Université P. et M. Curie (Paris VI) date de mise à jour: 16/02/2009
Deuxième semestre 2008/2009

Master de sciences et technologies 1ère année - Mention : Mathématiques et applications
Spécialité : Mathématiques Fondamentales MO11 : (12 ECTS)

Quatrième fascicule : 16/02/2009

2.8 Théorie de Galois

Il existe un très grand nombre de références pour cette section § 2.8 et la suivante § 2.9. Il suffit de consulter le catalogue de la bibliothèque avec comme mot clé *Galois*.

Le cours accéléré de DEA par Alain Kraus

http ://www.institut.math.jussieu.fr/m2/aa/dea02-03/Galois.pdf

est accessible en ligne. Les trois premiers chapitres constituent une présentation complète du sujet.

Les deux livres d'algèbre (par Dummit et Foote d'une part, Lang d'autre part) cités au début du polycopié contiennent chacun une section sur le sujet : [5] Chap. 14 et [9] Chap. VI.

L'appendice C de [8] donne un résumé du sujet.

Pour en savoir plus, le Chapitre 5 *Théorie des Corps commutatifs* des *Éléments de Mathématiques* par N. Bourbaki est une des meilleures sources d'information.

Pour des exercices, voir par exemple les deux volumes de Mohamed Ayad dans la collection Ellipses :

- Ayad, Mohamed. - *Théorie de Galois, 122 exercices corrigés niveau I* .Paris : Ellipses, 1997
- Ayad, Mohamed. - *Théorie de Galois 115 exercices corrigés niveau II*, Paris : Ellipses, 1997

ainsi que le livre de Bruno Deschamps

- *Problèmes d'arithmétique des corps et de théorie de Galois*, Hermann, Collection Méthodes 1998.

Une extension algébrique L/K est dite *galoisienne* si elle est normale et séparable. C'est équivalent à dire que pour tout $\alpha \in L$ le nombre de conjugués de α dans L est le degré $[K(\alpha) : K]$ de α sur K.

Soit L/K une extension. On note $\mathrm{Aut}(L/K)$ le groupe des K-automorphismes de L.

Lemme 2.29. *Quand L/K est une extension finie, le groupe* $\mathrm{Aut}(L/K)$ *est fini d'ordre* $\leq [L : K]$.

Démonstration. On écrit $L = K(\alpha_1, \ldots, \alpha_m)$. Un K-automorphisme σ de L est entièrement déterminé par $\big(\sigma(\alpha_1), \ldots, \sigma(\alpha_m)\big) \in L^m$. Pour $1 \leq i \leq m$ soit d_i le degré de α_i sur $K(\alpha_1, \ldots, \alpha_{i-1})$. Ainsi $[L : K] = d_1 \cdots d_m$. Quand σ décrit $\mathrm{Aut}(L/K)$, il y a au plus d_1 valeurs possibles $\sigma(\alpha_1) \in L$ (à savoir les conjugués sur K de α_1 dans L) et quand on impose les valeurs de $\sigma(\alpha_1), \ldots, \sigma(\alpha_{i-1})$, il y a au plus d_i valeurs possibles $\sigma(\alpha_i) \in L$ (les conjugués dans L de α_i sur le corps $K\big(\sigma(\alpha_1), \ldots, \sigma(\alpha_{i-1})\big)$). □

Théorème 2.30. *Soit L/K une extension finie. Alors l'extension L/K est galoisienne si et seulement si le groupe* $\mathrm{Aut}(L/K)$ *est d'ordre égal à* $[L : K]$.

Démonstration. Si l'extension L/K est galoisienne finie, le théorème 2.19 (dans lequel on prend $N = K$) montre que le groupe $\mathrm{Aut}(L/K)$ a $[L : K]$ éléments.

Inversement, si $\mathrm{Aut}(L/K)$ a $[L : K]$ éléments, soit $\alpha_1 \in L$; on peut écrire (comme dans la démonstration du lemme 2.29) $L = K(\alpha_1, \ldots, \alpha_m)$ avec des éléments $\alpha_2, \ldots, \alpha_m$ dans L. L'égalité $|\mathrm{Aut}(L/K)| = d_1 \cdots d_m$ montre en particulier que α_1 a d_1 conjugués sur K dans L, avec $d_1 = [K(\alpha_1) : K]$. Donc l'extension L/K est galoisienne.

□

Soit L/K une extension algébrique et soit $G = \mathrm{Aut}(L/K)$. Pour chaque extension M de K contenue dans L le groupe $\mathrm{Aut}(L/M)$ est un sous-groupe de G. Inversement pour chaque sous-groupe H de G, le sous-ensemble

$$L^H = \{x \in L \ ; \ \sigma(x) = x \text{ pour tout } \ \sigma \in H\}$$

de L est un sous-corps de L contenant K, appelé *sous-corps de L fixé par H.*

$$H = \mathrm{Aut}(L/M) \left(\begin{array}{c} L \\ | \\ M = L^H \\ | \\ K \end{array} \right) G$$

De ces définitions on déduit immédiatement :

Lemme 2.31. *Soit L/K une extension algébrique et soit $G = \mathrm{Aut}(L/K)$. Les deux applications*

$$M \mapsto \mathrm{Aut}(L/M) \quad \text{et} \quad H \mapsto L^H$$

sont décroissantes :

Si H et H' sont des sous-groupes de G avec $H \subset H'$, alors $L^{H'} \subset L^H$.

Si M et M' sont deux extensions de K contenues dans L avec $M' \subset M$, alors

$$\mathrm{Aut}(L/M) \subset \mathrm{Aut}(L/M').$$

$$\left. \begin{array}{c} L \\ | \\ H \left(\begin{array}{c} M = L^H \\ | \\ M' = L^{H'} \end{array} \right) H' \\ | \\ K \end{array} \right\} G$$

Quand L/K est une extension galoisienne, le groupe $\mathrm{Aut}(L/K)$ est appelé *groupe de Galois de L sur K* et noté $\mathrm{Gal}(L/K)$.

Théorème 2.32.

1. *Soient L/k une extension, G un sous-groupe de $\mathrm{Aut}(L/k)$ et K le corps L^G.*

a) *Si G est fini, alors L/K est une extension galoisienne finie de groupe de Galois G.*

b) *Si l'extension L/k est algébrique, alors L/K est une extension galoisienne.*

$$G \left(\begin{array}{c} L \\ | \\ K = L^G \\ | \\ k \end{array} \right.$$

2. *Soit L/K une extension galoisienne de groupe de Galois $G = \mathrm{Aut}(L/K)$. Alors $L^G = K$.*

Démonstration. 1. a) Soit $\alpha \in L$. Soit m le nombre d'éléments de l'ensemble $E = \{\sigma(\alpha)\ ;\ \sigma \in G\}$. Notons $E = \{\alpha_1, \dots, \alpha_m\}$. Le groupe G opère sur E par $(\sigma, \alpha_i) \mapsto \sigma(\alpha_i)$, ce qui signifie que l'application qui à $\sigma \in G$ associe $\alpha_i \mapsto \sigma(\alpha_i)$ est un homomorphisme de G dans le groupe symétrique $\mathfrak{S}_E$.

Le polynôme $P(X) = \prod_{i=1}^m (X - \alpha_i)$ vérifie $\sigma(P) = P$. Par définition de K cela signifie $P \in K[X]$. Comme $P(\alpha) = 0$, on en déduit que α est algébrique sur K. Soit f le polynôme irréductible de α sur K. Comme $P \in K[X]$ s'annule en α, il en résulte que f divise P dans $K[X]$. Mais f s'annule en chaque conjugué de α sur K, donc en chaque élément de E et par conséquent P divise f, donc finalement $P = f$. Cela montre que E a autant d'éléments que le degré de α sur K, donc E est l'ensemble de tous les conjugués de α sur K et l'extension L/K est galoisienne. Nous venons de voir que tout élément de L est de degré $\le |G|$ sur K. Donc L est une extension algébrique de K. De plus, d"après le corollaire 2.21 toute extension finie de K contenue dans L a un degré $\le |G|$; donc L est une extension finie de K et $[L : K] \le |G|$. Mais on a $[L : K] \ge |\mathrm{Aut}(L/K)|$; de plus G est un sous-groupe de $\mathrm{Aut}(L/K)$. Par conséquent $G = \mathrm{Aut}(L/K)$.
1. b) Soit $\alpha \in L$. L'ensemble $E = \{\sigma(\alpha)\ ;\ \sigma \in G\}$ est constitué de conjugués de α sur k, donc est fini. Comme ci-dessus le polynôme irréductible de α sur K est $\prod_{\beta \in E}^m (X - \beta)$. On vérifie ainsi que le nombre de conjugués de α sur K est égal à $[K(\alpha) : K]$. Donc l'extension L/K est galoisienne.
2. Soit d le degré de α sur K. Le polynôme irréductible de α sur K est $\prod_{j=1}^d \big(X - \sigma_j(\alpha)\big)$ où $\sigma_1, \dots, \sigma_d$ sont des éléments de $\mathrm{Aut}(L/K)$ et $\sigma_1(\alpha), \dots, \sigma_d(\alpha)$ sont deux-à-deux distincts. De plus, l'ensemble des $\sigma(\alpha)$ pour σ décrivant $\mathrm{Aut}(L/K)$ est $\{\sigma_1(\alpha), \dots, \sigma_d(\alpha)\}$. Alors $\alpha \in L^{\mathrm{Aut}(L/K)}$ équivaut à $d = 1$, donc à $\alpha \in K$.

□

Du théorème 2.32 (parties 1.b) et 2.) on déduit qu'une extension algébrique L/K est galoisienne si et seulement si $L^{\mathrm{Aut}(L/K)} = K$.

Voici le théorème principal de la théorie de Galois pour les extensions finies ; il affirme que, pour une extension galoisienne finie, la correspondance que nous venons d'introduire entre les extensions intermédiaires et les sous-groupes du groupe de Galois est bijective.

Théorème 2.33 (Théorème de Galois)**.** *Soit L/K une extension galoisienne finie de groupe de Galois $G = \mathrm{Gal}(L/K)$.*

1. *Si M est une extension de K contenue dans L et si on note $H = \mathrm{Aut}(L/M)$, alors L/M est une extension galoisienne de groupe de Galois H et on a*

$$[L : M] = |H| \quad et \quad M = L^H.$$

2. *Si H est un sous-groupe de G et $M = L^H$ le sous-corps de L fixé par H, alors L/M est une extension galoisienne et on a*

$$[L : M] = |H| \quad et \quad H = \mathrm{Gal}(L/M).$$

3. *Si M est une extension de K contenue dans L et si on note H le sous-groupe $\mathrm{Gal}(L/M)$ de G, alors l'extension M/K est galoisienne si et seulement si H est normal dans G. Dans ce cas le groupe de Galois de M/K est isomorphe au quotient G/H.*

Démonstration. 1. L'extension L/M est séparable et normale, donc galoisienne et son groupe de Galois est $H = \mathrm{Aut}(L/M)$. On a $M \subset L^H \subset L$ et l'extension L/L^H est galoisienne finie de groupe de Galois H par le théorème 2.32. Donc $[L : M] = |H|$ et $M = L^H$.

2. Comme $M = L^H$ est un corps intermédiaire $K \subset M \subset L$, l'extension L/M est galoisienne de groupe de Galois $\mathrm{Aut}(L/M)$. Le théorème 2.32 montre que l'extension L/L^H est galoisienne finie de groupe de Galois H. Comme $M = L^H$ on en déduit $H = \mathrm{Aut}(L/M)$ et $[L : M] = |H|$.

3. Supposons l'extension M/K galoisienne. Soient $\sigma \in H$ et $\tau \in G$. Il s'agit de vérifier $\tau^{-1} \circ \sigma \circ \tau \in H$. Pour cela on prend $x \in M$; l'extension M/K étant galoisienne, on a $\tau(x) \in M$, donc $\sigma \circ \tau(x) = \tau(x)$ et ainsi $\tau^{-1} \circ \sigma \circ \tau(x) = x$. Cela montre que le sous-groupe H de G est normal.

Inversement si H est normal dans G soit $x \in M$ et soit $\tau \in G$. Il s'agit de vérifier $\tau(x) \in M$, c'est-à-dire $\sigma \circ \tau(x) = \tau(x)$ pour tout $\sigma \in H$. En effet comme $\sigma \in H$ et que H est normal dans G on a $\tau^{-1} \circ \sigma \circ \tau \in H$, donc $\tau^{-1} \circ \sigma \circ \tau(x) = x$.

On suppose encore que H est normal dans G, c'est-à-dire que l'extension M/K est galoisienne ; la restriction de σ à M est alors un K-automorphisme de M. L'application qui envoie un élément $\sigma \in \mathrm{Aut}(L/K)$ sur sa restriction M définit un homomorphisme de G dans $\mathrm{Aut}(M/K)$ de noyau H. Son image est donc isomorphe au quotient G/H. Comme

$$|G| = [L : K] = [L : M][M : K] = |H|[M : K],$$

il en résulte que cet homomorphisme est surjectif : son image est $\mathrm{Aut}(M/K)$.

□

Exercice. Soient L/K une extension galoisienne finie de groupe de Galois G, H un sous-groupe de G, $M = L^H$ et $\sigma \in G$. Alors l'extension $L/\sigma(M)$ est galoisienne de groupe de Galois $\sigma H \sigma^{-1}$ et $\sigma(M) = L^{\sigma H \sigma^{-1}}$.

Une extension galoisienne est dite *abélienne, cyclique, résoluble,...* si son groupe de Galois l'est. Rappelons qu'un groupe fini G est *résoluble* s'il existe une suite de sous-groupes

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_{s-1} \subset G_s$$

dans laquelle chaque G_i est un sous-groupe normal de G_{i+1} avec un quotient G_{i+1}/G_i cyclique $(0 \leq i \leq s-1)$.

2.9 Théorie de Galois : quelques exemples

2.9.1 Corps cyclotomiques

Soient n un entier positif, E_n le corps cyclotomique de niveau n et ζ_n une racine primitive n-ième de l'unité, de sorte que $E_n = \mathbf{Q}(\zeta_n)$.

Nous avons vu (Proposition 2.28) que E_n est une extension galoisienne de $\mathbf{Q}$ de groupe de Galois $(\mathbf{Z}/n\mathbf{Z})^\times$.

Supposons n premier et notons $n = p$, $E_p = E$, $\zeta_p = \zeta$. Le groupe des éléments inversibles du corps $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ est cyclique, donc l'extension $E/\mathbf{Q}$ est cyclique de groupe de Galois $G \simeq (\mathbf{Z}/p\mathbf{Z})^\times$ d'ordre $p-1$. Si k est un entier premier à p, notons σ_k l'automorphisme de E déterminé par $\sigma_k(\zeta) = \zeta^k$.

Lemme 2.34. *L'ordre de σ_k dans G est égal à l'ordre de la classe de k modulo p.*

Démonstration. Pour $h \geq 1$ on a $\zeta^h = 1$ si et seulement si p divise h. Donc pour $m \geq 1$ on a $\zeta^m = \zeta$ si et seulement si $m \equiv 1 \pmod{p}$. D'autre part $\sigma_k^m(\zeta) = \zeta^{k^m}$. Il en résulte que l'ordre de σ_k dans G est le plus petit entier m tel que $k^m \equiv 1 \pmod{p}$, c'est l'ordre de la classe de k dans $(\mathbf{Z}/p\mathbf{Z})^\times$. □

Comme ζ est racine du polynôme

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$$

il est de degré $p-1$ sur $\mathbf{Q}$ et $\{1, \zeta, \zeta^2, \ldots, \zeta^{p-2}\}$ est une base sur $\mathbf{Q}$ de E. On préfère d'utiliser comme base $\{\zeta, \zeta^2, \ldots, \zeta^{p-2}, \zeta^{p-1}\}$ car ce sont précisément les racines primitives p-ièmes de l'unité, qui sont donc permutés par les σ_k.

Soit H un sous-groupe de G. Posons

$$\alpha_H = \sum_{\sigma \in H} \sigma(\zeta).$$

On vérifie que $\mathbf{Q}(\alpha_H)$ est le sous-corps E^H de E fixé par H.

Par exemple pour $p = 7$ le groupe G est cyclique d'ordre 6, il est engendré par σ_3 :

$$G = \{1,\ \sigma_3,\ \sigma_3^2 = \sigma_2,\ \sigma_3^3 = \sigma_6,\ \sigma_3^4 = \sigma_4,\ \sigma_3^5 = \sigma_5\},$$

ce qui correspond au fait que $(\mathbf{Z}/7\mathbf{Z})^\times$ est engendré par 3 (on dit que 3 est une *racine primitive modulo* 7) :

$$(\mathbf{Z}/7\mathbf{Z})^\times = \{1,\ 3,\ 3^2 \equiv 2,\ 3^3 \equiv 6,\ 3^4 \equiv 4,\ 3^5 \equiv 5\}.$$

Le groupe G a quatre sous-groupes, deux triviaux $\{1\}$ et G d'ordres 1 et 6 respectivement, et deux non triviaux $\{1, \sigma_6\}$ et $\{1, \sigma_2, \sigma_4\}$. Le seul élément d'ordre 2 dans G est σ_6 qui est la restriction à E de la conjugaison complexe, puisque $\sigma_6(\zeta) = \zeta^{-1} = \overline{\zeta}$. Le sous corps fixé par la conjugaison complexe est le sous-corps réel maximal M de E, il est engendré sur $\mathbf{Q}$ par $\alpha = \zeta + \overline{\zeta}$, comme nous l'avons déjà vu au § 2.7 comme exemple d'application de la proposition 2.28. Le corps $M = \mathbf{Q}(\alpha)$ est cubique cyclique sur $\mathbf{Q}$, le groupe de Galois est engendré par la restriction de σ_2 à M : les conjuqués de α sur $\mathbf{Q}$ sont

$$\alpha_1 = \alpha, \quad \alpha_2 = \sigma_2(\alpha) = \zeta^2 + \zeta^5 = \zeta^2 + \overline{\zeta}^2, \quad \alpha_3 = \sigma_2^2(\alpha) = \zeta^4 + \zeta^3 = \zeta^3 + \overline{\zeta}^3.$$

On trouve le polynôme irréductible de α sur $\mathbf{Q}$ en calculant (facilement) $\alpha_1 + \alpha_2 + \alpha_3 = -1$, $\alpha_1\alpha_2\alpha_3 = 1$ et (un peu moins facilement) $\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 = -2$. Le polynôme cherché est donc $X^3 + X^2 - 2X - 1$.

Il reste un dernier sous-corps N de E dont nous n'avons pas encore parlé, c'est le sous-corps fixé par le sous-groupe d'ordre 3 (et d'indice 2) de G. Donc N est l'unique sous-corps quadratique de E, engendré sur $\mathbf{Q}$ par

$$\beta = \zeta + \sigma_2(\zeta) + \sigma_4(\zeta) = \zeta + \zeta^2 + \zeta^4.$$

Le conjugué de β est

$$\beta^* = \tau(\beta) = \sigma_3(\beta) = \zeta^3 + \zeta^6 + \zeta^5.$$

On vérifie facilement $\beta + \beta^* = -1$, $\beta\beta^* = 2$, donc β est racine du polynôme quadratique $X^2 + X + 2$ dont le discriminant est -7. Ainsi l'unique sous-corps quadratique de L est $\mathbf{Q}(\sqrt{-7})$.

Soit $n = p_1^{a_1} \cdots p_k^{a_k}$ la décomposition en facteurs premiers d'un entier $n \geq 2$. La décomposition du groupe multiplicatif $(\mathbf{Z}/n\mathbf{Z})^\times$ par le théorème chinois :

$$(\mathbf{Z}/n\mathbf{Z})^\times \simeq (\mathbf{Z}/p_1^{a_1}\mathbf{Z})^\times \times \cdots \times (\mathbf{Z}/p_k^{a_k}\mathbf{Z})^\times$$

permet de déduire du théorème 2.28 l'énoncé suivant : (cf. [5] corollaire 27 p. 579).

Corollaire 2.35. *Soit $n = p_1^{a_1} \cdots p_k^{a_k}$ un entier ≥ 2 décomposé en facteurs premiers. Notons E_n le corps cyclotomique $\mathbf{Q}(\zeta_n)$ de niveau n et F_i le corps cyclotomique $E_{p_i^{a_i}} = \mathbf{Q}(\zeta_{p_i^{a_i}})$ de niveau $p_i^{a_i}$. Alors*

$$\mathrm{Gal}(E_n/\mathbf{Q}) \simeq \mathrm{Gal}(F_1/\mathbf{Q}) \times \cdots \times \mathrm{Gal}(F_k/\mathbf{Q}).$$

2.9.2 Constructions à la règle et au compas

Les trois questions classiques posées par les géomètres grecs sur les constructions à la règle et au compas sont les suivantes : peut-on construire, en utilisant uniquement ces deux instruments,
• (*Duplication du cube*) un cube ayant un volume double d'un cube donné ?
• (*Trisection d'un angle*) un angle égal au tiers d'un angle donné ?
• (*Quadrature du cercle*) un carré ayant une aire égale à celle d'un disque donné ?

Ces questions reviennent à construire respectivement la racine cubique d'un nombre donné, le cosinus du tiers d'un angle dont le cosinus est donné, le nombre π.

En termes algébriques on considère le plan cartésien $\mathbf{R}^2$ avec l'unité de longueur donnée par la distance entre $(0,0)$ et $(0,1)$ et à partir de ces deux points on itère les constructions suivantes, dont la réunion produit l'ensemble des *points constructibles* :
– On peut construire la droite qui passe par deux points donnés.
– On peut construire un cercle de rayon donné et de centre préalablement construit.
– À chaque étape on peut ajouter à l'ensemble déjà construit l'intersection de deux droites, de deux cercles, d'une droite et d'un cercle, chacune de ces lignes ayant été précédemment construites.

Un nombre réel est dit *constructible* si le point $(x,0)$ est constructible à la règle et au compas à partir de $(0,0)$ et $(0,1)$.

Des constructions géométriques classiques montrent que les nombres constructibles forment un sous-corps de $\mathbf{R}$ et que si x est constructible, alors $\sqrt{x}$ l'est aussi. Les images suivantes sont extraites de [5] § 13.3.

It is an elementary fact from geometry that if two lengths a and b are given one may construct using straightedge and compass the lengths $a \pm b$, ab and a/b (the first two are clear and the latter two are given by the construction of parallel lines (Figure 1)).

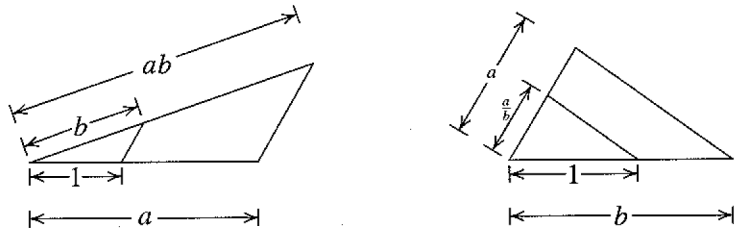

Fig. 1

It is also an elementary geometry construction to construct $\sqrt{a}$ if a is given: construct the circle with diameter $1 + a$ and erect the perpendicular to the diameter as indicated in Figure 2. Then $\sqrt{a}$ is the length of this perpendicular.

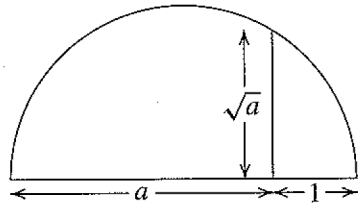

Fig. 2

L'énoncé suivant est facile à démontrer (voir par exemple [5] § 13.3).

Proposition 2.36. *Soit x un nombre réel. Les assertions suivantes sont équivalentes :*
- *x est constructible.*
- *x est algébrique sur $\mathbf{Q}$ et son corps de décomposition sur $\mathbf{Q}$ a pour degré une puissance de 2.*
- *x appartient à un corps de nombres galoisien sur $\mathbf{Q}$ de degré une puissance de 2.*

Comme $\sqrt[3]{2}$ est de degré 3 sur $\mathbf{Q}$, on en déduit l'impossibilité de la duplication du cube.

Il existe des angles dont on peut construire le tiers à la règle et au compas (par exemple π), mais il en existe aussi pour lesquels une telle construction est impossible. Un exemple est $\pi/3$. On a $\cos(\pi/3) = 1/2$ et la formule

$$\cos\theta = 4\cos^3(\theta/3) - 3\cos(\theta/3)$$

montre que le nombre $\beta = 2\cos(\pi/9) = 1,87938\ldots$ est racine du polynôme $X^3 - 3X - 1$. Ce polynôme est irréductible sur $\mathbf{Q}$. Donc β est de degré 3 sur $\mathbf{Q}$, par conséquent il n'est pas constructible.

Pour la quadrature du cercle, l'impossibilité vient de la transcendance du nombre π que nous ne démontrons pas ici (une démonstration est donnée dans l'Annexe A du livre de Lang *Algèbre* [9]).

On déduit du corollaire 2.35 qu'un polygone régulier à n côtés peut être construit à la règle et au compas si et seulement si $\varphi(n)$ est une puissance de 2.

Pour un nombre premier p, dire que $\varphi(p) = p-1$ est une puissance de 2 revient à dire que p est de la forme $2^m + 1$. Il est facile de voir que dans ce cas l'exposant m est lui même une puissance de 2 : quand k est impair, l'identité $x^k + 1 = (x+1)(x^{k-1} - x^{k-2} + \cdots + x^2 - x + 1$ montre que $x^k + 1$ est divisible par $x + 1$.

On appelle *nombre premier de Fermat* tout nombre premier de la forme $F_s = 2^{2^s} + 1$ avec s entier ≥ 0. Les nombres

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65\,537$$

sont des nombres premiers de Fermat. On ignore s'il y en a d'autres (on s'attend à ce que leur nombre soit fini mais on ne le sait pas). Que $F_5 = 2^{2^5} + 1$ ne soit pas un nombre premier a été découvert par Euler. On peut le vérifier ainsi.

Lemme 2.37. *Le nombre $F_5 = 2^{32} + 1$ est divisible par* 641.

Démonstration. (D'après [7], § 2.5). On écrit

$$641 = 625 + 16 = 5^4 + 2^4 \quad \text{et} \quad 641 = 5 \cdot 128 + 1 = 5 \cdot 2^7 + 1.$$

L'identité $x^4 - 1 = (x+1)(x-1)(x^2+1)$ montre que $x^4 - 1$ est divisible par $x+1$, donc $5^4 \cdot 2^{28} - 1$ est divisible par 641. Mais 641 divise aussi $5^4 \cdot 2^{28} + 2^{32}$, donc il divise la différence $2^{32} + 1$.

□

Le théorème de Galois 2.33 permet de démontrer l'énoncé suivant :

Proposition 2.38. *Soit n un entier ≥ 3. Un polygone régulier peut être construit à la règle et au compas si et seulement si n est de la forme $2^k p_1 \cdots p_r$ où k est un entier ≥ 0 et $p_1, \ldots, p_r$ des nombres premiers de Fermat deux-à-deux distincts.*

On trouvera dans [5] § 14.5 d'autres informations sur ce thème, notamment une construction géométrique du polygone régulier à 17 côtés due à J.H. Conway (voir aussi [6]).

2.9.3 Résolution par radicaux

Un nombre complexe est dit *exprimable par radicaux* s'il existe un corps de nombres K le contenant, une tour de corps

$$\mathbf{Q} = K_0 \subset K_1 \subset \cdots \subset K_{s-1} \subset K_s = K,$$

et, pour $1 \leq i \leq s$, un entier $n_i \geq 1$ et un élément $\alpha_i \in K_i$ tels que $K_i = K_{i-1}(\alpha_i)$ avec $\alpha_i^{n_i} \in K_{i-1}$.

On pose $a_i = \alpha_i^{n_i}$ et on écrit $\alpha_i = \sqrt[n_i]{a_i}$ (avec un léger abus de notation : il y a plusieurs racines n_i-ièmes de α_i, mais le corps engendré ne dépend pas de ce choix lorsque les racines n_i-ièmes de l'unité appartiennent au corps de base, ce qui est une hypothèse licite ici) et donc $K_i = K_{i-1}(\sqrt[n_i]{a_i})$.

Soit K un corps de caractéristique nulle. On définit le *groupe de Galois d'un polynôme séparable* $f \in K[X]$ comme le groupe de Galois d'un corps de décomposition de f sur K.

Un polynôme est *résoluble par radicaux* si toutes ses racines sont exprimables par radicaux.

Le théorème de Galois 2.33 permet de démontrer l'énoncé suivant (voir par exemple [5] § 14.7 Th. 39).

Théorème 2.39. *Un polynôme f est résoluble par radicaux si et seulement si son groupe de Galois est résoluble.*

Soit n un entier ≥ 5. Il est connu que le groupe $\mathfrak{S}_n$ n'est pas résoluble et qu'il existe des corps de nombres galoisiens sur $\mathbf{Q}$ de groupe de Galois $\mathfrak{S}_n$. Un tel corps est le corps de décomposition d'un polynôme qui n'est donc pas résoluble par radicaux.

Par exemple le polynôme $X^5 - 6X + 3$ a pour groupe de Galois sur $\mathbf{Q}$ le groupe symétrique $\mathfrak{S}_5$ d'ordre $5! = 120$, il n'est donc pas résoluble par radicaux.

L'outil essentiel pour la démonstration du théorème 2.39 est un théorème dû à Kummer dont nous donnons seulement l'énoncé (voir par exemple [5], Prop. 36 et 37, § 14.7 ou [9] Th. 6.2 Chap. VI § 6) :

Théorème 2.40. *Soient L/K une extension et n un entier positif qui n'est pas divisible par la caractéristique de K. On suppose que K contient les racines n-ièmes de l'unité. Alors l'extension est cyclique si et seulement s'il existe $\alpha \in L$ tel que $L = K(\alpha)$ et $\alpha^n \in K$.*

2.9.4 Fonctions symétriques, discriminant

Soit $f \in K[X]$ un polynôme séparable de degré n à coefficient dans un corps K. Le groupe de Galois de f sur K a été défini (§ 2.9.3) comme le groupe de Galois $G = \mathrm{Gal}(L/K)$ du corps de décomposition L de f sur K. Ce groupe de Galois agit sur l'ensemble E des racines de f par permutation, donc s'injecte dans le groupe symétrique $\mathfrak{S}_n$.

Si f est produit de polynômes irréductibles $f = f_1 \cdots f_k$ dans $K[X]$ et si n_i désigne le degré de f_i, alors le groupe de Galois s'injecte dans le produit $\mathfrak{S}_{n_1} \times \cdots \times \mathfrak{S}_{n_k}$.

Si f est irréductible sur K, alors G agit sur E de façon *transitive* : pour tout α et β dans E il existe $\sigma \in G$ tel que $\sigma(\alpha) = \beta$. Inversement, si on suppose f sans facteur carré et si, pour tout α et β dans E il existe $\sigma \in G$ tel que $\sigma(\alpha) = \beta$, alors f est irréductible sur K.

Nous allons donner un sens précis à l'affirmation suivante :

Le groupe de Galois d'un polynôme "générique" de degré n est le groupe symétrique $\mathfrak{S}_n$. (2.41)

On désigne par L le corps $\mathbf{Q}(x_1, \ldots, x_n)$ des fractions rationnelles en n indéterminées sur $\mathbf{Q}$ (on peut remplacer le corps de base $\mathbf{Q}$ par un corps de caractéristique nulle, mais cela en fait n'ajoute rien). On définit les *fonctions symétriques élémentaires* $s_1, \ldots, s_n \in \mathbf{Q}[x_1, \ldots, x_n]$ par la relation

$$(X - x_1)(X - x_2) \cdots (X - x_n) = X^n - s_1 X^{n-1} + s_2 X^{n-2} - \cdots + (-1)^n s_n.$$

On a par exemple

$$s_1 = x_1 + \cdots + x_n, \quad s_n = x_1 \cdots x_n$$

et

$$s_2 = x_1x_2 + x_1x_3 + \cdots + x_1x_n + x_2x_3 + \cdots + x_2x_n + \cdots + x_{n-1}x_n.$$

Plus généralement, pour $1 \leq k \leq n$, la k-ième fonction symétrique élémentaire en n variables est

$$s_k = \sum_{i_1 < i_2 < \cdots < i_k} x_{i_1} x_{i_2} \cdots x_{i_k}.$$

Le *polynôme générique de degré n* est le polynôme $f(X) = (X - x_1)(X - x_2) \cdots (X - x_n)$. On note encore K le corps $\mathbf{Q}(s_1, \ldots, s_n)$, qui est un sous-corps de L. Le polynôme f a ses coefficients dans

K et son corps de décomposition sur K est L. Comme f est de degré n, le groupe de Galois G de L sur K est (isomorphe à) un sous-groupe de $\mathfrak{S}_n$. En particulier on a $[L : K] \leq n!$.

Toute permutation de $\{1, \ldots, n\}$ induit un automorphisme de L qui laisse invariant chacun des s_k $(1 \leq k \leq n)$, ce qui donne une injection de $\mathfrak{S}_n$ dans G. Il en résulte que l'extension $L/L^{\mathfrak{S}_n}$ est de degré $n!$ et de groupe de Galois $\mathfrak{S}_n$. Par le théorème de Galois 2.33, le sous-corps $L^{\mathfrak{S}_n}$ de L fixé par $\mathfrak{S}_n$ n'est autre que K.

Une fonction rationnelle $F(x_1, \ldots, x_n) \in L$ est appelée *symétrique* si elle est invariante sous l'action de $\mathfrak{S}_n$. Nous avons ainsi démontré :

Proposition 2.42. *Une fraction rationnelle $F(x_1, \ldots, x_n) \in \mathbf{Q}(x_1, \ldots, x_n)$ est symétrique si et seulement s'il existe une fraction rationnelle G en n indéterminées telle que*

$$F(x_1, \ldots, x_n) = G(s_1, \ldots, s_n).$$

La fraction rationnelle G est unique. Si F est un polynôme, alors G est aussi un polynôme : un algorithme pour calculer G est donné dans l'exercice 37 du § 14.6 de [5]. L'idée consiste à considérer le monome $Ax_1^{a_1} \cdots x_n^{a_n}$ de F qui est dominant pour l'ordre lexicographique et à soustraire $As_1^{a_1-a_2} s_2^{a_2-a_3} \cdots s_n^{a_n}$.

Ceci montre en passant que $s_1, \ldots, s_n$ sont algébriquement indépendants.

Pour revenir à notre affirmation (2.41) sur les polynômes "génériques", on part d'un polynôme unitaire f de degré n dont les coefficients sont des indéterminées ; on l'écrit

$$f(X) = X^n - s_1 X^{n-1} + s_2 X^{n-2} - \cdots + (-1)^n s_n. \tag{2.43}$$

On désigne par K le corps des fractions rationnelles $\mathbf{Q}(s_1, \ldots, s_n)$ en n indéterminées sur $\mathbf{Q}$, par L un corps de décomposition de f sur K et par $x_1, \ldots, x_n$ les racines de f dans L. Ainsi $L = K(x_1, \ldots, x_n)$. Vérifions que les x_i sont *algébriquement indépendants sur* $\mathbf{Q}$, c'est-à-dire que si $p \in \mathbf{Q}[X_1, \ldots, X_n]$ est un polynôme non nul, alors $p(x_1, \ldots, x_n) \neq 0$ (voir § 2.9.7). Sinon le produit

$$P(X_1, \ldots, X_n) = \prod_{\sigma \in \mathfrak{S}_n} p(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$$

serait un polynôme non nul symétrique qui s'annule en $(x_1, \ldots, x_n)$, ce qui fournirait une relation de dépendance algébrique non triviale entre $s_1, \ldots, s_n$. On en déduit :

Théorème 2.44. *Si $s_1, \ldots, s_n$ sont des indéterminées sur $\mathbf{Q}$, le polynôme générique (2.43) est séparable et a pour groupe de Galois $\mathfrak{S}_n$ sur le corps $\mathbf{Q}(s_1, \ldots, s_n)$.*

Un exemple de polynôme symétrique est donné par le *discriminant*.

Définition. Soient L un corps et $x_1, \ldots, x_n$ des éléments de L. On définit le *discriminant* de $(x_1, \ldots, x_n)$ par

$$D = \prod_{1 \leq i < j \leq n} (x_i - x_j)^2 = (-1)^{n(n-1)/2} \prod_{1 \leq i \neq j \leq n} (x_i - x_j).$$

Le *discriminant générique* est celui pour lequel $x_1, \ldots, x_n$ sont des indéterminées et $L = \mathbf{Q}(x_1, \ldots, x_n)$. C'est un polynôme symétrique, donc d'après la proposition 2.42 il s'exprime comme

un polynôme en les fonctions symétriques élémentaires $s_1, \dots, s_n$. Une des deux racines carrées de D est

$$\sqrt{D} = \prod_{1 \le i < j \le n} (x_i - x_j).$$

L'autre est $-\sqrt{D}$. Le corps quadratique engendré par $\sqrt{D}$ sur $\mathbf{Q}(s_1, \dots, s_n)$ est le sous-corps fixé par le groupe alterné $\mathfrak{A}_n$ de $\mathfrak{S}_n$.

On définit aussi le *discriminant* d'un polynôme unitaire $f \in K[X]$ en considérant un corps de décomposition L de f sur K : dans $L[X]$ ce polynôme se factorise complètement

$$f(X) = (X - \alpha_1) \cdots (X - \alpha_n)$$

et le discriminant de f est défini comme le discriminant de $(\alpha_1, \dots, \alpha_n)$. D'après ce qui précède il appartient à K.

Le groupe de Galois G d'un polynôme irréductible f de degré n sur un corps K de caractéristique nulle est un sous-groupe de $\mathfrak{S}_n$; on obtient un tel isomorphisme en numérotant les racines de f dans un corps de décomposition de f sur K et en considérant G comme un groupe de permutation de ces racines. Ainsi :

Proposition 2.45. *Ce sous-groupe G de $\mathfrak{S}_n$ est contenu dans $\mathfrak{A}_n$ si et seulement si le discriminant D de f est un carré dans K.*

Le discriminant d'un polynôme quadratique X^2+aX+b est a^2-4b, celui d'un polynôme cubique $X^3 + pX + q$ est $-4p^3 - 27q^2$. Un polynôme irréductible de degré 3 a pour groupe de Galois sur $\mathbf{Q}$ le groupe cyclique d'ordre 3 (qui n'est autre que le groupe alterné $\mathfrak{A}_3$) si le discriminant est un carré dans $\mathbf{Q}$, c'est le groupe symétrique $\mathfrak{S}_3$ (groupe non commutatif d'ordre 6) sinon. Cela permet de distinguer les polynômes cubiques dont un corps de rupture est galoisien des autres.

Voici une méthode pour calculer un discriminant. Soit L un corps, soient $x_1, \dots, x_n$ des éléments de L et soit D leur discriminant. Considérons le polynôme

$$P(X) = \prod_{i=1}^{n} (X - x_i).$$

Sa dérivée est

$$P('X) = \sum_{i=1}^{n} \prod_{\substack{1 \le j \le n \\ j \ne i}} (X - x_j).$$

Ainsi pour $1 \le i \le n$ on a

$$P'(x_i) = \prod_{\substack{1 \le j \le n \\ j \ne i}} (x_i - x_j).$$

Par conséquent

$$\prod_{i=1}^{n} P'(x_i) = (-1)^{n(n-1)/2} D.$$

Comme exemple nous utilisons cet argument pour calculer le discriminant des polynômes cyclotomiques d'indice un nombre premier ([6] Chap. 10, § 10.5, Exemple 10.12).

Proposition 2.46. *Soit p un nombre premier impair. Le discriminant du polynôme cyclotomique Φ_p d'indice p est*

$$(-1)^{(p-1)/2}p^{p-2}.$$

Démonstration. On utilise ce qui précède avec $P = \Phi_p$, $n = p-1$ et $x_i = \zeta^i$ $(1 \le i \le p-1)$. On a

$$P(X) = \frac{X^p - 1}{X - 1} \quad \text{et} \quad P'(X) = \frac{pX^{p-1}}{X-1} - \frac{X^p - 1}{(X-1)^2}.$$

Par conséquent pour $1 \le i \le p-1$

$$P'(\zeta^i) = \frac{p\zeta^{i(p-1)}}{\zeta^i - 1}.$$

Le produit des racines de P est le terme constant $P(0)$ (le degré $p-1$ est pair)

$$\prod_{i=1}^{p-1} \zeta^i = 1.$$

Le polynôme minimal des nombres $\zeta^i - 1$ $(1 \le i \le p-1)$ est $P(X+1)$ dont le terme constant est p :

$$\prod_{i=1}^{p-1} (\zeta^i - 1) = p.$$

On trouve ainsi

$$\prod_{i=1}^{p-1} P'(\zeta^i) = p^{p-2}.$$

□

Exercice. Soit p un nombre premier. Vérifier que l'unique sous-corps quadratique de $\mathbf{Q}(\zeta_p)$ est le corps $\mathbf{Q}(\sqrt{\epsilon p})$, où $\epsilon = 1$ si $p \equiv 1 \pmod 4$ et $\epsilon = -1$ si $p \equiv 3 \pmod 4$.
(Voir [5] § 14.5).

2.9.5 Compléments

Nous avons vu au § 2.9.1 que le corps cyclotomique $\mathbf{Q}(\zeta_p)$ contenait un unique sous-corps quadratique. Il n'est pas difficile de développer l'argument pour déduire qu'inversement, tout corps quadratique sur $\mathbf{Q}$ est contenu dans un corps cyclotomique. Un résultat beaucoup plus général est le *théorème de Kronecker-Weber : toute extension abélienne de $\mathbf{Q}$ est contenue dans une extension cyclotomique*. Voir par exemple le Théorème 2.10 de [8].

Un des problèmes ouverts les plus important du sujet est le *problème inverse de Galois* : *Est-il vrai que tout groupe fini est un groupe de Galois sur $\mathbf{Q}$?* C'est facile pour un groupe abélien, c'est connu pour beaucoup de groupes (en particulier pour $\mathfrak{S}_n$ et $\mathfrak{A}_n$), mais pas encore pour tous.

2.9.6 Exercices

a) *Étude du corps de décomposition de $X^8 - 2$. Référence : [5].*

On désigne par θ la racine réelle du polynôme $X^8 - 2$ et par ζ une racine primitive 8ème de l'unité. Le corps de décomposition du polynôme $X^8 - 2$ est $K = \mathbf{Q}(\theta, \zeta)$. Sous un élément σ du groupe de Galois G de K sur $\mathbf{Q}$ l'image de ζ est une des 4 racines primitives 8èmes de l'unité, à savoir ζ, ζ^3, ζ^5 ou $\zeta^7 = \zeta^{-1} = \overline{\zeta}$. L'image de θ est l'un des 8 conjugués de θ, à savoir $\zeta^j\theta$. À priori cela fait $4 \times 8 = 32$ possibilités pour σ. Mais on a $K = \mathbf{Q}(\theta, i)$, donc K a pour degré 16 sur $\mathbf{Q}$. Donc σ est déterminé par l'image de θ et l'image de i ce qui ne fait plus que 16 possibilités et cela décrit donc tous les éléments de G. Noter que l'existence, pour chaque couple formé d'un conjugué de θ et d'un conjugué de i, d'un éléments du groupe de Galois qui envoie (θ, i) sur ce couple, résulte du dénombrement que nous venons de faire.

Comme $\theta^4 = \sqrt{2} = \zeta + \zeta^7$, les images par un automorphisme de K de θ et ζ doivent vérifier cette relation, ce qui justifie la réduction de 32 à 16.

b) Compositum d'une extension finie et d'une extension Galoisienne

Référence : polycopié online de Robert B. Ash (`www.math.uiuc.edu/~ash/Algebra.html`) Abstract algebra basic graduate year 11/02 Chapter 6 Galois Theory p.6 Theorem 6.2.2)

Dans la correspondance de Galois, si H_1 et H_2 sont deux sous-groupes du groupe de Galois, quel est le corps fixé par $H_1 \cap H_2$? Si K_1 et K_2 sont deux corps intermédiaires, quel est le groupe de Galois associé à $K_1 \cap K_2$?

Soient E/F une extension galoisienne (finie) et K/F une extension finie.
Montrer que EF est une extension galoisienne de K.
Montrer que le groupe de Galois de EK/K est (isomorphe à) un sous-groupe du groupe de Galois de E/F. En déduire que $[EK : K]$ divise $[E : F]$. Donner un exemple qui montre que l'hypothèse E/F galoisienne n'est pas superflue.
Montrer que $[EK : K] = [E : F]$ si et seulement si $E \cap K = F$.
On suppose de plus que l'extension K/F est galoisienne. Montrer que le groupe de Galois $G(EK/E \cap K)$ de EK sur $E \cap K$ est le produit direct de ses deux sous-groupes $G(EK/E)$ et $G(EK/K)$.

2.9.7 Extensions transcendantes

Des références pour cette section sont [9] Chap. VIII et [5] § 14.9.

Soit K/k une extension. Une partie S de K est dite *algébriquement libre sur k* si, pour toute famille finie $\{s_1, \ldots, s_n\}$ d'éléments de S deux-à-deux distincts et pour tout polynôme non nul P en n variables à coefficients dans k, on a $P(s_1, \ldots, s_n) \neq 0$. Par abus de langage, on dit aussi que les éléments de S sont algébriquement indépendants sur k.

Un sous-ensemble maximal de K algébriquement libre est appelé *base de transcendance de K sur k*. De cette définition il résulte que si B est une base de transcendance de K sur k, alors K est une extension algébrique de $k(B)$.

Le lemme suivant montre que deux bases de transcendance ont le même nombre d'éléments.

Lemme 2.47. *Soient $S = \{s_1, \ldots, s_n\}$ une partie de K algébriquement libre sur k et soit $T = \{t_1, \ldots, t_m\}$ une famille génératrice de l'extension K/k : autrement dit $K = k(t_1, \ldots, t_m)$. Alors il existe une base de transcendance B de K sur k telle que $S \subset B \subset T$.*

Ce lemme est un analogue pour l'indépendance algébrique du lemme de la base incomplète pour les espaces vectoriels. Une version un peu plus précise est indiquée dans [5], c'est un analogue du *lemme de remplacement* pour les espaces vectoriels ([5], § 11.1, Th. 3 p. 390) qui s'énonce ainsi :

> Si $\{a_1, \ldots, a_n\}$ est une base de transcendance et $\{b_1, \ldots, b_m\}$ un système générateur de l'extension K/k, on peut réordonner $a_1, \ldots, a_n$ de telle sorte que pour tout $k = 0, \ldots, n$, $\{b_1, \ldots, b_k, a_{k+1}, \ldots, a_n\}$ soit une base de transcendance

Le nombre d'éléments d'une base de transcendance d'une extension K/k est appelé *degré de transcendance de K sur k* ; nous le noterons $\mathrm{degtr}_k K$. On dit aussi que c'est la *dimension algébrique de K sur k.*

Quand on a des extensions finies $K \subset L \subset F$, les degrés de multiplient (cf. lemme 2.1). En revanche les degrés de transcendance s'ajoutent.

Lemme 2.48. *Soient $K \subset L \subset F$ trois corps. L'extension F/K a un degré de transcendance fini si et seulement si les deux extensions L/K et F/L ont un degré de transcendance fini. Dans ce cas*

$$\mathrm{degtr}_K F = \mathrm{degtr}_L F + \mathrm{degtr}_K L.$$

$$\begin{matrix} & F & \\ \mathrm{degtr}_L F & | & \\ & L & \\ \mathrm{degtr}_K L & | & \\ & K & \end{matrix} \quad \mathrm{degtr}_K F$$

Démonstration. Si A est une base de transcendance de L sur K et B une base de transcendance de F sur L, alors $A \cup B$ est une base de transcendance de F sur K.

□

Une extension algébrique est une extension de degré de transcendance 0.

Exercice. Soient $x_1, \ldots, x_m$ des nombres complexes algébriquement indépendants sur $\mathbf{Q}$. Cela signifie que pour tout polynôme non nul $P \in \mathbf{Q}[X_1, \ldots, X_n]$, le nombre $P(x_1, \ldots, x_n)$ n'est pas nul. Montrer qu'ils sont algébriquement indépendants sur le corps des nombres algébriques. En déduire que pour tout polynôme non constant à coefficients algébriques $P \in \overline{\mathbf{Q}}[X_1, \ldots, X_n]$, le nombre $P(x_1, \ldots, x_n)$ est transcendant sur $\mathbf{Q}$.

Lemme 2.49. *Soient K et L deux extensions d'un corps k. Les propriétés suivantes sont équivalentes :*
(i) Si $\{x_1, \ldots, x_n\}$ sont des éléments de K linéairement indépendants sur k, alors ils sont linéairement indépendants sur L.
(ii) Si $\{y_1, \ldots, y_n\}$ sont des éléments de L linéairement indépendants sur k, alors ils sont linéairement indépendants sur K.

Quand les conditions équivalentes du lemme 2.49 sont satisfaites on dit que les deux extensions K/k et L/k sont *linéairement disjointes* (ou encore que *les deux corps K et L sont linéairement disjoints sur k*).

Exercice. Soient K et L deux extensions d'un corps k et soit B une base de K sur k. Alors les deux extensions K/k et L/k sont linéairement disjointes si et seulement si les éléments de B sont linéairement indépendants sur L.

Exercice. On définit par récurrence une suite croissante de corps $(E_n)_{n\geq 0}$ de la façon suivante. On part de $E_0 = \mathbf{Q}$. Pour $n \geq 1$, on définit E_n comme la clôture algébrique du corps engendré sur E_{n-1} par les nombres $\exp(x) = e^x$, où x décrit E_{n-1}. On désigne par E la réunion des E_n, $n \geq 0$.

On définit de même une suite croissante de corps $(L_n)_{n\geq 0}$ de la façon suivante. On part de $L_0 = \mathbf{Q}$. Pour $n \geq 1$, on définit L_n comme la clôture algébrique du corps engendré sur L_{n-1} par les nombres complexes y tels que $e^y \in L_{n-1}$. On désigne par L la réunion des L_n, $n \geq 0$.

Montrer que la conjecture de Schanuel implique que les corps E et L sont linéairement disjoints sur $\overline{\mathbf{Q}}$.
`Référence` : http ://arxiv.org/abs/0804.3520

Une extension K/k est dite *transcendante pure* s'il existe une base de transcendance S telle que $K = k(S)$. D'après le *Théorème de Lüroth*, si t est transcendant sur k, toute extension K de k contenue dans $k(t)$ est transcendante pure.

2.9.8 Le théorème de Bézout et le résultant de deux polynômes

Le théorème de Bézout est un outil essentiel dans l'étude des intersections de courbes algébriques planes dans un plan projectif. Il repose sur une méthode d'élimination. [3]

2.9.8.1 Résumé

Soient K un corps algébriquement clos, F_1 et F_2 deux polynômes homogènes de $K[T, X, Y]$ de degrés d_1, d_2 respectivement, sans facteur irréductible commun dans cet anneau factoriel. Nous allons voir que les deux courbes projectives planes $C_1 = Z(F_1)$ et $C_2 = Z(F_2)$ n'ont qu'un nombre fini de points communs, disons $P_1, \ldots, P_k$, et que $k \leq d_1 d_2$. Nous définirons ensuite la multiplicité d'intersection $m(P_i; C_1, C_2)$ de C_1 et C_2 au point P_i, $(1 \leq i \leq k)$, et nous montrerons

$$\sum_{i=1}^{k} m(P_i; C_1, C_2) = d_1 d_2.$$

Enfin nous définissons la multiplicité $m(P, C)$ d'un point P sur une courbe plane C, et nous montrons

$$m(P_i; C_1, C_2) \geq m(P_i, C_1) m(P_i, C_2).$$

[3] Michel Waldschmidt, *Le théorème de Bézout et le résultant de deux polynômes*. RMS 114ème année Janvier 2004 numéro 1, 26–34.
http ://www.rms-math.com/

Le cas le plus simple est l'intersection d'une courbe affine plane $C_1 \subset \mathbf{A}_2(K)$ d'équation $F(X,Y) = 0$, où $F \in K[X,Y]$ a un degré total d_1, avec une courbe affine plane C_2 dont l'équation a la forme $Y = Q(X)$, où $Q \in K[X]$ est de degré d_2. On trouve les coordonnées des points d'intersection en substituant $Q(X)$ à Y dans l'équation de C_1 et en résolvant $F(X, Q(X)) = 0$. Ce cas très simple permet déjà de traiter l'intersection d'une courbe plane quelconque avec une droite ou avec une conique (on peut écrire une conique sous forme $Y = Q(X)$, avec Q de degré 2). Cet exemple montre la nécessité de se placer dans l'espace projectif, et sur un corps algébriquement clos, pour espérer obtenir une égalité dans le théorème de Bézout. Le rôle du résultant est d'*éliminer* la variable Y, même quand l'équation de C_2 n'est pas de la forme $Y = Q(X)$.

2.9.8.2 Première forme du théorème de Bézout : $k \leq d_1 d_2$.

Nous allons montrer que deux courbes projectives planes C_1, C_2, de degrés d_1 et d_2, sans composantes communes, n'ont qu'un nombre fini de points d'intersection, et ce nombre est majoré par le produit $d_1 d_2$. La démonstration utilisera le résultant de deux polynômes.

a) Résultant de deux polynômes en une variable.

Soit A un anneau commutatif unitaire. On désigne par S l'anneau $A[X]$ des polynômes en une variable à coefficients dans A, et, pour d entier ≥ 0, on note S_d le A-module des polynômes de degré $\leq d$. Ainsi S_d est libre sur A, de rang $d+1$, une base étant donnée par X^i, $(0 \leq i \leq d)$.

Soient P et Q deux polynômes de S de degrés p et q :

$$P(X) = a_0 + a_1 X + \cdots + a_p X^p, \qquad Q(X) = b_0 + b_1 X + \cdots + b_q X^q.$$

L'homomorphisme de A-modules

$$\begin{array}{ccc} S_{q-1} \times S_{p-1} & \longrightarrow & S_{p+q-1} \\ (U,V) & \longmapsto & UP + VQ \end{array}$$

a pour matrice, dans les bases citées,

$$\begin{pmatrix} a_0 & 0 & \cdot & \cdot & \cdot & 0 & b_0 & 0 & \cdots & 0 \\ a_1 & a_0 & \cdot & \cdot & \cdot & 0 & b_1 & b_0 & \cdots & 0 \\ \vdots & \vdots & \cdot & \cdot & \cdot & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{p-1} & a_{p-2} & \cdot & \cdot & \cdot & 0 & b_{p-1} & b_{p-2} & \cdots & b_0 \\ a_p & a_{p-1} & \cdot & \cdot & \cdot & 0 & b_p & b_{p-1} & \cdots & b_1 \\ 0 & a_p & \cdot & \cdot & \cdot & 0 & b_{p+1} & b_p & \cdots & b_2 \\ \vdots & \vdots & \cdot & \cdot & \cdot & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdot & \cdot & \cdot & a_0 & b_{q-1} & b_{q-2} & \cdots & b_{q-p} \\ 0 & 0 & \cdot & \cdot & \cdot & a_1 & b_q & b_{q-1} & \cdots & b_{q-p+1} \\ 0 & 0 & \cdot & \cdot & \cdot & a_2 & 0 & b_q & \cdots & b_{q-p+2} \\ \vdots & \vdots & \cdot & \cdot & \cdot & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdot & \cdot & \cdot & a_p & 0 & 0 & \cdots & b_q \end{pmatrix}$$

Les q premières colonnes sont les composantes, dans la base $(1, X, \ldots, X^{p+q-1})$, de $P, XP, \ldots, X^{q-1}P$, tandis que les p dernières sont les composantes, dans la même base, de $Q, XQ, \ldots, X^{p-1}Q$. La diagonale principale est $(a_0, \ldots, a_0, b_q, \ldots, b_q)$.

Définition. Le déterminant de cette matrice est appelé le *résultant* de P et Q. On le note $\mathrm{Res}(P,Q)$. Le *résultant universel* est le résultant des deux polynômes

$$U_0 + U_1X + \cdots + U_pX^p, \quad \text{et} \quad V_0 + V_1X + \cdots + V_qX^q,$$

dans l'anneau $A_{pq} = \mathbf{Z}[U_0, U_1, \ldots, U_p, V_0, V_1, \ldots, V_q]$ des polynômes à coefficients dans $\mathbf{Z}$ en $p+q+2$ indéterminées. On obtient le résultant de P et Q par *spécialisation*, c'est-à-dire comme image par l'homomorphisme canonique de A_{pq} dans A qui envoie U_i sur a_i et V_j sur b_j. Cet homomorphisme canonique n'est injectif que si l'anneau A est de caractéristique nulle.

L'écriture du résultant sous forme de déterminant donne facilement :

Proposition 2.50. *Le résultant universel est un polynôme en $U_0, U_1, \ldots, U_p, V_0, V_1, \ldots, V_q$, homogène de degré q en $U_0, \ldots, U_p$, et homogène de degré p en $V_0, \ldots, V_q$.*

On obtient aussi facilement :

Proposition 2.51. *Il existe deux polynômes U et V dans S, de degrés $< q$ et $< p$ respectivement, tels que le résultant $R = \mathrm{Res}(P,Q)$ de P et Q s'écrive $R = UP + VQ$.*

On en déduit que si P et Q ont un zéro commun (dans A, ou dans un corps contenant A), alors $\mathrm{Res}(P,Q) = 0$. Nous allons voir la réciproque. Nous aurons besoin du résultat suivant :

Proposition 2.52. *Soient A_0 un anneau, $A = A_0[Y_1, \ldots, Y_n]$ l'anneau des polynômes en n indéterminées à coefficients dans A_0, et P, Q des polynômes de $A_0[Y_0, \ldots, Y_n]$, homogènes de degrés p et q respectivement. On considère P et Q comme des éléments de $A[Y_0]$, et on note $R = \mathrm{Res}_{Y_0}(P,Q) \in A$ leur résultant (par rapport à la variable Y_0). Alors R est homogène de degré pq en $Y_1, \ldots, Y_n$.*

Démonstration. Ecrivons

$$P = a_0 + a_1Y_0 + \cdots + a_pY_0^p, \qquad Q = b_0 + b_1Y_0 + \cdots + b_qY_0^q,$$

avec a_i et b_j homogènes de degré $p-i$ et $q-j$ respectivement dans A. Soit $R(Y_1, \ldots, Y_n) \in A$ le résultant. On a

$$R(TY_1, \ldots, TY_n) = \begin{vmatrix} T^pa_0 & 0 & \cdots & 0 & 0 & T^qb_0 & 0 & \cdots & 0 & 0 \\ T^{p-1}a_1 & T^pa_0 & \cdots & 0 & 0 & T^{q-1}b_1 & T^qb_0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & a_p & Ta_{p-1} & 0 & 0 & \cdots & b_q & Tb_{q-1} \\ 0 & 0 & \cdots & 0 & a_p & 0 & 0 & \cdots & 0 & b_q \end{vmatrix}$$

On multiplie la première colonne par T^q, la seconde par T^{q-1}, ..., puis la colonne commençant par T^qb_0 par T^p, la suivante par T^{p-1}, ... On a ainsi multiplié le déterminant par T^r avec

$$r = \sum_{i=1}^{q} i + \sum_{j=1}^{p} j = \frac{q(q+1))}{2} + \frac{p(p+1)}{2}.$$

Dans la i-ème ligne, $(1 \le i \le p+q)$, on peut mettre en facteur $T^{p+q+1-i}$, et on trouve

$$T^rR(TY_1, \ldots, TY_n) = T^sR(Y_1, \ldots, Y_n),$$

avec $s = \sum_{i=1}^{p+q} i$, donc

$$s - r = \frac{(p+q)(p+q+1))}{2} - \frac{q(q+1))}{2} - \frac{p(p+1)}{2} = pq,$$

ce qui donne le résultat voulu. □

Voici une des propriétés fondamentales du résultant.

Proposition 2.53. *Si*

$$P(X) = a_0 \prod_{i=1}^{p} (X - \alpha_i) \quad et \quad Q(X) = b_0 \prod_{j=1}^{q} (X - \beta_j),$$

alors

$$\begin{aligned} \mathrm{Res}(P,Q) &= a_0^q b_0^p \prod_{i=1}^{p} \prod_{j=1}^{q} (\alpha_i - \beta_j) \\ &= (-1)^{pq} b_0^p \prod_{j=1}^{q} P(\beta_j) \\ &= a_0^q \prod_{i=1}^{p} Q(\alpha_i). \end{aligned}$$

Démonstration. Par spécialisation on peut supposer que A est l'anneau des polynômes à coefficients dans $\mathbf{Z}$ en les variables $a_0, b_0, \alpha_1, \ldots, \alpha_p, \beta_1, \ldots, \beta_q$. Dans cet anneau factoriel, $\alpha_i - \beta_j$ est un élement irréductible, qui divise $R = \mathrm{Res}(P,Q)$ (car si on spécialise en $\alpha_i = \beta_j$, alors le résultant est nul). On remarque alors que

$$a_0^q b_0^p \prod_{i=1}^{p} \prod_{j=1}^{q} (\alpha_i - \beta_j)$$

est homogène de degré q en les coefficients de P, et de degré p en les coefficients de Q. Il en résulte que cet élément est de la forme cR, avec $c \in \mathbf{Z}$. Le coefficient du monôme $a_0^p b_0^q$ étant 1, on obtient l'égalité annoncée. □

Corollaire 2.54. *Soit K un corps contenant A dans lequel P et Q se décomposent en facteurs de degrés 1. Alors le résultant* $\mathrm{Res}(P,Q)$ *est nul si et seulement si P et Q ont un zéro commun dans K. En particulier, si l'anneau A est factoriel, alors* $\mathrm{Res}(P,Q) = 0$ *si et seulement si P et Q ont un facteur irréductible commun.*

b) Application aux courbes.
Voici une première forme (faible) du théorème de Bézout. On travaille sur un corps K quelconque.

Théorème 2.55. *Soient F et G deux formes (polynômes homogènes) de $K[T,X,Y]$, de degrés d_1 et d_2 respectivement, sans facteur irréductible commun. Alors l'ensemble des $(t:x:y) \in \mathbf{P}_2(K)$ tels que $F(t,x,y) = G(t,x,y) = 0$ est fini, avec au plus $d_1 d_2$ éléments.*

Démonstration. Le principe de la démonstration est le suivant : on prend k points (distincts) communs aux deux courbes $Z(F)$ et $Z(G)$, disons $P_i = (t_i : x_i : y_i)$, $(1 \le i \le k)$. On choisit des coordonnées homogènes de telle sorte que $(1:0:0)$ ne soit pas l'un des P_i, ce qui permet de définir la projection $\pi(P_i) = (t_i : x_i) \in \mathbf{P}_1$ des P_i, et on demande en plus que ces projections soient deux-à-deux distinctes. On prend ensuite le résultant de F et G par rapport à Y ; c'est un polynôme non nul, homogène en T, X de degré $d_1 d_2$, qui s'annule en chaque $\pi(P_i)$. D'où la majoration annoncée : $k \le d_1 d_2$.

Précisons comment se fait le choix des coordonnées homogènes. On considère les droites joignant les points P_i. Comme on peut agrandir le corps K sans affaiblir l'énoncé, on peut choisir un point P_0 en dehors de la réunion de ces droites. On prend un repère projectif tel que ce point ait pour coordonnées projectives $(0:0:1)$. Le fait que P_0, P_i, P_j ne soient pas alignés pour $i \ne j$ signifie précisément que les deux points $(t_i : x_i)$ et $(t_j : x_j)$ de $\mathbf{P}_1$ sont distincts. □

Exercices.
• Soient $C_1, \ldots, C_s$ des courbes affines planes de degré d, sur un corps K algébriquement clos. On suppose que le sous-ensemble $C_1 \cap \cdots \cap C_s$ de $\mathbf{A}_2(K)$ est fini. Montrer que cet ensemble a au plus d^2 éléments.
• Soient $F_1, \ldots, F_s$ des polynômes de $K[X,Y]$, dont le degré en X est $\le L$, et le degré en Y est $\le M$. On note C_i la courbe affine $Z(C_i)$, $(i = 1, \ldots, s)$, et on suppose que $C_1 \cap \ldots \cap C_s$ est fini. Soient $(x_1, y_1), \ldots, (x_k, y_k)$ des points distincts de $C_1 \cap \ldots \cap C_s$, avec $x_1, \ldots, x_k$ deux-à-deux distincts. Montrer que l'on a $k \le 2LM$.

2.9.8.3. Multiplicité d'intersection de deux courbes planes

Le théorème précédent donne seulement une inégalité : $k \le d_1 d_2$. La raison est claire : on a utilisé le fait qu'un polynôme en une variable de degré d a au plus d racines dans un corps K. Pour obtenir une égalité, il faut d'une part supposer le corps algébriquement clos, et d'autre part compter les racines avec multiplicités. Ceci va nous fournir une des définitions possibles de la multiplicité d'intersection de deux courbes en un point.

a) Définition de $m(P; C_1, C_2)$.
Soient C_1 et C_2 deux courbes sur un corps algébriquement clos, et P un point d'intersection de C_1 et C_2. On va définir un entier $m(P; C_1, C_2)$, qui est la multiplicité d'intersection de C_1 et C_2 au point P. Comme la définition va être locale, on va travailler dans le plan affine. On va choisir des coordonnées (c'est là toute la difficulté : vérifier que la définition ne dépend pas de ce choix), de telle sorte que $P = (0,0)$; on écrit les équations des deux courbes $F(X,Y) = 0$ et $G(X,Y) = 0$, on désigne par $R(X)$ le résultant par rapport à Y de F et G, et on considère l'ordre du zéro de R au point 0. Appelons-le m. Il est facile de voir que , dès que l'intersection comporte plus d'un point, m dépend du choix des coordonnées affines. Par définition, $m(P; C_1, C_2)$ sera le minimum de ces valeurs de m pour tous les choix possibles de coordonnés affines avec $P = (0,0)$.

Montrons déjà que l'entier m est invariant quand on effectue un changement de coordonnées de la forme

$$X' = X \qquad Y' = Y + \lambda X,$$

avec $\lambda \in K$. Pour cela considérons le polynôme

$$R(\lambda, X) = \mathrm{Res}_Y\big(F(X, \lambda X + Y), G(X, \lambda X + Y)\big).$$

Montrons [4] qu'il ne dépend pas de λ. Pour cela écrivons-le

$$R(\lambda, X) = c_0 + c_1\lambda + \cdots + c_N\lambda^N,$$

avec $c_i \in K[X]$, et $c_N \neq 0$. Par hypothèse les deux polynômes F et G sont sans facteur irréductible commun, donc

$$\mathrm{Res}_Y(F, G) = R(0, X) = c_0(X)$$

n'est pas nul. Soit $\alpha \in K$ tel que $c_0(\alpha)c_N(\alpha) \neq 0$. Si on avait $N > 0$, on pourrait trouver une racine λ_0 au polynôme $R(\lambda, \alpha)$ (le corps K est algébriquement clos). Alors les deux polynômes $F(\alpha, \lambda_0\alpha + Y)$ et $G(\alpha, \lambda_0\alpha + Y)$ ont un résultant nul, donc une racine commune, disons $Y = \beta$, ce qui entraîne que $F(\alpha, Y)$ et $G(\alpha, Y)$ ont aussi une racine commune, à savoir $\lambda_0\alpha + \beta$. Ceci contredit le choix de α avec $R(0, \alpha) = c_0(\alpha) \neq 0$.

Il reste à voir l'effet d'un changement de variables de la forme

$$X' = X + \mu Y \qquad Y' = Y.$$

On définit maintenant

$$\bar{R}(\mu, X) = \mathrm{Res}_Y\big(F(X + \mu Y, Y), G(X + \mu Y, Y)\big).$$

C'est encore un polynôme en μ et X ; écrivons-le sous la forme :

$$\bar{R}(\mu, X) = A_m(\mu)X^m + \cdots + A_N(\mu)X^N,$$

avec $m \leq N$ et $A_m \neq 0$. Alors pour tous les μ pour lesquels $A_m(\mu) \neq 0$, l'ordre de $\bar{R}(\mu, X)$ au point $X = 0$ est égal à m, et pour les autres μ l'ordre en question est plus grand. Donc cet entier m n'est autre que $m(P; C_1, C_2)$.

b) Le théorème de Bézout (forme définitive)

Théorème 2.56. *Soient C_1 et C_2 deux courbes projectives planes, sur un corps algébriquement clos, de degrés d_1 et d_2 respectivement, sans composantes communes. Soient $P_1, \ldots, P_k$ leurs points d'intersection. Alors*

$$\sum_{i=1}^{k} m(P_i; C_1, C_2) = d_1 d_2.$$

[4] Cela résulte aussi de la proposition du §1

Démonstration. On reprend la démonstration du théorème 1. On sait que les points d'intersection sont en nombre fini (par le théorème 1). On choisit un système de coordonnées projectives du plan dans lequel ces points ont des coordonnées $(t_i : x_i : y_i)$ avec $t_i \neq 0$, et ont des projections $\pi(P_i) = (t_i : x_i) \in \mathbf{P}_1$, $(1 \leq i \leq k)$ deux-à-deux distinctes. Ces points P_i sont donc dans le complémentaire de l'hyperplan $t_i = 0$, que l'on munit de sa structure de plan affine $\mathbf{A}_2(K)$. Soient $F(X,Y) = 0$ et $G(X,Y) = 0$ les équations correspondantes des courbes affines $C_1 \cap \mathbf{A}_2(K)$ et $C_2 \cap \mathbf{A}_2(K)$. Notons m_i la multiplicité du point x_i/t_i comme zéro du résultant $R(X) = \mathrm{Res}_Y(F,G)$. Ce résultant R est un polynôme en X de degré $d_1 d_2$, et ses racines sont $x_1/t_1, \ldots, x_k/t_k$, avec les multiplicités $m_1, \ldots, m_k$. Donc

$$m_1 + \cdots + m_k = d_1 d_2.$$

Rappelons que m_i dépend du choix des coordonnées, que $m_i \leq m(P_i; C_1, C_2)$, et que l'égalité a lieu pour presque tout choix des coordonnées ; plus précisément, pour tout choix "générique" de coordonnées, (c'est-à-dire sur un ouvert de Zariski), on $m_i = m(P_i; C_1, C_2)$, ce qui donne le résultat annoncé. On obtient de plus $m_i = m(P_i; C_1, C_2)$ pour tout choix de coordonnées dans lequel les x_i sont deux-à-deux distincts. □

2.9.8.4 Multiplicité d'un point sur une hypersurface.

Soit C une hypersurface projective dans $\mathbf{P}_n(K)$, et P un point de C. On va définir la multiplicité $m(P,C)$ de P sur C. On choisit un hyperplan projectif ne contenant pas P, puis un repère affine du complémentaire $\mathbf{A}_n(K)$ de cet hyperplan dans lequel P a pour coordonnées $(0, \ldots, 0)$. On écrit l'équation de $C \cap \mathbf{A}_n(K)$ sous la forme $F(X_1, \ldots, X_n) = 0$, avec $F \in K[X_1, \ldots, X_n]$. On écrit alors F comme somme de polynômes homogènes :

$$F(X_1, \ldots, X_n) = F_m(X_1, \ldots, X_n) + \cdots + F_d(X_1, \ldots, X_n),$$

avec $m \leq d$, F_i de degré d_i, $(m \leq i \leq d)$ et $F_m \neq 0$. Comme $F(0) = 0$, on a $m \geq 1$. Cet entier m ne dépend pas du choix des coordonnées choisies ; on le note $m(P,C)$. Le point P est dit *simple* (ou *régulier*) sur C si $m = 1$; dans ce cas $F_1(X_1, \ldots, X_n) = 0$ est l'équation d'un hyperplan affine, appelé *hyperplan tangent à C au point P*.

Proposition 2.57. *Soient C_1 et C_2 deux courbes projectives planes, et soit $P \in C_1 \cap C_2$. Alors*

$$m(P; C_1, C_2) \geq m(P, C_1) m(P, C_2).$$

Démonstration. Il s'agit de vérifier que si F et G sont deux éléments de $K[X,Y]$, s'écrivant sous la forme

$$F = F_r + \cdots + F_{d_1}, \qquad G = G_s + \cdots + G_{d_2}$$

avec F_i et G_j homogènes de degrés i et j respectivement, et $r \leq d_1$, $s \leq d_2$, alors leur résultant $R(X) = \mathrm{Res}_Y(F,G)$ a un zéro à l'origine d'ordre au moins rs. On reprend un argument déjà utilisé au §1 : on écrit

$$F = f_0 X^r + f_1 X^{r-1} Y + \cdots + f_r Y^r + \cdots, \qquad G = g_0 X^s + g_1 X^{s-1} Y + \cdots + g_s Y^s + \cdots$$

et le résultant s'écrit

$$\begin{pmatrix} f_0X^r & 0 & \cdots & 0 & g_0X^s & 0 & \cdots & 0 \\ f_1X^{r-1} & f_0X^r & \cdots & 0 & g_1X^{s-1} & g_0X^s & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ f_r & f_{r-1}X & \cdots & 0 & \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \end{pmatrix}.$$

On multiplie la première colonne par X^s, la seconde par X^{s-1}, ..., puis la colonne commençant par g_0X^s par X^r, la suivante par X^{r-1}, ... On a ainsi multiplié le résultant par une puissance de X, avec l'exposant

$$\sum_{i=1}^{r} i + \sum_{j=1}^{s} j = \frac{r(r+1)}{2} + \frac{s(s+1)}{2}.$$

Dans la i-ème ligne, $(1 \le i \le r+s)$, on peut mettre en facteur $X^{r+s+1-i}$, donc la multiplicité du zéro à l'origine de R est au moins

$$\sum_{i=1}^{r+s} i - \frac{r(r+1)}{2} - \frac{s(s+1)}{2} = rs.$$

□

Références complémentaires.

- Voir [9], Chap. IV, §8, p.200–204 pour la définition et les propriétés de base du résultant ; voir aussi Chap. IX, §3 et §4.
- P.Samuel. Géométrie projective ; PUF, 1986.
  Voir Chap. I, §C, p. 26–29 pour la notion de multiplicité d'un point sur une hypersurface.
- R.J. Walker. Algebraic curves ; Springer Verlag, 1978.
  Voir Chap. I, §9 et §10 pour le résultant, Chap. III, §2 pour la multiplicité d'un point sur une courbe, et Chap. III, §3 pour une forme du théorème de Bézout (tenant compte du produit des multiplicités des points sur chaque courbe). Voir aussi Chap. IV, §5 pour des compléments.
- G. and M. Orzech. Plane algebraic curves ; Marcel Dekker, 1981.
  Voir Chap. 18, p.174–178, où la multiplicité d'intersection est définie en termes des anneaux locaux des courbes au point considéré.
- R. Hartshorne. Algebraic geometry ; Springer Verlag, Graduate Texts **52** 1977.
  Pour tout savoir sur le sujet !