!]$ avec $i \neq j$.

   Réciproquement, si $\alpha_i = \alpha_j$ pour un couple $(i, j) \in [\![1, n]\!] \times [\![1, n]\!]$ avec $i \neq j$, alors le colonnes i et j de la matrice M sont égales donc $\det(M) = 0$.

2. Une première méthode consiste à procéder par factorialité. D'abord, la matrice M est homogène en $(\alpha) = (\alpha_1, \dots, \alpha_n)$ de multidegrés (e, d) avec $d_i = n-1$ et $e_j = n-j$ pour $i, j \in [\![1, n]\!]$. Donc $D = \det(M)$ est un polynôme homogène en (α) de degré $\sum_{j=0}^{n-1} j = n(n-1)/2$. On voit que le coefficient dominant de D en α_n est 1 car le terme de degré maximum en α_n dans de développement de $\det(M)$ s'obtient comme produit des coefficients sur la diagonale de M.

   Pour $i \in [\![1, n]\!]$ fixé, on pose $B = A[\alpha_1, \dots, \alpha_{i-1}, \alpha_{i+1}, \dots, \alpha_n]$ et on regarde D comme élément de $A = B[\alpha_i]$. Pour $i \neq j \in [\![1, n]\!]$ on peut diviser D par $\alpha_i - \alpha_j$ et obtenir $D = U(\alpha_i - \alpha_j) + V$ avec $V \in B$. Comme $D(\alpha_j) = 0$ d'après la question précédente, on trouve $V = 0$, donc $\alpha_i - \alpha_j$ divise D. Comme $\alpha_i - \alpha_j$ sont irréductibles non conjugués de A pour tout couple $i \neq j$ dans $[\![1, n]\!]$, on voit que $\prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i)$ divise D puis que ces polynômes sont égaux en comparant les degrés et les coefficients dominants en α_n.

   Une autre méthode consiste à effectuer des opérations sur les colonnes de M. Soit C_j la j-ième colonne de M. C'est long mais non sans intérêt. On continue d'appeler C_j la j-ième colonne de chaque étape de l'algorithme de Gauss.

I) La colonne C_1 est laissée inchangée. Par contre on remplace $C_2 \leftarrow C_2 - \alpha_1 C_1$, puis $C_j \leftarrow C_j - \alpha_1^{j-1} C_1$, pour $j \in [\![2, n]\!]$ pour obtenir :

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & \alpha_2 - \alpha_1 & \alpha_2^2 - \alpha_1^2 & \cdots & \alpha_2^{n-1} - \alpha_1^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_n - \alpha_1 & \alpha_n^2 - \alpha_1^2 & \cdots & \alpha_n^{n-1} - \alpha_1^{n-1} \end{pmatrix}.$$

II) Définissons pour p, q entiers le polynôme symétrique $T_q(X_1, \ldots, X_p)$, somme de tous les monômes distincts de degré q en $X_1, \ldots, X_p$ pris avec coefficient 1. Autrement dit :

$$T_q(X_1, \ldots, X_p) = \sum_{1 \le i_1 \le \cdots \le i_p \le q} X_{i_1} \cdots X_{i_p}.$$

Donc la matrice précédente s'écrit aussi :

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & \alpha_2 - \alpha_1 & (\alpha_2 - \alpha_1) T_1(\alpha_1, \alpha_2) & \cdots & (\alpha_2 - \alpha_1) T_{n-2}(\alpha_1, \alpha_2) \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_n - \alpha_1 & (\alpha_n - \alpha_1) T_1(\alpha_1, \alpha_n) & \cdots & (\alpha_n - \alpha_1) T_{n-2}(\alpha_1, \alpha_n) \end{pmatrix}.$$

On remarque la formule suivante :

$$T_q(X_1, \ldots, X_p, Y_1, \ldots, Y_r) = \sum_{\ell=0}^{q} T_\ell(X_1, \ldots, X_p) T_{q-\ell}(Y_1, \ldots, Y_r). \tag{1}$$

III) Posons $T_q = 0$ pour $q < 0$. On fait ensuite, pour $j \in [\![1, n]\!]$, le remplacement suivant :

$$C_j \leftarrow C_j - T_{j-2}(\alpha_1, \alpha_2) C_2.$$

Ceci n'a lieu en pratique que pour $j \in [\![3, n]\!]$ car $T_q = 0$ si $q < 0$. On obtient :

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & \alpha_2 - \alpha_1 & 0 & \cdots & 0 \\ 1 & \alpha_2 - \alpha_1 & (\alpha_3 - \alpha_1)(\alpha_3 - \alpha_2) & \cdots & (\alpha_3 - \alpha_1)(\alpha_3 - \alpha_2) T_{n-3}(\alpha_1, \alpha_2, \alpha_3) \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_n - \alpha_1 & (\alpha_n - \alpha_1)(\alpha_n - \alpha_2) & \cdots & (\alpha_n - \alpha_1)(\alpha_n - \alpha_2) T_{n-3}(\alpha_1, \alpha_2, \alpha_n) \end{pmatrix}.$$

IV) On continue de la sorte, ainsi pour $k \in [\![2, n]\!]$ on passe la k-ième étape de l'algorithme en remplaçant :

$$C_j \leftarrow C_j - T_{j-k+1}(\alpha_1, \ldots, \alpha_{k-1}) C_{k-1}, \qquad \text{pour tout } j \ge k.$$

Les étapes déjà vues correspondent aux cas $k = 2$ et $k = 3$. On passe à l'étape suivante en remplaçant k par $k + 1$.

V) Montrons que, par cet algorithme, on obtient de nouvelles colonnes de la forme :

$$C_j = \left((\alpha_i - \alpha_1) \cdots (\alpha_i - \alpha_{k-1}) T_{j-k}(\alpha_1, \ldots, \alpha_{k-1}, \alpha_i) \right)_{i \in [\![1, n]\!]}. \tag{2}$$

Remarquons aussi que, une fois (2) démontrée, on aura la conclusion $D = \prod_{1 \le i < j \le n} (\alpha_j - \alpha_i)$ car la matrice $(C_1, \ldots, C_n)$ est triangulaire inférieure donc :

$$D = \prod_{j=1}^{n} C_{j,j} = \prod_{i=1}^{n} \prod_{\ell=1}^{i-1} (\alpha_i - \alpha_\ell).$$

VI) La preuve de (2) se fait par récurrence sur k, les cas $k = 1, 2$ étant déjà faits. L'égalité est à montrer seulement pour $i \in [\![k + 1, n]\!]$. Il suffit d'assumer la validité de la formule

jusqu'à l'étape k et de la montrer au rang $k+1$, ce qu'on fait par le calcul suivant. On remplace C_j par $C_j - T_{j-k+1}(\alpha_1,\dots,\alpha_{k-1})C_{k-1}$ donc par :

$$\begin{aligned}
C_j &= \prod_{\ell=1}^{k-1}(\alpha_i-\alpha_\ell)T_{j-k}(\alpha_1,\dots,\alpha_{k-1},\alpha_i) - T_{j-k}(\alpha_1,\dots,\alpha_k)\prod_{\ell=1}^{k-1}(\alpha_i-\alpha_\ell) = \\
&= \prod_{\ell=1}^{k-1}(\alpha_i-\alpha_\ell)\left(T_{j-k}(\alpha_1,\dots,\alpha_{k-1},\alpha_i) - T_{j-k}(\alpha_1,\dots,\alpha_k)\right) = \\
&= \prod_{\ell=1}^{k-1}(\alpha_i-\alpha_\ell)\left(\sum_{\ell=0}^{j-k} T_{j-k-\ell}(\alpha_1,\dots,\alpha_{k-1})(\alpha_i^\ell-\alpha_k^\ell)\right) = \\
&= \prod_{\ell=1}^{k-1}(\alpha_i-\alpha_\ell)\left(\sum_{\ell=0}^{j-k} T_{j-k-\ell}(\alpha_1,\dots,\alpha_{k-1})(\alpha_i-\alpha_k)T_{\ell-1}(\alpha_i,\alpha_k)\right) = \\
&= \prod_{\ell=1}^{k}(\alpha_i-\alpha_\ell)\left(\sum_{\ell=0}^{j-k} T_{j-k-\ell}(\alpha_1,\dots,\alpha_{k-1})T_{\ell-1}(\alpha_i,\alpha_k)\right) = \\
&= \prod_{\ell=1}^{k}(\alpha_i-\alpha_\ell)T_{j-k-1}(\alpha_1,\dots,\alpha_k,\alpha_i),
\end{aligned}$$

où a utilisé l'équation (1). C'est ce qu'il fallait montrer.

3. On passe par l'exercice 4. On a :

$$P'(X) = \sum_{\ell=1}^{n}\prod_{j\in[\![1,n]\!]\setminus\{\ell\}}(X-\alpha_j).$$

Comme $\prod_{j\in[\![1,n]\!]\setminus\{\ell\}}(\alpha_i-\alpha_j)=0$ si $i\neq\ell$, on en obtient :

$$\mathrm{Res}(P,P') = \prod_{i=1}^{n}P'(\alpha_i) = \prod_{i=1}^{n}\sum_{\ell=1}^{n}\prod_{j\in[\![1,n]\!]\setminus\{\ell\}}(\alpha_i-\alpha_j) = \prod_{i=1}^{n}\prod_{j\in[\![1,n]\!]\setminus\{i\}}(\alpha_i-\alpha_j).$$

C'est ce qu'on voulait. En effet comme P est unitaire, son discriminant $\Delta(P)$ vaut :

$$\Delta(P) = (-1)^{\frac{n(n-1)}{2}}\mathrm{Res}(P,P') = (-1)^{\frac{n(n-1)}{2}}\prod_{i=1}^{n}\prod_{j\in[\![1,n]\!]\setminus\{i\}}(\alpha_i-\alpha_j) = \prod_{1\le i<j\le n}(\alpha_j-\alpha_i)^2,$$

le signe étant dû aux $n(n-1)/2$ applications de la formule $(\alpha_i-\alpha_j)(\alpha_j-\alpha_i) = -(\alpha_j-\alpha_i)^2$, chaque application ayant lieu pour le choix d'un couple (i,j) dans $[\![1,n]\!]$ pour $i<j$, et ces couples étant au nombre de $\binom{n}{2} = n(n-1)/2$.

4. Soit N la matrice dont on doit calculer le déterminant. On a :

$$N = (M^t)M,$$

donc $\det(N) = D^2$ est le discriminant de P.

Exercice 10. Soient K un corps, $M\in \mathrm{GL}_n(K)$ et $v\in K^n$ un vecteur. Montrer que l'unique solution $X = {}^t(x_1,\dots,x_n)$ de l'équation $MX = v$ est donnée par

$$x_i = \frac{\det(M_i)}{\det(M)}, \quad 1\le i\le n,$$

où M_i est la matrice obtenue à partir de M en remplaçant la i-ème colonne par v.

Solution 10. Soit $M = (a_{i,j})$, donc :

$$M = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ \vdots & & & \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix}$$

Notons $N = (b_{i,j})$ la comatrice $\mathrm{Co}(M)$:

$$b_{i,j} = (-1)^{i+j} \det \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,j-1} & a_{1,j+1}\cdots & a_{1,n} \\ \vdots & & & & & \\ a_{i-1,1} & a_{i-1,2} & \cdots & a_{i-1,j-1} & a_{i-1,j+1}\cdots & a_{i-1,n} \\ a_{i-1,1} & a_{i+1,2} & \cdots & a_{i+1,j-1} & a_{i+1,j+1}\cdots & a_{i+1,n} \\ \vdots & & & & & \\ a_{n,1} & a_{n,2} & \cdots & a_{n,j-1} & a_{n,j+1}\cdots & a_{n,n} \end{pmatrix}$$

On peut écrire m_1 vecteur colonne de M et e_i vecteur de la base canonique $(e_1, \ldots, e_n)$. Puis $A_i = (e_1, \ldots, e_{i-1}, X, e_{i+1}, \ldots, e_n)$. Donc :

$$MA_i = (m_1, \ldots, m_{i-1}, MX, m_{i+1}, \ldots, m_n) = M_i.$$

Ceci implique $\det(M)\det(A_i) = \det(M_i)$ donc $\det(A_i) = \det(M_i)/\det M$ sachant que M est inversible. Ensuite, on a clairement $x_i = \det(A_i)$.

Exercice 1. Soient $K \subset L$ une extension de corps et $\alpha \in L$.

1. Montrer que :
$$K(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} \middle| f, g \in K[X], g(\alpha) \neq 0 \right\}.$$

Soit $K = \mathbb{C}$, $L = \mathbb{C}(T)$ puis $\alpha_1 = T^2$, $K_1 = \mathbb{C}(\alpha_1)$, $\alpha_2 = T^2 - 2T$ et $K_2 = \mathbb{C}(\alpha_2)$. Posons $K_0 = K_1 \cap K_2$.

2. Montrer que L est algébrique sur K_1 et sur K_2.
3. Soit $\alpha \in K_0$. Utiliser $h_1, h_2 \in L$ tels que $h_1(T^2) = \alpha(T) = h_2(T^2 - 2T)$ pour montrer :
$$\alpha(-T) = \alpha(T), \qquad \alpha(2 - T) = \alpha(T), \qquad \text{puis :} \qquad \alpha(T) = (T + 2).$$
4. Montrer que, si $z_0 \in \mathbb{C}$ est un zéro de $z \mapsto \alpha(z)$, alors $z_0 + 2$ en est un autre. Déduire $K_0 = \mathbb{C}$.
5. Conclure que l'intersection d'extensions algébriques ne l'est pas forcément.

Solution 1. Rappelons que $K[\alpha]$ est le plus petit sous anneaux de L contenant α et K tandis que $K(\alpha)$ est le plus petit sous corps de L contenant α et K. On a $K[\alpha] \subset K(\alpha)$, avec égalité ssi α algébrique.

1. Notons :
$$A = \left\{ \frac{f(\alpha)}{g(\alpha)} \middle| f, g \in K[X], g(\alpha) \neq 0 \right\}.$$
   - On a, pour tout $f, g \in K[X]$, des éléments $f(\alpha), g(\alpha) \in K[\alpha]$. Ainsi, si $g(\alpha) \neq 0$, alors $f(\alpha)/g(\alpha) \in K(\alpha)$. Nous avons montré $A \subset K(\alpha)$.
   - Par ailleurs, A contient α et K. De plus, A est un sous corps de L puisque, pour $r_1 = f_1(\alpha)/g_1(\alpha)$ et $r_2 = f_2(\alpha)/g_2(\alpha)$ éléments de A, on a :
$$r_1 r_2 = \frac{f_1(\alpha) f_2(\alpha)}{g_2(\alpha) g_2(\alpha)} \in A, \qquad r_1 + r_2 = \frac{f_1(\alpha) g_2(\alpha) + f_2(\alpha) g_1(\alpha)}{g_2(\alpha) g_2(\alpha)} \in A,$$
     car $g_1(\alpha) g_2(\alpha) \neq 0$. De plus, si $r_1 \neq 0$ alors $1/r_1 = g_1(\alpha)/f_1(\alpha)$ appartient à A car $f_1(\alpha) \neq 0$.
   - Ainsi A est un sous corps de L contenant K et α, il contient donc le plus petit de ces sous corps, i.e. $K(\alpha)$. Donc $K(\alpha) \subset A$. Finalement, $A = K(\alpha)$.
2. Comme $L = K(T)$, il suffit de montrer que T est algébrique sur K_1 et K_2. Il s'agit de trouver un polynôme annulateur p_i en T à coefficients dans K_i. Pour K_1, on a $K_1 = \mathbb{C}(\alpha_1) \subset \mathbb{C}(T)$, avec $\alpha_1 = T^2$. On considère $p_1(X) = X^2 - \alpha_1 \in K_1[X]$. Alors $p_1(T) = T^2 - \alpha_1 = 0$, donc p_1 convient. Pour K_2, on a $\alpha_2 = T^2 - T$ donc si on pose $p_2(X) = X^2 - X - \alpha_2$ on trouve $p_2(T) = T^2 - T - \alpha_2 = 0$, donc T est algébrique sur $K_2 = \mathbb{C}(\alpha_2)$.
3. Rappelons que $L = \mathbb{C}(T)$.
   - Comme $\alpha \in K_1 = \mathbb{C}(T^2)$, on a $\alpha = h_1(T^2)$. pour un certain $h_1 = f_1/g_1$ où $f_1(X), g_1(X) \in \mathbb{C}[X]$ avec $g_1(T) \neq 0$.
   - De même $\alpha \in K_2 = \mathbb{C}(T^2 - 2T)$, donc $\alpha = h_2(T^2 - 2T)$ pour un certain $h_2 = f_2/g_2$ où $f_2(X), g_2(X) \in \mathbb{C}[X]$ avec $g_2(T^2 - 2T) \neq 0$.
   - Ainsi $\alpha = \alpha(T) = h_1(T^2)$ et $\alpha(-T) = h_1((-T)^2) = h_1(T^2) = \alpha_1(T)$. De même $\alpha = \alpha(T) = h_2(T^2 - 2T)$ donne :
$$\alpha(2 - T) = h_2((2 - T)^2 - 2(2 - T)) = \alpha_2(T).$$

— On en obtient :

$$\alpha(T+2) = \alpha(2-(-T)) = \alpha(-T) = \alpha(T).$$

4. Si $\alpha(z_0) = 0$ alors $\alpha(z_0+2) = \alpha(z_0) = 0$. Soit alors $\alpha = f(T)/g(T) \in K_0 \subset \mathbb{C}(T)$, donc $f, g \in \mathbb{C}[X]$ et $g(T) \neq 0$. Supposons $\deg(f) > 0$. Alors, comme $\mathbb{C}$ est algébriquement clos, il existe $z_0 \in \mathbb{C}$ tel que $f(z_0) = 0$. Ainsi, du fait que $\alpha(z_0+2) = 0$ on déduit que z_0+2 est racine de f et par conséquent f admet pour racine tous les points de la forme z_0+2k, $k \in \mathbb{N}$, hormis éventuellement pour les valeurs (en nombre fini) de k telles que $g(z_0+2k) = 0$. Comme f ne possède qu'un nombre fini de racines, cela n'est pas possible.

   Nous avons exclu le cas $\deg(f) > 0$, donc f doit être constante. On considère maintenant $\alpha' = 1/\alpha = g/f$, bien sûr $f(T) \neq 0$ (f est une constante). De même on aura $\alpha'(z_0+2) = 0$ dès lors que $\alpha'(z_0) = 0$. On en déduit que g est aussi constante, donc $\alpha = f/g \in \mathbb{C}$. Nous avons montré $K_0 \subset \mathbb{C}$. L'inclusion réciproque est évidente, donc $K_0 = \mathbb{C}$.

5. Les extensions L/K_1 et L/K_2 sont algébriques. Pour $\mathbb{C} = K_0 = K_1 \cap K_2$, l'extension L/K_0 n'est pas algébrique, car T n'est pas algébrique sur $\mathbb{C}$.

Exercice 2. Soit K un corps.

1. Montrer que toute extension de degré fini de K est de type fini.
2. Montrer qu'il existe des extensions de type fini de K qui ne sont pas de degré fini.

Solution 2. Une extension L de K est de type fini s'il existe $\alpha_1, \ldots, \alpha_n \in L$ tels que $L = K(\alpha_1, \ldots, \alpha_n)$. Une extension L de K est de degré fini si $\dim_K(L) < \infty$.

1. Soit L une extension de degré fini de K et soit $(\alpha_1, \ldots, \alpha_n)$ une K-base de L. Alors $L = K(\alpha_1, \ldots, \alpha_n)$, donc L est de type fini. En effet, évidemment $K(\alpha_1, \ldots, \alpha_n) \subset L$. Par ailleurs, tout élément de L s'écrit comme combinaison linéaire de $(\alpha_1, \ldots, \alpha_n)$ à coefficients dans K, donc appartient à $K(\alpha_1, \ldots, \alpha_n)$.
2. Par exemple $L = K(X)$ est de type fini sur K (par définition), mais n'est pas de degré fini sur K, car les éléments $(1, X, \ldots, X^n, \ldots)$ sont libres sur K.

Exercice 3. Soient E, F, L des corps tels que $E \subset L$ et $F \subset L$. On note $E[F] = F[E]$ le sous anneau de L engendré par $E \cup F$ et EF le sous corps de L engendré par $E \cup F$.

1) Montrer que $E[F]$ est formé des éléments de L de la forme

$$a_1 b_1 + \cdots + a_n b_n$$

avec $a_1, \ldots, a_n \in E$ et $b_1, \ldots, b_n \in F$.

2) Montrer que EF est le corps des fractions de $E[F]$.

3) Soit $\alpha, \beta \in L$, et $f, g \in E[X]$ polynômes annulateurs de α, β, avec $n = \deg(g)$. Soit :

$$h(X) = g(Y - X) \in A[X],$$
$$k(X) = X^n g(Y/X) \in A[X],$$
$$\ell(X) = f(X^2 Y) \in A[X].$$

Montrer que $\mathrm{Res}_X(f, h)$ annule $\alpha + \beta$, $\mathrm{Res}_X(f, k)$ annule $\alpha\beta$ et, si $\alpha \neq 0$, alors $\mathrm{Res}_X(f, \ell)$ annule $1/\alpha$.

4) Montrer que, si E et F sont algébriques sur $E \cap F$, alors $E[F] = EF$.

Solution 3. Notons A la partie de L suivante :

$$A = \{a_1 b_1 + \cdots + a_n b_n \mid n \in \mathbb{N}, \forall i \in [\![1, n]\!], a_i \in E, b_i \in F\}.$$

1) On voit que A contient E et F. Un calcul direct montre que, pour tout $a, a' \in A$ on a $a - a' \in A$ et $aa' \in A$. Ainsi A est un sous anneau de L qui contient E et F donc A contient le plus petit parmi ces sous anneaux, à savoir $E[F]$.

   Réciproquement, pour $n \in \mathbb{N}$ fixé et $a_1, \dots, a_n \in E$ et $b_1, \dots, b_n \in F$ on voit que $a = a_1b_1 + \cdots + a_nb_n$ appartient à $E[F]$ car pour chaque $i \in [\![1, n]\!]$ on a $a_i, b_i \in E[E]$ donc $a_ib_i \in E[F]$ donc aussi $a \in E[F]$. Ainsi $A \subset E[F]$ donc finalement $A = E[F]$.

2) Soit B le corps des fractions de $E[F]$. Le corps B contient E et F, donc il contient le plus petit des sous corps de L contenant E et F, i.e. $EF \subset B$. Réciproquement, pour $f, g \in E[F] \times E[F]^*$, on a $f, g \in EF$ donc $f/g \in EF$ car $g \neq 0$. Si on résume, $B \subset EF$. Conclusion, $B = EF$.

3) Soit $\gamma = \alpha + \beta$. Posons $R = \mathrm{Res}_X(h, f) \in K[Y]$. Remarquons que le coefficient dominant en X de $g(Y - X)$ est le même que celui de $g(X)$. Ainsi, $\deg_X(g(\gamma - X)) = \deg_X(g(Y - X))$. La même chose vaut pour f car f ne dépend pas de Y. Par conséquent :

$$R(\gamma) = \mathrm{Res}_X(g(\gamma - X), f(X)).$$

   Maintenant, comme α est racine commune de $f(X)$ et $g(\gamma - X)$, on obtient $\mathrm{Res}_X(g(\gamma - X), f(X)) = 0$. Ainsi, $R(\gamma) = 0$. Nous avons montré que R annule γ.

   De même on pose $\delta = \alpha\beta$ et $S = \mathrm{Res}_X(k, f)$. On obtient que $\deg_X(X^n g(Y/X)) = \deg_X(X^n g(\delta/X))$, puis de même pour f. Ainsi :

$$S(\delta) = \mathrm{Res}_X(X^n g(\delta/X), f(X)).$$

   De nouveau α est racine commune de $f(X)$ et $X^n g(\delta/X)$ donc ce résultant est nul i.e. $S(\delta) = 0$. Pour $1/\alpha$ c'est le même argument.

4) On a $E[F] \subset EF$. Pour l'implication réciproque, on peut utiliser la question précédente. Ou alors on peut raisonner comme suit. Soit $a \in EF$, donc il existe $(b, c) \in E[F] \times E[F]^*$ tels que $a = b/c$.

   Soit $c = a_1b_1 + \cdots + a_nb_n$ pour certains $n \in \mathbb{N}^*$, $a_i \in E$, $b_i \in F$ pour tout $i \in [\![1, n]\!]$. Ainsi, $b \in M = E(b_1, \dots, b_n) \subset EF$. On voit que M est une extension de degré fini de E. En effet, $E(b_1)$ est de degré fini sur E car b_1 est algébrique sur $E \cap F$. De même $E(b_1, b_2)$ est de degré fini sur $E(b_1)$ car b_2 est algébrique sur $E \cap F$. En itérant cette remarque on obtient que M est de degré fini sur E.

   En particulier $E(c) \subset M$ est de dimension finie sur E donc c est algébrique sur E. Ainsi, $E(c) = E[c]$, en particulier $c \in E[F]$. Par conséquent, $a = b/c \in E[F]$. On a donc montré $E[F] = EF$.

Exercice 4. Soient K, E, L trois corps tels que $K \subset E \subset L$.

1) Montrer que $[L : K] < \infty$ ssi $[E : K] < \infty$ et $[L : E] < \infty$.
2) Soit F un corps tel que $K \subset F \subset L$. Montrer que, si $[F : E \cap F] < \infty$, alors $[EF : E] < \infty$.
3) Montrer que, si $[E : E \cap F] < \infty$ et $[F : E \cap F] < \infty$ alors $[EF : E \cap F] < \infty$.
4) Montrer que $[F : E \cap F] \leq [EF : E \cap F]$, $[E : E \cap F] \leq [EF : F]$ et que, si E, F sont algébriques sur $E \cap F$ alors :

$$[EF : K] \leq [F : K][E : K].$$

5) Décrire le cas $[EF : K] = [F : K][E : K]$.

Solution 4. On note $\#A$ le cardinal d'un ensemble A.

1) Soit $(\alpha_i \mid i \in I)$ une K-base de E et $(\beta_j \mid j \in J)$ une E-base de L. Alors le théorème de la base télescopique affirme que $(\alpha_i\beta_j \mid (i, j) \in I \times J)$ est une K-base de L. Le cardinal de cette base est $\#I\#J$, ce qui est fini ssi I et J sont finis.

2) Soit $[F : E \cap F] < \infty$. Il existe alors une $(E \cap F)$-base $(\alpha_1, \dots, \alpha_n) \in F^n$ de F. Un élément de $a \in E[F]$ s'écrit $a = a_1 b_1 + \cdots + a_m b_m$ pour un certain $m \in \mathbb{N}$, et, pour $i \in [\![1, m]\!]$, $a_i \in E$ et $b_i \in F$. Ainsi, il existe $x_{i,j} \in E \cap F$ tels que $b_i = \sum_{j=1}^{n} x_{i,j} \alpha_j$, donc :

$$a = \sum_{j=1}^{n} y_j \alpha_j, \qquad \text{où :} \qquad y_j = \sum_{i=1}^{m} a_i x_{i,j} \in E.$$

Donc $(\alpha_1, \dots, \alpha_n)$ est une famille de $E[F]$ génératrice au-dessus de E.

Par conséquent, tout élément $a \in E[F]^*$ est algébrique sur E donc $E(a) = E[a]$. On en déduit que $E[F] = EF$. Ainsi, $(\alpha_1, \dots, \alpha_n)$ est une famille de EF génératrice au-dessus de E. Comme cette famille a cardinal n, on a $[EF : E] \leq n = [F : E \cap F]$.

3) Soit $(\alpha_1, \dots, \alpha_n) \in E^n$ une $(E \cap F)$-base de E et $(\beta_1, \dots, \beta_\ell) \in F^\ell$ une $(E \cap F)$-base de F. Un élément $a \in E[F]$ s'écrit $a = a_1 b_1 + \cdots + a_m b_m$ pour un certain $m \in \mathbb{N}$, et, pour $i \in [\![1, m]\!]$, $a_i \in E$ et $b_i \in F$. Ainsi, il existe $x_{i,j}$ et $y_{i,k}$ dans $E \cap F$ tels que pour tout $i \in [\![1, m]\!]$ on ait $a_i = \sum_{j=1}^{n} x_{i,j} \alpha_j$ et $b_i = \sum_{k=1}^{\ell} x_{i,k} \beta_k$. Ainsi :

$$a = \sum_{j=1}^{n} \sum_{k=1}^{\ell} z_{j,k} \alpha_j \beta_k, \qquad \text{où :} \qquad z_{j,k} = \sum_{i=1}^{m} x_{i,j} y_{i,k}.$$

Ainsi, $(\alpha_j \beta_k \mid (j,k) \in [\![1, n]\!] \times [\![1, \ell]\!])$ est une famille génératrice de $E[F]$ au-dessus de $E \cap F$.

On en déduit que tout élément a de $E[F]^*$ est algébrique sur $E \cap F$ donc $E \cap F(a) = E \cap F[a]$. Ainsi, $E[F] = EF$, donc ce qui précède montre $[EF : E \cap F] \leq n\ell$, i.e. :

$$[EF : E \cap F] \leq [E : E \cap F][F \cap E \cap F].$$

4) Comme $E \cap F \subset E \subset EF$ et $E \cap F \subset E = F \subset EF$, on a :

$$[EF : E \cap F] = [EF : E][E : E \cap F] \geq [E : E \cap F],$$
$$[EF : E \cap F] = [EF : F][F : E \cap F] \geq [F : E \cap F].$$

Ensuite, soit $(\alpha_i \mid i \in I)$ une K-base de E. Un élément $a \in EF$ s'écrit $a = b/c$ avec $(b, c) \in E[F] \times E[F]^*$. Par l'exercice 3, nous avons $EF = E[F]$, donc $a \in EF$ s'écrit $a_1 b_1 + \cdots + a_m b_m$ pour certains $m \in \mathbb{N}^*$, $a_i \in E$, $b_i \in F$, pour tout $i \in [\![1, m]\!]$. Ainsi, il existe $x_{i,j} \in K$ tels que, pour tout $i \in [\![1, m]\!]$, on ait $a_i = \sum_{j \in I} x_{i,j} \alpha_j$, avec pour tout $i \in [\![1, m]\!]$ fixé, seulement un ensemble fini J_i de valeurs de $j \in I$ donne $x_{i,j} \neq 0$.

Alors $a = \sum_{j \in I} y_j \alpha_j$ où $y_j = \sum_{i=1}^{m} x_{i,j} b_i$. Ainsi, $\alpha_j = 0$ sauf pour un nombre fini de valeurs de $j \in I$, ces valeurs étant contenues dans $\cup_{i=1}^{m} J_i$. On a donc $y_j \in F$ pour tout $j \in I$. Ainsi, $(\alpha_i \mid i \in I)$ est une famille génératrice pour EF au-dessus de F, donc $[EF : F] \leq [E : K]$. On en obtient :

$$[EF : K] = [EF : F][F : K] \leq [E : K][F : K].$$

5) D'après la discussion qui précède, ce cas se produit ssi $[EF : F] = [E : K]$.

Exercice 5. Soit $K = \mathbb{Q}(\alpha)$ où α satisfait l'équation

$$\alpha^3 + \alpha^2 + \alpha + 2 = 0\,.$$

Exprimer $(\alpha^2 + \alpha + 1)(\alpha^2 + \alpha)$ et $(\alpha - 1)^{-1}$ sous la forme suivante, avec $a, b, c \in \mathbb{Q}$:

$$a\alpha^2 + b\alpha + c$$

Solution 5. Le polynôme $f = X^3 + X^2 + X + 2 \in \mathbb{Q}[X]$ est annulateur pour α, unitaire et irréductible. En effet, comme f a degré 3, il suffit de voir que f n'a pas de racine $r = p/q$ dans $\mathbb{Q}$, avec $\mathrm{pgcd}(p, q) = 1$. On sait que, si r était une telle racine alors p divise le terme constant 2 de f et q divise le coefficient dominant 1 de f, donc $r = \pm 2$. Mais ni 2 ni -2 ne sont racines de f.

De cette façon on voit que a, b, c existent, quelque soit l'élément de K choisi, car une $\mathbb{Q}$-base de K est $(1, \alpha, \alpha^2)$, du moment que K est isomorphe à $\mathbb{Q}[X]/(f)$.

Pour le calcul, on a :

$$(\alpha^2+\alpha+1)(\alpha^2+\alpha) = -2\alpha - 2,$$
$$(\alpha-1)^{-1} = -(1/5)\alpha^2 - (2/5)\alpha - 3/5.$$

Pour trouver ces expressions on peut envisager plusieurs méthodes.

— On développe $(\alpha^2+\alpha+1)(\alpha^2+\alpha) = \alpha^4+2\alpha^3+2\alpha^2+\alpha$ puis on remplace α^3 par $-(\alpha^2+\alpha+2)$, α^4 par $-\alpha(\alpha^2+\alpha+2)$ puis on itère ces remplacements jusqu'à obtenir l'expression cherchée.

— On fait la division euclidienne dans $\mathbb{Q}[X]$ de $p = (X^2+X+1)(X^2+X)$ par f, ce qui donne $q \in \mathbb{Q}[X]$ et $r \in \mathbb{Q}[X]_2$ tels que :

$$(X^2+X+1)(X^2+X) = qf + r.$$

De cette façon, $r(\alpha) = a\alpha^2 + b\alpha + c$ est l'expression cherchée.

— Pour $1/(\alpha-1)$, on procède par identification des coefficients et utiliser $\alpha^3 = -(\alpha^2+\alpha+2)$ donc écrire :

$$(a\alpha^2+b\alpha+c)(\alpha-1) = \alpha^2(b-2a) + \alpha(c-b-a) - (2a+c) = 1.$$

Ainsi, on obtient :

$$\frac{1}{\alpha-1} = -\frac{1}{5}(\alpha^2+2\alpha+3).$$

— Sinon, comme f est irréductible et $g = X-1 \in \mathbb{Q}[X]$ n'est pas multiple de f, on peut trouver par l'algorithme d'Euclide $u, v \in \mathbb{Q}[X]$ tels que $uf+vg = 1$. On aura donc $v(\alpha) = (\alpha-1)^{-1}$. Dans ce cas on trouve immédiatement $u = 1/5$ et $v = 1/5(X^2+2X+3)$, ce qui confirme le résultat trouvé précédemment.

Exercice 6. Soient α, β deux éléments algébriques sur un corps K. Soient f, g les polynômes minimaux de α, β sur K, respectivement. On suppose que les degrés de f et g sont premiers entre eux. Montrer que g est un polynôme irréductible dans $K(\alpha)[X]$.

Solution 6. Soit $n = \deg(f)$ et $m = \deg(g)$. Soit $L = K(\alpha, \beta)$. On a $\beta \in L$ de degré $\deg(G)$ sur $K[\alpha]$, où G est le polynôme minimal de β sur $K(\alpha)$. Soit $u = \deg(G)$. On a :

$$[L : K] = [K(\alpha, \beta) : K(\alpha)][K(\alpha) : K] = un.$$

Le polynôme G est un diviseur de g donc comme G et g sont unitaires on a $G = g$ ssi $u = m$ ssi g est irréductible sur $K(\alpha)$.

Or de même $[L : K] = vm$ où v est le degré du polynôme minimal de α sur $K(\beta)$. Ainsi $un = vm$. Comme $\operatorname{pgcd}(m, n) = 1$, on a alors $u = m$ et $v = n$ par factorialité. Ainsi $g = G$ et g est irréductible sur $K(\alpha)$.

Exercice 7. Soit $\zeta = e^{2\pi i/3}$ et $i = e^{2\pi i/2}$. Donner les polynômes minimaux sur $\mathbb{Q}$ des éléments de $\mathbb{C}$ suivants :

$$\zeta\sqrt{2}, \qquad i+\zeta, \qquad \zeta+\sqrt{3}.$$

Solution 7. Pour trouver des polynômes annulateurs des éléments en question on peut utiliser l'exercice 3. Nous montrons ici d'autres méthodes.

On a $\zeta^3 = 1$ donc $X^3 - 1$ est annulateur pour ζ. Puis le facteur $X^2 + X + 1$ est irréductible car de degré 2 sans racines réelles, tandis que $X - 1$ n'est pas annulateur pour ζ, ainsi $X^2 + X + 1$ est le polynôme minimal de ζ.

On sait que $\zeta\sqrt{2}$ appartient à $\mathbb{Q}(\sqrt{2}, \zeta) = \mathbb{Q}(\sqrt{2})(\zeta)$ donc la formule du degré implique que $\deg(\zeta\sqrt{2}) \leq [\mathbb{Q}(\sqrt{2}, \zeta) : \mathbb{Q}] \leq 4$. On calcule les puissances de $\zeta\sqrt{2}$ donc :

$$(\zeta\sqrt{2})^2 = 2\zeta^2, \qquad (\zeta\sqrt{2})^3 = 2\sqrt{2}, \qquad (\zeta\sqrt{2})^4 = 4\zeta.$$

On a $\zeta + \zeta^2 = -1$ donc on voit que :

$$(\zeta\sqrt{2})^4 + 2(\sqrt{2}\zeta)^2 + 4 = 4\zeta + 4\zeta^2 + 4 = 0.$$

Ainsi $f(X) = X^4 + 2X^2 + 4$ est annulateur pour $\sqrt{2}\zeta$. Pour voir qu'il est irréductible, on regarde ses racines, qui sont $\sqrt{2}\xi$, $\sqrt{2}\zeta$, $\sqrt{2}\bar{\xi}$ et $\sqrt{2}\bar{\zeta}$, où $\xi = e^{2i\pi/6}$ est racine primitive sixième de 1 donc $\zeta = \xi^2$. La décomposition de f en irréductibles sur $\mathbb{C}$ s'écrit :

$$f(X) = (X - \sqrt{2}\xi)(X - \sqrt{2}\bar{\xi})(X - \sqrt{2}\zeta)(X - \sqrt{2}\bar{\zeta}).$$

La décomposition en irréductibles sur $\mathbb{R}$ s'écrit donc :

$$f(X) = (X^2 - 2\sqrt{2}X + 2)(X^2 + 2\sqrt{2}X + 2).$$

On voit qu'aucun produit de ces termes de degré 2 n'est à coefficients rationnels, donc par factorialité dans $\mathbb{C}[X]$ on obtient que f est irréductible dans $\mathbb{Q}[X]$.

Pour $i + j$, on propose une méthode d'algèbre linéaire. On sait que le polynôme minimal sur $\mathbb{Q}$ de $i + j$ a degré 2 ou 4 car $M = \mathbb{Q}(i, j)$ est une extension de degré 4 de $\mathbb{Q}$ et $i + j$ est irrationnel. En effet, $[M : \mathbb{Q}] = 2[M : \mathbb{Q}(i)]$ car $i^2 + 1 = 0$ et i n'appartient pas à $\mathbb{Q}$. Puis $[M : \mathbb{Q}(i)] = 2$ car $j^2 + j + 1 = 0$ et j n'appartient pas à $\mathbb{Q}(i)$, en effet $j = -1/2 + i\sqrt{3}/2$ dans $\mathbb{C}$, et comme $(1, i)$ est une $\mathbb{Q}$-base de $\mathbb{Q}(i)$ on devrait avoir $\sqrt{3}/2 \in \mathbb{Q}$, ce qui n'est pas le cas.

Donc un polynôme annulateur de $i + j$ s'écrit $f(X) = a_4X^4 + \cdots + a_0$ avec $a_i \in \mathbb{Q}$ pour $i \in [\![0, 4]\!]$ et :

$$\begin{cases} a_0 - 2a_2 + a_3 + 7a_4 = 0, & \text{pour } 1, \\ a_1 - 4a_3 + 4a_4 = 0, & \text{pour } i, \\ a_1 - a_2 - 3a_3 + 7a_4 = 0, & \text{pour } j, \\ 2a_2 - 3a_3 - 4a_4, & \text{pour } ij. \end{cases}$$

Ceci donne un système linéaire dont la matrice en la base canonique de $\mathbb{Q}[X]_4$ est :

$$M = \begin{pmatrix} 1 & 0 & -2 & 1 & 7 \\ 0 & 1 & 0 & -4 & 4 \\ 0 & 1 & -1 & -3 & 7 \\ 0 & 0 & 2 & -3 & -4 \end{pmatrix}$$

On voit par un pivot de Gauss immédiat que M a rang 4, donc l'espace vectoriel E des solutions de ce système a dimension 1. Or si il existait un polynôme annulateur g de $i + j$ de degré $n < 4$, on aurait cgX^k annulateur de $i + j$, pour $k = 0, \ldots, 4 - n$ et $c \in \mathbb{Q}$. Ces polynômes formant une famille libre, on aurait $\dim(E) > 1$. Ainsi le polynôme minimal de $i + j$ a degré 4. La seule solution de E satisfaisant $a_4 = 1$ donne le polynôme minimal de $i + j$, à savoir :

$$x^4 + 2x^3 + 5x^2 + 4x + 1.$$

Par des arguments similaires on trouve le polynôme minimal sur $\mathbb{Q}$ de $j + \sqrt{3}$, qui s'écrit $x^4 + 2x^3 - 3x^2 - 4x + 13$.

Exercice 8. Montrer qu'un corps fini n'est pas algébriquement clos.

Solution 8. On écrit K corps de cardinal $n \in \mathbb{N}$ comme $K = \{\alpha_1, \ldots, \alpha_n\}$. Ainsi on considère :

$$f(X) = 1 + \prod_{i=1}^{n}(X - \alpha_i).$$

Pour tout $\alpha \in K$ il existe $i \in [\![1, n]\!]$ tel que $\alpha = \alpha_i$, donc $f(\alpha) = 1$. Ainsi f n'a pas de racine dans K, de sorte que K n'est pas algébriquement clos.

Exercice 9. Soient K un corps et $\mathcal{F} = \{f_i\}_{i \in I}$ une famille de polynômes dans $K[X]$.

1. Soient L_1, L_2 deux corps de décomposition de $\mathcal{F}$. Montrer qu'il existe un K-isomorphisme $\sigma : L_1 \to L_2$, c'est-à-dire un isomorphisme de corps σ tel que $\sigma|_K = \mathrm{id}_K$.

2. Soit M une clôture algébrique de K. Montrer que M contient un unique corps de décomposition de $\mathcal{F}$.

Solution 9. Cet exercice dit que deux corps de décomposition sont abstraitement isomorphes et qu'ils sont même égaux si on fixe une clôture algébrique commune.

1. Il existe des clôtures algébriques M_1 et M_2 de L_1 et L_2, ainsi pour $i = 1, 2$ on a M_i corps algébriquement clos, algébrique sur L_i. Comme L_i est algébrique sur K, M_i est aussi une clôture algébrique de K. Il existe donc un K-isomorphisme $\varphi : M_1 \to M_2$.

   Montrons que φ définit un K-isomorphisme de L_1 sur L_2. Comme L_1 et L_2 sont des corps de décomposition de $\mathcal{F}$, il suffit de montrer que, quel que soit $i \in I$, φ envoie une racine $\alpha \in L_1$ de f_i dans L_2 et que φ^{-1} envoie une racine $\beta \in L_2$ de f_i dans L_1. Or ceci est clair, en effet $f_i(\varphi(\alpha)) = f_i(\alpha) = 0$ puisque φ est un K-isomorphisme, donc $\varphi(\alpha) \in M_2$ est racine de f_i et par conséquent $\varphi(\alpha) \in L_2$. Pour β, c'est le même argument.
2. Comme M est algébriquement clos, f_i est scindé sur M donc toutes les racines de f_i appartiennent à M. Ainsi, le sous corps de M engendré par K et la réunion des racines de (f_i), pour tout $i \in I$, est un corps de décomposition de $\mathcal{F}$.

   Montrons que le corps de décomposition de $\mathcal{F}$ dans M est unique. Soient L et N deux corps de décomposition de $\mathcal{F}$ contenus dans M. Alors N et L contiennent K et la réunion des racines de (f_i), pour $i \in I$. Donc N et L contiennent le sous corps F de M engendré par K et les racines en question. Comme N et L sont engendrés sur K par ces racines, on a $N = F = L$.

Exercice 10. Soient K un corps et L une clôture algébrique de K. Soient $\alpha, \beta \in L \setminus K$. Établir l'équivalence des deux conditions suivantes :

i) il existe un K-automorphisme φ de L tel que $\varphi(\alpha) = \beta$;

ii) α et β ont le même polynôme minimal sur K.

Solution 10. On considère $K(\alpha)$ et $K(\beta)$ dans L. Si f et g sont les polynômes minimaux de α et β au-dessus de K, alors on a un isomorphisme :

$$K(\alpha) \simeq K[X]/(f), \qquad K(\beta) \simeq K[X]/(g).$$

La surjection $K[X] \to K(\beta)$ qui envoie X sur β définit une application du quotient $K[X]/(f)$ vers $K(\beta)$ si et seulement si $f(\beta) = 0$, i.e. si et seulement si $g \mid f$. Comme f et g sont irréductibles et unitaires, ceci équivaut à $f = g$. Ainsi, il existe un K-isomorphisme $K(\alpha) \to K(\beta)$ ssi $f = g$.

Passons aux implications. Si il existe un K-automorphisme $\varphi : L \to L$ tel que $\varphi(\alpha) = \beta$ alors φ envoie $K(\alpha)$ sur $K(\beta)$ et comme ces deux espaces vectoriels ont même dimension (finie) et φ est injective, on en obtient un K-isomorphisme φ_0 de $K(\alpha)$ sur $K(\beta)$. D'après ce qui précède, $f = g$.

Réciproquement, soit $f = g$. Ainsi, nous avons montré qu'il existe un K-isomorphisme $\varphi_0 : K(\alpha) \to K(\beta)$ qui envoie α sur β. Le corps L est une clôture algébrique de K et par conséquent des sous corps $K(\alpha)$ et $K(\beta)$ de L.

On regarde alors les deux extensions suivantes, d'abord l'inclusion $i : K(\alpha) \subset L$ et ensuite la composition $j = i \circ \varphi_0 : K(\alpha) \to K(\beta) \to L$. Les deux sont une clôture algébrique de $K(\alpha)$. On sait qu'il existe alors un isomorphisme $\varphi : L \to L$ tel que $\varphi \circ i = j = i \circ \varphi_0$. Ainsi φ convient.

Exercice 11. Soit $P \in K[X]$ un polynôme de degré $n \geq 1$ et $L \supset K$ son corps de décomposition. Montrer que $[L : K]$ divise $n!$.

Solution 11. Par récurrence sur n, et cela pour toute extension de corps. En effet, si $n = 1$ on a $L = K$. Soit $n > 1$ et supposons le résultat valide pour tout degré inférieur à n.

— Soit P irréductible sur K et considérons $\alpha \in L$ une racine de P et le corps $F = K(\alpha) \subset L$. Si on regarde P comme élément de $F[X]$ alors $P(X) = (X - \alpha)Q(X)$ pour un certain polynôme $Q \in F[X]$ de degré $n - 1$. Ainsi, par récurrence $[L : F]$ divise $(n - 1)!$. De plus $[F : K] = n$ car P est irréductible sur K. Ainsi, $[L : K] = [L : F][F : K]$ divise $n!$.

— Soit P réductible donc $P = QR$ avec Q irréductible sur K et de degré $m < n$. Alors le corps de décomposition F de Q sur K est un sous corps de L qui satisfait $[F : K] \mid m!$ par récurrence. De même, L est le corps de décomposition de R sur F donc $[L : F] \mid (m-n)!$. Ainsi :

$$[L : K] = [L : F][F : K] \mid m!(n-m)! \mid n!$$

En effet, $u!v! \mid (u+v)!$, du fait que $\binom{u+v}{v}$ est un entier.

Exercice 12. Soit α un nombre réel tel que $\alpha^4 = 5$.

1. Montrer que $\mathbb{Q}(i\alpha^2)$ est une extension normale de $\mathbb{Q}$.
2. Montrer que $\mathbb{Q}(\alpha + i\alpha)$ est une extension normale de $\mathbb{Q}(i\alpha^2)$.
3. Montrer que $\mathbb{Q}(\alpha + i\alpha)$ n'est pas une extension normale de $\mathbb{Q}$.

Solution 12. Extension normale ssi corps décomposition.

1) L'élément $i\alpha^2$ annule $x^2 + 5$, polynôme de degré 2, donc extension normale (racine et son opposé).
2) L'élément $\alpha + i\alpha$ annule $x^2 - 2i\alpha^2$. Polynôme de degré 2, donc extension normale.
3) Remarquons que ceci revient à donner un exemple de tour d'extensions normales qui n'est pas normale. Posons $\beta = i\alpha^2$ et $\gamma = \alpha + i\alpha$. Donc :

$$y^2 - 2\beta = 0, \qquad \beta^2 + 5 = 0, \qquad \gamma^4 + 20 = 0.$$

Le polynôme $x^4 + 20$ est irréductible sur $\mathbb{Q}$. Il se décompose dans $\mathbb{Q}(i, \gamma)$ de la façon suivante :

$$x^4 + 20 = (x - \gamma)(x + \gamma)(x - i\gamma)(x + i\gamma).$$

Donc l'extension est normale ssi $i\gamma \in \mathbb{Q}(\gamma)$, autrement dit ssi $i \in \mathbb{Q}(\gamma)$. Mais si $i \in \mathbb{Q}(\gamma)$, comme $\gamma = \alpha + i\alpha$ on aurait $\alpha \in \mathbb{Q}(\gamma)$ donc $\mathbb{Q}(i, \alpha) \subset \mathbb{Q}(\gamma)$. Mais ceci est impossible, parce que $[\mathbb{Q}(i, \alpha) : \mathbb{Q}] = 8$, ce que l'on voit par $\mathbb{Q}(i, \alpha) = \mathbb{Q}(\alpha)(i)$ et $i \notin \mathbb{Q}(\alpha)$ car $\mathbb{Q}(\alpha) \subset \mathbb{R}$.

Exercice 13. Décrire les corps de décomposition des polynômes suivants sur $\mathbb{Q}$:

a) $X^2 - 2$;
b) $X^3 - 2$;
c) $X^2 + X + 1$;
d) $X^6 + X^3 + 1$.

Solution 13. Le corps de décomposition K de f est de la forme $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, où les α_i sont les racines du polynôme f.

a) $X^2 - 2$. Dans ce cas, $K = \mathbb{Q}(\sqrt{2})$.
b) $X^3 - 2$. Soit $\alpha = \sqrt[3]{2}$. Le polynôme $f(X) = X^3 - 2$ s'annule en α, et est irréductible sur $\mathbb{Q}$ d'après Eisenstein, donc $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Par contre, cette extension est totalement réelle, donc elle ne peut pas être le corps de décomposition de f. En effet ce dernier contient αj, où $j = e^{2\pi i/3}$. Ensuite, le polynôme minimal de j est $X^2 + X + 1$ et $[\mathbb{Q}(j) : \mathbb{Q}] = 2$. On que $\mathbb{Q}(\alpha, j)$ contient toutes les racines de f, puisque celles-ci sont α, αj et αj^2. Donc $K \subset \mathbb{Q}(\alpha, j)$. De même, K contient ces trois racines, donc K contient α et $j = \alpha j/\alpha$. Ainsi K contient $\mathbb{Q}(\alpha, j)$. Finalement $K = \mathbb{Q}(\alpha, j)$. On a alors $[K : \mathbb{Q}] = 6$.
c) $X^2 + X + 1$. C'est facile, c'est $K = \mathbb{Q}(j)$.
d) $X^6 + X^3 + 1$. On a $f(X) = X^6 + X^3 + 1$ et $f(X^3 - 1) = X^9 - 1 = g(X)$. Les racines de f sont les racines primitives d'ordre 9 de 1. En effet, les racines d'ordre 9 ou 1 sont les racines de g, et le facteur $X^3 - 1$ regroupe les racines qui ne sont pas primitives (d'ordre 3 ou 1). Donc,

si on pose $\alpha = e^{2\pi i/9}$, alors $\mathbb{Q}(\alpha)$ contient toutes les racines de f. Enfin f est irréductible sur $\mathbb{Q}$ d'après Eisenstein, car

$$f(X+1) = X^6 + 6X^5 + 15X^4 + 21X^3 + 18X^2 + 9X + 3.$$

Donc on a $[K : \mathbb{Q}] = 6$.

Exercice 14. Soit K un corps, $f \in K[X]$ de degré trois et L un corps de décomposition de f.

1. Montrer que $[L : K]$ divise 6 puis que f est irréductible ssi $[L : K]$ est multiple de 3.
2. Montrer que $[L : K] = 3$ ssi f est irréductible et son discriminant est un carré de K.
3. Calculer $[L : K]$ si $K = \mathbb{Q}$ et $f = X^3 - 6X^2 + 15X + 11$.
4. Calculer $[L : K]$ si $K = \mathbb{Q}(i)$ et $f = X^3 + 7X - 7i$.

Solution 14. On peut supposer f unitaire sans perte de généralité. Le discriminant de f vaut $\Delta_f = (\alpha_3 - \alpha_2)^2(\alpha_3 - \alpha_1)^2(\alpha_2 - \alpha_1)^2$, $\alpha_1, \alpha_2, \alpha_3$ étant les racines de f dans L.

1. On connaît la réponse d'après les exercices précédents. En tout cas, si f est irréductible alors on a $[K(\alpha_1) : K] = 3$ et $f(X) = (X - \alpha_1)g(X)$ avec $g(X) \in K(\alpha_1)[X]$ de degré 2. Donc $L = K(\alpha_1, \alpha_2)$ avec α_2 racine de g, car $g(X) = (X - \alpha_1)(X - \alpha_3)$ avec $\alpha_3 \in K(\alpha_1, \alpha_2)$, du fait que le quotient de g par $X - \alpha_2$ est unitaire de degré 1.

   Donc si $\alpha_2 \in K(\alpha_1)$ alors $[L : K] = 3$, cette condition étant équivalente à ce que $\Delta_g = (\alpha_3 - \alpha_2)^2$ soit un carré dans $K(\alpha_1)$.

   Autrement, g est irréductible et $[L : K] = 6$. Par ailleurs si f n'est pas irréductible alors soit $L = K$ (si f a ses racines dans K) soit f possède un facteur irréductible de degré 2 et une racine dans K, auquel cas $[L : K] = 2$.

   Quoi qu'il arrive, comme $\Delta_g = (\alpha_3 - \alpha_2)^2$, nous avons la relation :

$$\Delta_f = (\alpha_3 - \alpha_1)^2(\alpha_2 - \alpha_1)^2\Delta_g = (g(\alpha_1))^2\Delta_g.$$

2. Soit Δ_f un carré de K et f irréductible. Si $g(\alpha_1) = 0$ alors g a une racine dans $K(\alpha_1)$ donc $L = K(\alpha_1)$ et $[L : K] = 3$. Sinon, si $g(\alpha_1) \neq 0$, de la relation entre les discriminants de f et g on déduit que Δ_g est un carré de $K(\alpha_1)$. Par conséquent $L = K(\alpha_1)$ et $[L : K] = 3$.

   Réciproquement, soit $[L : K] = 3$. Alors f est irréductible comme nous venons de le voir. De plus nous avons vu que Δ_g est un carré dans $K(\alpha_1)$ et par conséquent, via la relation entre les discriminants de f et g, on voit que Δ_f est un carré de $K(\alpha_1)$.

   Soit alors δ une racine de $X^2 - \Delta_f \in K[X]$ dans une extension de K et considérons $F = K(\delta)$. On a $[F : K] = 2$ ssi Δ_f n'est pas un carré de K, sinon $K = F$. Considérons $G = K(\alpha_1, \delta)$. On a :

$$[G : K] = 3[G : K(\alpha_1)] = [G : F][F : K].$$

   Or comme Δ_f est un carré de $K(\alpha_1)$, le polynôme annulateur $X^2 - \Delta_f$ de δ possède une racine dans $K(\alpha_1)$. Autrement dit, $G = K(\alpha_1)$ et $[G : K] = 3$. Par conséquent, $[F : K] \neq 2$, ainsi $[F : K] = 1$ i.e. $K = F$ et Δ_f est un carré de K.

3. Pour $K = \mathbb{Q}$ et $f = X^3 - 6X^2 + 15X + 11$, on voit que f n'a pas de racine et est donc irréductible sur $\mathbb{Q}$, par exemple en utilisant le fait qu'un racine rationnelle $r = p/q$ avec $\text{pgcd}(p, q) = 1$ doit satisfaire $q = \pm 1$ et $p \mid 11$, or ni 11 ni -11 ne sont racines de f. On calcule le discriminant $\Delta_f = 3^3 \times 17 \times 37$, ce qui n'est pas un carré de $\mathbb{Q}$, donc $[L : K] = 6$.

4. Pour $K = \mathbb{Q}(i)$ et $f = X^3 + 7X - 7i$, on considère l'anneau $\mathbb{Z}[i]$ des entiers de Gauss. On voit que 7 est un irréductible de $\mathbb{Z}[i]$ car sinon $7 = (a + ib)(a - ib) = a^2 + b^2$ pour certains $a, b \in \mathbb{Z}$, or 7 n'est pas somme de deux carrés. Ainsi f est irréductible sur $\mathbb{Z}[i]$, et comme $\mathbb{Q}(i)$ est le corps des fractions de $\mathbb{Z}[i]$, on a aussi f irréductible sur $\mathbb{Q}(i)$. Le discriminant de f vaut 49, ce qui est un carré dans $\mathbb{Q}(i)$, donc $[L : K] = 3$.

Exercice 15. Déterminer le corps de décomposition de $X^3 + 2X + 1$ sur $\mathbb{F}_3$.

Solution 15. D'abord, f est irréductible sur $\mathbb{F}_3$, car f est de degré 3 sans racines dans $\mathbb{F}_3$. Ainsi posons $F = \mathbb{F}_3(\alpha)$ corps de rupture de f sur $\mathbb{F}_3$ donc $f(\alpha) = 0$. On a $F \simeq \mathbb{F}_{27}$. Dans F, on a :

$$f(X) = (X - \alpha)g(X), \qquad \text{avec :} \qquad g(X) = X^2 + \alpha X + \alpha^2 - 1.$$

Le discriminant de ce polynôme est $\Delta = \alpha^2 - 4(\alpha^2 - 1) = 1$. Ainsi, dans F le polynôme g possède les racines :

$$\frac{-\alpha \pm 1}{2} \in F.$$

Ainsi, $F \simeq \mathbb{F}_{27}$ est les corps de décomposition de f. Par ailleurs on aurait pu utiliser l'exercice 14 et le fait que le résultant de f vaut 1 pour conclure également que $\mathbb{F}_3(\alpha)$ est le corps de décomposition de f.

Exercice 16. Soit $f = X^3 - X + 1$ et $\mathbb{F}_q$ un corps à q éléments.

1. Montrer que f est irréductible sur $\mathbb{F}_3$.
2. Montrer que f est irréductible sur $\mathbb{F}_9$.
3. Trouver toutes les racines de f dans $\mathbb{F}_{27}$ puis factoriser f dans $\mathbb{F}_{27}$.

Solution 16. On sait que f est irréductible sur K ssi f n'a pas de racine dans K.

1. On voit que $f(0) = f(1) = f(2) = 1$.
2. Le corps $\mathbb{F}_9$ est une extension quadratique de $\mathbb{F}_3$, donc f reste irréductible sur $\mathbb{F}_9$ par l'exercice 6.
3. Soit L le corps de rupture de f sur $\mathbb{F}_3$. Comme f est irréductible de degré 3 sur $\mathbb{F}_3$, on a $[L : \mathbb{F}_3] = 3$ donc $\mathbb{F}_3$ est un corps à 27 éléments donc $L \simeq \mathbb{F}_{27}$ car tous les corps finis de cardinal donné sont isomorphes. Plus explicitement, si on considère $\mathbb{F}_{27}$ comme corps de décomposition de $X^{27} - X$ sur $\mathbb{F}_3$ alors, comme $\alpha \in L^*$ et $\#L^* = 26$ on a $\alpha^{26} = 1$ donc α est racine de $X^{27} - X$, i.e. $\alpha \in \mathbb{F}_{27}$. Ceci montre $L \subset \mathbb{F}_{27}$ puis $L = \mathbb{F}_{27}$ par égalité des cardinaux.

   De ce fait, L contient aussi les autres racines de f, car $L = \mathbb{F}_{27}$ contient toutes les racines de $X^{27} - X$ et f divise $X^{27} - X$. Ainsi f est scindé sur $\mathbb{F}_{27}$. Pour factoriser f on procède par division euclidienne, ce qui donne :

   $$f(X) = (X - \alpha)(X^2 + \alpha X + \alpha^2 - 1) = (X - \alpha)(X - \alpha - 1)(X - \alpha + 1),$$

   où les racines du polynôme quadratique $X^2 + \alpha X + \alpha^2 - 1$ sont trouvées facilement car son discriminant vaut $\alpha^2 - 4\alpha + 4 = 1$ dans $\mathbb{F}_3$.

Exercice 17. Considérons $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$.

1. Montrer que $f = X^2 - X - 1$ est irréductible sur $\mathbb{F}_3$.
2. Soit α la classe de X dans $\mathbb{F}_9 = \mathbb{F}_3[X]/(f)$. Montrer que α a ordre 8 dans $\mathbb{F}_9^*$.
3. Donner l'ordre et le polynôme annulateur de β pour tout $\beta \in \mathbb{F}_9^*$.

Solution 17. On sait qu'un polynôme de degré 2 est irréductible ssi il n'a pas de racine.

1. On voit que $f(0) = f(1) - 1$, $f(-1) = 1$, donc f est irréductible.
2. On calcule les puissances de α comme suit :

j	1	2	3	4	5	6	7	8
α^j	α	$\alpha+1$	$-\alpha+1$	-1	$-\alpha$	$-\alpha-1$	$\alpha-1$	1

3. Comme $\mathbb{F}_3(\alpha)$ a dimension 2 sur $\mathbb{F}_3$, il s'agit d'un corps de cardinal 9 donc tous ces éléments sont racines de $X^9 - X$. On factorise ce polynôme sur $\mathbb{F}_3$ pour obtenir :

   $$X^9 - X = X(X - 1)(X + 1)(X^2 - X - 1)(X^2 + 1)(X^2 + X - 1).$$

— Les éléments $1, -1$ de $\mathbb{F}_3 \subset \mathbb{F}_9$ sont racines des trois premiers facteurs ci-dessus. Ces éléments ont ordre 1 et 2.

— Les éléments de $\mathbb{F}_9 \setminus \mathbb{F}_3$ sont racines des polynômes restants. On a α racine de f, puis l'autre racine α' de f satisfait $\alpha + \alpha' = 1$ donc $\alpha' = 1 - \alpha$. Ceci aurait pu être obtenu aussi en remarquant que $\alpha^3 = 1 - \alpha$ est racine du polynôme minimal f de α du fait que $x \mapsto x^3$ est le morphisme de Frobenius.

— Les racines $\pm\beta$ de $X^2 + 1$ ont ordre 4 car $\beta^2 = -1$ donc $\beta^4 = 1$ tandis que β n'a pas ordre 1 ou 2 (car on aurait alors $\beta = \pm 1$).

— On sait que $\mathbb{F}_9^*$ est cyclique d'ordre 8, engendré par α et que l'indicatrice d'Euler φ satisfait $\varphi(8) = 4$ donc il existe 4 éléments d'ordre 8 dans $\mathbb{F}_9^*$, à savoir $\alpha, \alpha^3, \alpha^5, \alpha^7$. Ainsi α^5 et $\alpha^7 = (\alpha^5)^3$ sont racines de $X^2 + X - 1$.

Exercice 18. Considérons $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$.

1. Montrer que $f_1 = X^2 - X + 1$ et $f_2 = X^2 + X + 1$ sont irréductibles sur $\mathbb{F}_5$.
2. Justifier que $K_1 = \mathbb{F}_5[X]/(f_1)$ et $K_2 = \mathbb{F}_5[X]/(f_2)$ sont deux corps isomorphes.
3. Trouver un isomorphisme φ explicite $K_1 \to K_2$.
4. Soit α_i la classe de X dans K_i. Dire quel est l'ordre de α_i dans K_i^*.
5. Montrer que $\alpha_2\varphi(\alpha_1)$ engendre K_2^*.
6. En factorisant $X^{25} - X \in \mathbb{F}_5[X]$, dénombrer les polynômes irréductibles de degré 2 sur $\mathbb{F}_5$.

Solution 18. On sait qu'un polynôme de degré 2 est irréductible ssi il n'a pas de racine.

1. On voit que ni f_1 ni f_2 n'ont de racine.
2. Ces deux anneaux sont des corps de rupture de f_1 et f_2, qui sont degré 2 sur $\mathbb{F}_5$ donc de cardinal 25. Ainsi, comme tous les corps finis de cardinal fixé sont isomorphes on a le résultat.
3. Procédons par analyse synthèse. Supposons qu'il existe un K-isomorphisme $\varphi : K_1 \to K_2$. Notons α_i l'image de X dans K_i pour $i = 1, 2$. Il existe $a, b \in \mathbb{F}_5$ tels que $\varphi(\alpha_1) = a\alpha_2 + b$.

   Soit $n \in \mathbb{N}$ et $a_i \in \mathbb{F}_5, \forall i \in [\![0, n]\!]$. Si $f = a_n X^n + \cdots + a_0 \in \mathbb{F}_5[X]$ annule α_1, alors :
   $$0 = \varphi(f(\alpha_1)) = f(\varphi(\alpha_1)).$$
   Ainsi, comme f_1 annule α_1, l'élément $a\alpha_2 + b$ doit aussi annuler f_1. De plus, on a $\alpha_2^2 = -\alpha_2 - 1$. Donc :
   $$0 = a^2\alpha_2^2 + 2ab\alpha_2 + b^2 - a\alpha_2 - b + 1 = b^2 - b + 1 - a^2 + a\alpha_2(-a + 2b - 1).$$
   Ainsi, comme $a \neq 0$ et $(1, \alpha_2)$ est une $\mathbb{Q}$-base de K_2, on obtient $a = 2b - 1$ donc $3b(1 - b) = 0$. Nous avons deux choix possibles donc, à savoir $(a, b) = (-1, 0)$ ou $(a, b) = (1, 1)$ i.e. $\varphi(\alpha_1) = \alpha_2$, ou $\varphi(\alpha_1) = \alpha_2 + 1$. Les inverses de ces morphismes ce calculent facilement.
4. On a $\alpha_2^2 = -2$ et -2 a ordre 4 dans $\mathbb{F}_5^*$ donc α_2 a ordre 8 dans $K_2 \simeq \mathbb{F}_{25}$. On trouve aussi $\alpha_1^3 = \alpha_1(\alpha_1 - 1) = (\alpha_1 - 1) - \alpha_1 = -1$ donc α_1^3 a ordre 2 de sorte que α_1 a ordre 6.
5. On a dit que α_1 a ordre 8 donc il en est de même pour $\varphi(\alpha_1)$, rappelons que α_2 a ordre 6. Ainsi, l'ordre de $\varphi(\alpha_1)\alpha_2$ est le ppcm de 8 et 6, à savoir 24, de sorte que $\varphi(\alpha_1)\alpha_2$ engendre le groupe $\mathbb{F}_{25}^*$.
6. On trouve 5 polynômes de degré 1 dans la factorisation de $X^{25} - X$, dont les racines sont les éléments de $\mathbb{F}_5$. Les autres polynômes sont de degré au moins 2, en fait précisément 2 car tout degré $d > 2$ fournirait un sous corps de $\mathbb{F}_{25}$ de cardinal $5^d > 25$ ce qui est absurde.

   Par ailleurs, si f est un polynôme irréductible unitaire de degré 2 sur $\mathbb{F}_5$ alors l'ensemble de ses racines forme un corps à 25 éléments, donc isomorphe au corps de décomposition de $X^{25} - X$. Ainsi, si α est racine de f, f est le polynôme minimal de α tandis que $X^{25} - X$

annule α de sorte que f divise $X^{25}-X$. Donc les polynômes de degré 2 unitaires irréductibles sur $\mathbb{F}_5$ sont précisément les facteurs de degré 2 unitaires dans la décomposition de $X^{25}-X$.

Comme $\#(\mathbb{F}_{25} \setminus \mathbb{F}_5) = 20$ et que tout polynôme irréductible unitaire de degré 2 est le polynômes unitaire d'exactement deux éléments distincts de $\mathbb{F}_{25} \setminus \mathbb{F}_5$, on a $20/2 = 10$ polynômes unitaires de degré 2 irréductibles sur $\mathbb{F}_5$. Ils sont :

$$\begin{aligned}
X^2 + X + 1 &\quad \text{éléments d'ordre 3,}\\
X^2 - X + 1 &\quad \text{éléments d'ordre 6,}\\
X^2 - 2 &\quad \text{éléments d'ordre 8,}\\
X^2 + 2 &\quad \text{éléments d'ordre 8,}\\
X^2 + 2X - 1 &\quad \text{éléments d'ordre 12,}\\
X^2 - 2X - 1 &\quad \text{éléments d'ordre 12,}\\
X^2 - X + 2 &\quad \text{éléments d'ordre 24,}\\
X^2 - 2X - 2 &\quad \text{éléments d'ordre 24,}\\
X^2 + 2X - 2 &\quad \text{éléments d'ordre 24,}\\
X^2 + X + 2 &\quad \text{éléments d'ordre 24.}
\end{aligned}$$

Exercice 19. Considérons $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ et, pour $n \in \mathbb{N}$, l'ensemble $\mathcal{P}_n$ des polynômes de degré n irréductibles dans $\mathbb{F}_2[X]$.

1. Déterminer $\mathcal{P}_2$.
2. Montrer que :
$$X^{16} + X = (X^4 + X) \prod_{f \in \mathcal{P}_4} f.$$
3. Déterminer tous les éléments de $\mathcal{P}_4$.
4. Montrer que, pour $m \in \mathbb{N}$, on a :
$$X^{2^m} + X = \prod_{d \mid m} \prod_{f \in \mathcal{P}_d} f.$$
5. Déterminer le cardinal de $\mathcal{P}_{16}$.

Solution 19. On rappelle que, en caractéristique 2, il n'y a pas lieu d'indiquer les signes.

1. On a $\mathcal{P}_2 = \{X^2 + X + 1\}$.
2. Les racines de $X^{16} + X$ forment les éléments de $\mathbb{F}_{16}$. Ce corps est une extension de degré 4 de $\mathbb{F}_2$. Ainsi, $\alpha \in \mathbb{F}_{16}$ possède un polynôme minimal de degré 1, 2 ou 4. Pour degré 1 on trouve les polynômes X et $X+1$ dont les racines sont les éléments de $\mathbb{F}_2$. Pour degré 2 on trouve le polynôme $X^2 + X + 1$, dont les racines sont les éléments de $\mathbb{F}_4 \setminus \mathbb{F}_2$, qui annulent $X^4 + X$ donc $X^3 + 1$ donc à fortiori $X^{15} + 1$ et par conséquent $X^{16} + X$. Ces éléments sont donc dans $\mathbb{F}_{16}$ et $X^2 + X + 1$ divise $X^{16} + X$. Les autres facteurs de $X^{16} + X$ ont degré d et on voit $d = 4$ car $d \mid 16$, $d > 4$ donnerait lieu à des extensions de cardinal plus grand que 16 tandis que nous avons déjà traité les facteurs de degré $d = 1, 2$.

   Tous les polynômes de degré n irréductibles sur $\mathbb{F}_2$ (ces polynômes étant unitaires du fait que $\mathbb{F}_2^*$ possède un seul élément) apparaissent une et une seule fois dans la factorisation de $X^{16} + X$. Ils apparaissent au moins une fois car un tel polynôme est minimal pour $\alpha \in \mathbb{F}_{16}$ et tout élément de $\mathbb{F}_{16}$ est racine de $X^{16} + X$. Une seule fois car $X^{16} + X$ est à racines distinctes dans son corps de décomposition (du fait que la dérivée de ce polynôme vaut 1). Ceci montre la formule cherchée.

3. On trouve les polynômes :
$$\mathcal{P}_4 = \{X^4 + X + 1, X^4 + X^3 + 1, X^4 + X^3 + X^2 + X + 1\}.$$

4. Les facteurs irréductibles de $F(X) = X^{2^m} + X$ apparaissent avec multiplicité 1.

   Soit $d \mid m$ et $f \in \mathcal{P}_d$, donc $m = dk$ pour un certain $k \in \mathbb{N}$. Une racine α de f appartient au corps de rupture de f, qui possède 2^d éléments donc est isomorphe à $\mathbb{F}_{2^d}$. Ainsi α est racine de $X^{2^d} + X$, i.e. $\alpha^{2^d} = \alpha$. Donc :
$$\alpha^{2^{2d}} = (\alpha^{2^d})^{2^d} = \alpha^{2^d} = \alpha,$$
   puis, en itérant k fois, $\alpha^{2^m} = \alpha$ donc f divise $X^{2^m} + X$.

   Réciproquement, tout facteur g irréductible unitaire de F a degré $d \mid n$ car une racine α de g engendre un sous corps $\mathbb{F}_2(\alpha)$ de $\mathbb{F}_{2^m}$ de degré d sur $\mathbb{F}_2$, tandis que $\mathbb{F}_{2^m}$ a degré m sur $\mathbb{F}_2$. Nous avons montré que la décomposition en irréductibles de F donne la formule cherchée.

5. Posons $\sigma_p = \#\mathcal{P}_{2^p}$. On a trouvé $\sigma_0 = 2$, $\sigma_1 = 1$. On a alors :
$$\sigma_p = \frac{1}{2^p}\left(2^{2^p} - \sum_{k=0}^{p-1} 2^k \sigma_k\right).$$
   Ceci donne $\sigma_3 = 30$ et $\sigma_4 = 4080$.