Constructions à la règle et au compas

Daniel PERRIN

Ce texte reprend le thème d'un TER (Travail d'Étude et de Recherche de master) posé à Orsay de nombreuses fois.

Ce thème est un peu particulier car, sur beaucoup de points, il y a des références, notamment dans des livres que j'ai moi-même écrits : [ME] et [DP] et je renverrai à ces livres pour la plupart des notions utilisées et certains résultats.

En fait, je me concentre ici sur trois points :

- *La caractérisation des extensions constructibles.*
- *Le contre-exemple d'un nombre algébrique de degré* 4 *non constructible.*
- *La construction du polygone régulier à* 17 *côtés.*

Dans ce thème, on utilise un peu de théorie de Galois. Les rudiments en sont rappelés dans l'annexe 1.

1 Introduction

Dans tout ce qui suit on ne considère que des corps de caractéristique zéro. On renvoie à [ME] chapitre 6, définitions 1.1 et 2.1 pour la définition des points et des nombres constructibles (sous-entendu, à la règle et au compas). On définit aussi :

1.1 Définition. *Soit $K \subset L$ une extension de corps. On dit que cette extension est* **constructible** *s'il existe des sous-corps $K = K_0 \subset K_1 \subset \cdots \subset K_n = L$ tels que chaque extension $K_{i-1} \subset K_i$ soit de degré ≤ 2 pour $i = 1, \ldots, n$.*

1.2 *Remarque.* Le théorème de la base télescopique (voir [DP] chapitre III, th. 1.4) montre qu'une extension constructible est finie (donc algébrique) et de degré une puissance de 2. Attention, la réciproque n'est pas vraie, voir 3.1 ci-dessous.

Le lien avec les nombres constructibles vient du théorème suivant :

1.3 Théorème. (Wantzel) *Un nombre réel x est constructible si et seulement si il existe une extension constructible $\mathbf{Q} \subset L$ telle que $x \in L$.*

En particulier un nombre constructible est algébrique de degré une puissance de 2 (mais, là encore, la réciproque est inexacte, voir 3.1).

2 Caractérisation des extensions constructibles

2.1 Proposition. *Soit $K \subset L$ une extension*[1] *normale. L'extension est constructible si et seulement $[L : K]$ est une puissance de* 2.

Démonstration. La condition est nécessaire. Le fait qu'elle est suffisante vient de la théorie de Galois et du lemme suivant :

2.2 Lemme. *Soient p un nombre premier et G un p-groupe. Il existe une suite de sous-groupes $G_0 = \{1\} \subset G_1 \subset \cdots \subset G_n = G$ tels que chaque G_{i-1} soit distingué et d'indice p dans G_i pour $i = 1, \ldots, n$.*

Démonstration. On pose $|G| = p^n$ et on raisonne par récurrence sur n. Le cas $n = 1$ est trivial. On sait que le centre Z de G n'est pas réduit à $\{1\}$. Il y a deux cas.

1) Si on a $Z \neq G$, disons $|Z| = p^d$ avec $d < n$, on a, en appliquant l'hypothèse de récurrence à Z, une suite de sous-groupes $Z_0 = \{1\} \subset Z_1 \subset \cdots \subset Z_d = Z$, d'indices p les uns dans les autres, chacun étant distingué dans le suivant. Par ailleurs, on considère le groupe quotient $H = G/Z$, de cardinal p^{n-d}. On applique l'hypothèse de récurrence à H. Il existe une suite de sous-groupes $H_0 = \{1\} \subset H_1 \subset \cdots \subset H_{n-d} = H$, d'indices p les uns dans les autres, chacun étant distingué dans le suivant. Si $\pi : G \to H$ est l'homomorphisme canonique, on obtient par image réciproque, une suite de sous-groupes $Z = \widehat{H_0} \subset \widehat{H_1} \subset \cdots \subset \widehat{H_{n-d}} = G$ avec la même propriété. En mettant bout à bout ces suites, on a le résultat voulu.

2) Si Z est égal à G, le groupe G est abélien et le raisonnement est analogue en passant au quotient par un sous-groupe N non trivial quelconque de G (par exemple engendré par un élément). Le lecteur écrira les détails.

2.3 Théorème. *Soit x un réel algébrique sur $\mathbf{Q}$, P son polynôme minimal et $L = D_{\mathbf{Q}}(P)$ le corps de décomposition de P sur $\mathbf{Q}$. Alors x est constructible si et seulement si $[L : \mathbf{Q}]$ est une puissance de* 2.

Démonstration. Comme l'extension $\mathbf{Q} \subset L$ est normale, la proposition 2.1 montre que la condition est suffisante.

Inversement, supposons x constructible de polynôme minimal P et soit $L = D_K(P)$. En vertu du théorème de l'élément primitif, on a $L = K(\alpha)$.

1. Donc galoisienne puisque la caractéristique est nulle.

Soient $x = x_1, x_2, \ldots, x_n$ les conjugués de x (c'est-à-dire les racines de P). Ils engendrent L. Si l'on montre que les x_i sont constructibles, les éléments du corps engendré le sont aussi, en particulier α, ce qui montre que L est de degré une puissance de 2.

Comme x est constructible, il est dans une extension K_n telle qu'il existe une suite de sous-corps $K = K_0 \subset K_1 \subset \cdots \subset K_n = L$, chaque extension $K_{i-1} \subset K_i$ étant de degré ≤ 2. On sait qu'il existe une extension normale M contenant K_n (voir 5.10). Cette extension est galoisienne et contient L puisqu'elle contient x et qu'elle est normale. En vertu de 5.14 il existe $\sigma_i \in \mathrm{Gal}(M/K)$ tel que $\sigma_i(x) = x_i$. Mais alors, on a la suite de corps $K \subset \sigma_i(K_1) \subset \cdots \subset \sigma_i(K_n)$, avec $\sigma_i(x) \in \sigma_i(K_n)$ et comme les σ_i sont des automorphismes, les extensions sont de degré 2, ce qui montre que x_i est constructible et on a le résultat.

3 Un contre-exemple

Le polynôme $P(X) := X^4 - X - 1$ est irréductible [2] sur $\mathbf{Q}$ et admet deux racines réelles (qui valent approximativement $-0,72$ et $1,22$). Nous allons montrer que ces racines sont des contre-exemples à l'idée naïve qu'un nombre algébrique de degré une puissance de 2 est constructible.

3.1 Théorème. *Soit x une racine réelle de $x^4 - x - 1 = 0$. Alors x est algébrique sur $\mathbf{Q}$, de degré 4, mais non constructible.*

Démonstration. Soit $L \subset \mathbf{C}$ le corps de décomposition de P. En vertu de 2.3, il suffit de montrer que le degré de L sur $\mathbf{Q}$ n'est pas une puissance de 2. Appelons x_1, x_2, x_3, x_4 les quatre racines complexes de P. On a donc une tour de sous-corps $\mathbf{Q} \subset \mathbf{Q}(x_1) \subset \mathbf{Q}(x_1, x_2) \subset \mathbf{Q}(x_1, x_2, x_3) = L$ (la dernière égalité vient de la relation $x_1 + x_2 + x_3 + x_4 = 0$ qui montre que x_4 est déjà dans $\mathbf{Q}(x_1, x_2, x_3)$). Comme P est irréductible, le degré de la première extension est 4 et on a, sur $\mathbf{Q}(x_1)$, $P(X) = (X - x_1)P_1(X)$ avec P_1 de degré 3. La deuxième extension est donc de degré ≤ 3 et elle est de degré 3 si P_1 est irréductible sur $\mathbf{Q}(x_1)$. De même la dernière extension est de degré 1 ou 2. En définitive, on voit que L est de degré $\leq 24 = 4 \times 3 \times 2$. Nous allons montrer que ce degré est multiple de 3. Pour cela, la théorie de Galois va nous servir de guide. En effet, on sait que le groupe de Galois G de L sur $\mathbf{Q}$ est un sous-groupe du groupe $\mathfrak{S}_4$ des permutations des x_i. Analysons la situation en faisant comme si c'était le groupe symétrique tout entier [3]. En

2. On le voit par réduction modulo 2, car ce polynôme n'a pas de racine dans $\mathbf{F}_2$, ni dans $\mathbf{F}_4$. En effet, les éléments de $\mathbf{F}_4$ vérifient $x^3 = 1$, donc $x^4 + x + 1 = 2x + 1 = 1$.

3. On montre facilement que c'est bien le cas.

vertu de la théorie de Galois, s'il y a une sous-extension de degré 3 dans L, elle doit apparaître comme le corps fixe d'un sous-groupe à 8 éléments de $\mathfrak{S}_4$, par exemple le groupe diédral $\mathbf{D}$ engendré par la transposition (12) et le groupe de Klein formé de l'identité et des doubles transpositions (12)(34), (13)(24) et (14)(23). Il est alors facile de fabriquer un élément candidat à être invariant par ce groupe, il suffit de prendre [4] $\alpha = x_1x_2 + x_3x_4$.

Les conjugués de α sont les transformés de α par permutation, vu l'invariance, il n'y en a plus que trois : α, $\beta = x_1x_3 + x_2x_4$ et $\gamma = x_1x_4 + x_2x_3$. On peut maintenant oublier cette phase d'analyse et prouver le lemme suivant :

3.2 Lemme. *Les éléments α, β, γ sont dans L et sont les racines du polynôme $R(Y) := Y^3 + 4Y - 1$. Ce polynôme est irréductible, de sorte que α, β, γ sont de degré 3 sur $\mathbf{Q}$ et L n'est pas constructible.*

Démonstration. On sait que α, β, γ sont racines du polynôme $Y^3 - \sigma_1 Y^2 + \sigma_2 Y - \sigma_3$ où les σ_i sont les fonctions symétriques élémentaires de α, β, γ. On a déjà $\sigma_1 = \alpha + \beta + \gamma = \sum_{i<j} x_ix_j$. Mais, ce terme est le coefficient de X^2 dans P, il est donc nul.

On a ensuite $\sigma_3 = \alpha\beta\gamma = x_1x_2x_3x_4(x_1^2 + x_2^2 + x_3^2 + x_4^2) + \sum_{i<j<k} x_i^2x_j^2x_k^2$. Mais, comme P n'a pas de terme en X^3, on a : $(x_1 + x_2 + x_3 + x_4)^2 = 0 = x_1^2 + x_2^2 + x_3^2 + x_4^2 + 2\sum_{i<j} x_ix_j$. On a vu que le dernier terme est nul et on en déduit que la somme des carrés l'est.

Par ailleurs, comme le terme en X de P, qui vaut $-\sum_{i<j<k} x_ix_jx_k$, est égal à -1, on a :

$$1 = (\sum_{i<j<k} x_ix_jx_k)^2 = \sum_{i<j<k} x_i^2x_j^2x_k^2 + 2x_1x_2x_3x_4 \sum_{i<j} x_ix_j$$

et, comme le dernier terme est nul, il en résulte qu'on a $\alpha\beta\gamma = 1$.

Enfin, calculons $\sigma_2 = \beta\gamma + \gamma\alpha + \alpha\beta = \sum_{i,j,k} x_i^2x_jx_k$. On a la relation :

$$0 = (x_1 + x_2 + x_3 + x_4) \sum_{i<j<k} x_ix_jx_k = \sigma_2 + 4x_1x_2x_3x_4$$

d'où $\sigma_2 = -4x_1x_2x_3x_4 = -4$.

On voit que α, β, γ sont les racines de R. Il reste à prouver que ce polynôme est irréductible sur $\mathbf{Q}$. Sinon, il aurait une racine rationnelle et même entière puisqu'il est unitaire et que $\mathbf{Z}$ est intégralement clos (voir [DP] p. 61 par exemple). Cette racine serait un diviseur de 1, donc ± 1, et on vérifie qu'il n'en est rien.

4. Pour le construire on prend x_1x_2 et ses transformés par le groupe $\mathbf{D}$.

4 La construction du polygone régulier à 17 côtés

4.1 Introduction

On travaille dans le plan affine euclidien rapporté à un repère orthonormé O, I, J.

Il s'agit de construire explicitement le polygone régulier à 17 côtés tracé sur le cercle unité et dont $I = (1, 0)$ est un des sommets. Pour cela il suffit de construire le nombre $\alpha = \cos\dfrac{2\pi}{17}$. En effet, on aura alors un autre sommet du polygone $M := (\cos\dfrac{2\pi}{17},\ \sin\dfrac{2\pi}{17})$ et il suffira de reporter la longueur IM sur le cercle pour obtenir les autres sommets du polygone. Si on pose $\zeta = e^{2i\pi/17}$ (racine primitive 17-ième de l'unité) on voit que 2α n'est autre que $\zeta + \zeta^{-1}$. On va donc travailler dans le corps cyclotomique $\mathbf{Q}(\zeta)$.

4.2 Rappel cyclotomique

Soit n un entier et soit $L = D_{\mathbf{Q}}(X^n - 1)$ le sous-corps de $\mathbf{C}$ engendré par les racines n-ièmes de l'unité. On rappelle (cf. [DP]) que le polynôme cyclotomique Φ_n est le polynôme à coefficients dans $\mathbf{Q}$ dont les racines sont les racines n-ièmes primitives de l'unité dans L. C'est un polynôme irréductible dont le degré est l'indicatrice d'Euler $\varphi(n)$. Si n est un nombre premier, on a $\Phi_n(X) = 1 + X + \cdots + X^{n-1}$ et il est facile de prouver l'irréductibilité.

4.1 Proposition. *Soit n un entier positif, $L = D_{\mathbf{Q}}(X^n - 1) = D_{\mathbf{Q}}(\Phi_n)$ le corps de décomposition de $X^n - 1$ sur $\mathbf{Q}$ et soit ζ une racine primitive n-ième de l'unité dans L. On a $L = \mathbf{Q}(\zeta)$. L'extension $L/\mathbf{Q}$ est galoisienne et on a un isomorphisme $\theta : G := \mathrm{Gal}(L/\mathbf{Q}) = \mathrm{Gal}(\Phi_n) \to (\mathbf{Z}/n\mathbf{Z})^*$ qui à $\sigma \in G$ associe l'entier i_σ défini par $\sigma(\zeta) = \zeta^{i_\sigma}$.*

Démonstration. Il est clair que l'extension est normale, donc galoisienne, et qu'on a $L = \mathbf{Q}(\zeta)$ car les autres racines sont des puissances de ζ. Soit $\sigma \in G$ et posons $\xi = \sigma(\zeta)$. Comme on a $\zeta^n = 1$ et que σ est un homomorphisme, on a $\xi^n = 1$, donc ξ est une racine de l'unité. De plus, en appliquant σ^{-1} à ξ, on voit que c'est une racine primitive. Elle s'écrit donc $\xi = \zeta^{i_\sigma}$ avec i_σ entier et comme $\zeta^n = 1$, on peut considérer que i_σ est un entier modulo n. Si τ est un autre élément du groupe de Galois, on a $\tau(\sigma(\zeta)) = \tau(\zeta^{i_\sigma}) = \tau(\zeta)^{i_\sigma} = \left(\zeta^{i_\tau}\right)^{i_\sigma} = \zeta^{i_\tau i_s}$. On voit que l'application $\sigma \mapsto i_\sigma$ est multiplicative. Appliquant cela avec $\tau = \sigma^{-1}$, on en déduit que i_σ est inversible modulo n.

Comme ζ engendre L, l'homomorphisme θ est injectif. Par ailleurs, on sait que le groupe $(\mathbf{Z}/n\mathbf{Z})^*$ est de cardinal $\varphi(n)$ (voir [DP] Ch. I). Comme Φ_n est irréductible, l'extension L est le corps de rupture de Φ_n, donc de degré $\varphi(n)$. Le groupe de Galois est donc de cardinal $\varphi(n)$ et l'homomorphisme est surjectif.

4.3 Le cas $n = 17$: calcul du groupe

4.2 Proposition. *Le groupe $G := \mathrm{Gal}(\Phi_{17}) \simeq H := (\mathbf{Z}/17\mathbf{Z})^*$ est un groupe cyclique d'ordre 16. Il est engendré notamment par l'homomorphisme τ défini par $\tau(\zeta) = \zeta^6$ et, si l'on pose $\sigma = \tau^2$ on a $\sigma(\zeta) = \zeta^2$.*

Démonstration. Il est bien connu que le groupe multiplicatif d'un corps fini est cyclique (voir [DP] Chapitre III Th. 2.7), donc en particulier $H = (\mathbf{Z}/17\mathbf{Z})^*$. Pour en trouver un générateur on examine d'abord le sous-groupe H_3 engendré par 2 qui contient 1, 2, 4, 8, $16 = -1$, -2, -4 et -8 (on a $-16 = 1$). C'est un sous-groupe d'ordre 8 et n'importe quel élément extérieur donne un générateur de H, par exemple 3 ($3^2 = 9 = -8$ est d'ordre 8) ou encore 6 qui a l'avantage de vérifier $6^2 = 36 \equiv 2 \pmod{17}$.

4.3 Corollaire. *Les sous-groupes de $H := (\mathbf{Z}/17\mathbf{Z})^*$ sont $\{1\} \subset H_1 \subset H_2 \subset H_3 \subset H$, où H_1 (resp. H_2, resp. H_3) est engendré par 2, (resp. 4, resp. -1) Les sous-groupes de G sont $\{1\} \subset G_1 \subset G_2 \subset G_3 \subset G$, engendrés respectivement par les automorphismes σ, σ^2, σ^4 de L qui associent à ζ les éléments ζ^2, ζ^4 et ζ^{-1}.*

Démonstration. On a déjà vu le groupe H_3. Ses sous-groupes non triviaux sont $H_2 = \{1, -1, 4, -4\}$ et $H_1 = \{1, -1\}$.

4.4 Ce que dit Galois

Une conséquence du théorème fondamental est la suivante :

4.4 Proposition. *L'extension $L/\mathbf{Q}$ est constructible. Précisément, on a la tour de sous-corps $\mathbf{Q} \subset L_3 \subset L_2 \subset L_1 \subset L$ de degrés $1, 2, 4, 8, 16$, où L_i est le corps fixe de G_i.*

Pour construire le polygone, on va construire successivement des éléments de L_3, puis de L_2, puis de L_1, chacun vérifiant une équation de degré 2 sur le corps du dessous.

4.5 Calcul des extensions intermédiaires

4.5.1 L'extension L_1

Il s'agit maintenant de décrire les extensions intermédiaires. On va le faire en descendant. Pour avoir un élément de L_1 il suffit de trouver un élément invariant par H_1, donc par σ^4, avec $\sigma^4(\zeta) = \zeta^{-1}$ et $\alpha = \alpha_1 = \zeta + \zeta^{-1}$ s'impose. On a d'ailleurs $L_1 = \mathbf{Q}(\alpha)$. En effet, il est clair que α est dans L_1, d'où l'inclusion $\mathbf{Q}(\alpha) \subset L_1$. Par ailleurs, $\mathbf{Q}(\zeta)$ est de degré au plus 2 sur $\mathbf{Q}(\alpha)$ car ζ vérifie l'équation $\zeta^2 - \alpha\zeta + 1 = 0$. Comme $\mathbf{Q}(\zeta)$ est de degré 16 sur $\mathbf{Q}$, cela montre que $\mathbf{Q}(\alpha)$ est de degré ≥ 8, donc égal à L_1.

4.5.2 L'extension L_2

Comme $L_2 \subset L_1$ est de degré 2, α vérifie une équation de degré 2 à coefficients dans L_2. Pour la trouver, il suffit de noter que le groupe de Galois de l'extension est le quotient H_2/H_1, engendré par la restriction à L_1 de l'automorphisme $\sigma^2 : \zeta \mapsto \zeta^4$. Le conjugué de $\alpha_1 = \zeta + \zeta^{-1}$ est donc $\alpha_2 = \zeta^4 + \zeta^{-4}$ et les coefficients de l'équation sont $\beta_1 = \alpha_1 + \alpha_2 = \zeta + \zeta^{-1} + \zeta^4 + \zeta^{-4}$ et $\beta_2 = \alpha_1\alpha_2 = \zeta^3 + \zeta^{-3} + \zeta^5 + \zeta^{-5}$. On vérifie qu'ils sont invariants par σ^2 donc qu'ils sont dans L_2. L'équation vérifiée par α est donc $\alpha^2 - \beta_1\alpha + \beta_2 = 0$.

4.5.3 L'extension L_3

Là encore $L_3 \subset L_2$ est de degré 2, de sorte que les β_i vérifient des équations de degré 2 à coefficients dans L_3. Le groupe de l'équation est le quotient H_3/H_2, engendré par la restriction de $\sigma : \zeta \mapsto \zeta^2$. On constate que le conjugué de β_1 est $\beta_3 = \zeta^2 + \zeta^{-2} + \zeta^8 + \zeta^{-8}$ et celui de β_2 est $\beta_4 = \zeta^6 + \zeta^{-6} + \zeta^7 + \zeta^{-7}$.

L'équation vérifiée par β_1 a donc pour coefficients $\beta_1 + \beta_3 := \gamma_1 = \zeta + \zeta^{-1} + \zeta^4 + \zeta^{-4} + \zeta^2 + \zeta^{-2} + \zeta^8 + \zeta^{-8}$ et $\beta_1\beta_3$. Ce dernier terme est la somme de tous les ζ^i distincts de 1. Il vaut donc -1 (à cause de $\Phi_{17}(\zeta) = 0$). Autrement dit, β_1 et β_3 sont les racines de $X^2 - \gamma_1 X - 1 = 0$. De même, β_2 et β_4 sont les racines de $X^2 - \gamma_2 X - 1 = 0$ avec $\gamma_2 = \zeta^3 + \zeta^{-3} + \zeta^5 + \zeta^{-5} + \zeta^6 + \zeta^{-6} + \zeta^7 + \zeta^{-7}$.

Il sera utile pour la construction de préciser les valeurs approchées des β_i : $\beta_1 \simeq 2,04948$, $\beta_2 \simeq 0,34415$, $\beta_3 \simeq -0,48792$ et $\beta_4 \simeq -2,90570$.

4.5.4 La dernière marche

Les éléments γ_1 et γ_2 étant dans L_3 sont algébriques sur $\mathbf{Q}$, de degré 2. Comme on passe de l'un à l'autre en appliquant τ, ils sont conjugués et l'équation a pour coefficients leur somme $\gamma_1 + \gamma_2 = -1$ (somme de toutes les racines primitives) et leur produit. Pour ce dernier, on a le lemme suivant :

4.5 Lemme. *On a* $\gamma_1\gamma_2 = -4$.

Démonstration. Le produit $\gamma_1\gamma_2$ est formé de 64 termes ζ^i avec $i \neq 0$. Puisque la somme $\sum_{i=-8}^{8} \zeta^i$ vaut 0, il suffit donc de montrer qu'il y a dans la somme 4 termes de chaque type. On peut bien entendu faire le calcul à la main, c'est facile, mais fastidieux. Une alternative est la suivante. On regarde par exemple le terme ζ^4. On l'obtient bien de quatre manières avec les termes de $\gamma_1\gamma_2$: $\zeta\zeta^3$, $\zeta^{-1}\zeta^5$, $\zeta^{-2}\zeta^6$ et $\zeta^{-8}\zeta^{-5}$. On en déduit qu'il en est de même pour tous les autres. En effet, si ζ^k est un terme quelconque, comme $\tau : \zeta \mapsto \zeta^6$ engendre le groupe de Galois, il existe n tel que $\zeta^{6n}\zeta^4 = \zeta^k$. Comme τ échange γ_1 et γ_2, il permute les produits de termes de γ_1 et γ_2. Ainsi, on obtiendra par exemple $\zeta^7 = \tau(\zeta)$, avec les produits $\tau(\zeta)\tau(\zeta^3) = \zeta^6\zeta$, $\tau(\zeta^{-1})\tau(\zeta^5) = \zeta^{-6}\zeta^{-4}$, $\tau(\zeta^{-2})\tau(\zeta^6) = \zeta^5\zeta^2$ et $\tau(\zeta^{-8})\tau(\zeta^{-5}) = \zeta^3\zeta^4$.

4.6 *Remarque.* Voici une autre piste pour montrer ce résultat que le lecteur détaillera à titre d'exercice :

1) Les racines de l'unité sont non seulement algébriques sur $\mathbf{Q}$, mais aussi entières sur $\mathbf{Z}$ (solutions d'équations unitaires à coefficients entiers). Il en est de même de leurs sommes, donc de γ_1 et γ_2. L'équation minimale de ces éléments est donc à coefficients entiers : $X^2 - X - n = 0$ avec $n \in \mathbf{Z}$.

2) Le discriminant de l'extension cyclotomique est 17 et $\mathbf{Q}(\zeta)$ contient donc l'extension $\mathbf{Q}(\sqrt{17})$ qui est donc égale à L_3. On en déduit facilement que l'on a $\Delta = 1 + 4n = 17k^2$ avec k entier.

3) On conclut facilement en majorant n (noter que les β_i sont ≤ 2 en valeur absolue).

Il résulte du lemme que γ_1, γ_2 sont les racines de $X^2 - X - 4 = 0$, équation de discriminant 17, et on a donc :

$$\gamma_1 = \frac{-1 + \sqrt{17}}{2} \quad \text{et} \quad \gamma_2 = \frac{-1 - \sqrt{17}}{2}.$$

4.7 *Remarque.* Pour valider ces formules, il faut vérifier que l'on a $\gamma_1 < \gamma_2$. Le plus simple est de calculer des valeurs approchées des $\zeta^k + \zeta^{-k} = 2\cos\frac{2k\pi}{17}$. On vérifie qu'on a $\gamma_1 \simeq 1,56155$ et $\gamma_2 \simeq -2,56155$.

4.6 La construction

4.6.1 Construire les racines d'une équation de degré 2

La théorie indique que c'est possible, mais on donne ici un procédé systématique et commode pour le faire. On travaille toujours dans le plan affine euclidien rapporté à un repère orthonormé O, I, J.

4.8 Proposition. *Soient b, c des nombres réels constructibles tels que b^2-4c soit positif et soient x_1, x_2 les racines (réelles) de l'équation $X^2+bX+c=0$. On considère le point $C=(0,c)$, le point $A=(-\frac{b}{2}, \frac{1+c}{2})$. Le cercle Γ de centre A passant par C passe aussi par J et les intersections de Γ avec l'axe des x sont les points d'abscisses x_1, x_2.*

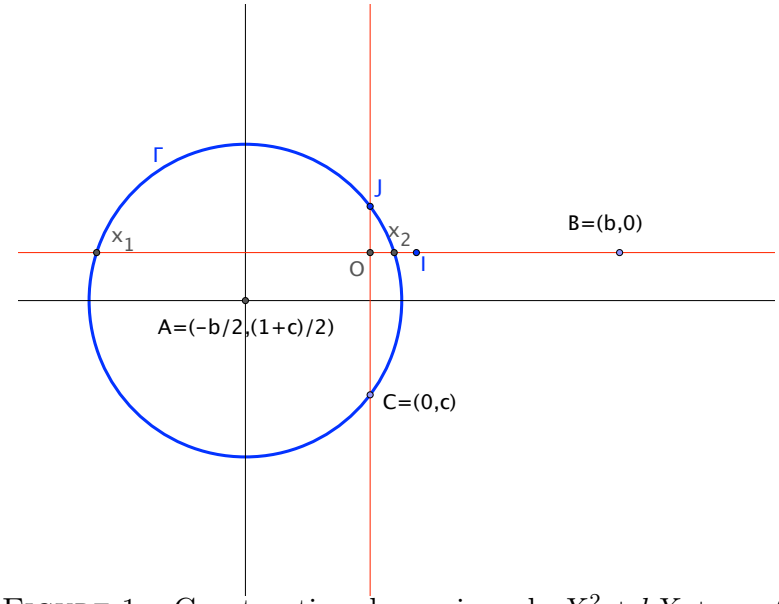

FIGURE 1 – Construction des racines de $X^2+bX+c=0$

Démonstration. Il est clair qu'on a $AC=AJ$, de sorte que Γ passe par J. On calcule alors la puissance p de O par rapport à Γ, $p=\overline{OJ}\,\overline{OC}=1.c=c$. On en déduit l'équation de Γ : $X^2+Y^2+bX-(1+c)Y+c=0$ et on voit que l'équation qui donne les points d'intersection avec l'axe des x est bien $X^2+bX+c=0$. On retrouve géométriquement ce fait en notant que si $M_1=(x_1,0)$ et $M_2=(x_2,0)$ sont ces points, le centre A est sur la médiatrice de $[M_1M_2]$, ce qui donne $\dfrac{x_1+x_2}{2}=-\dfrac{b}{2}$ et la puissance de O par rapport à Γ est $\overline{OM_1}\,\overline{OM_2}=x_1x_2$, ce qui donne $x_1x_2=c$.

4.9 *Remarque.* Avec un logiciel de géométrie, il est facile de fabriquer un outil qui réalise cette construction. C'est ce que j'ai fait avec Geogebra.

4.6.2 Construction du 17-gone

On commence par construire les racines γ_1 et γ_2 de l'équation $X^2-X-4=0$ par la méthode indiquée ci-dessus. On construit ensuite les β_i et enfin $\alpha=2\cos(2\pi/17)$. La construction du polygone est alors immédiate.

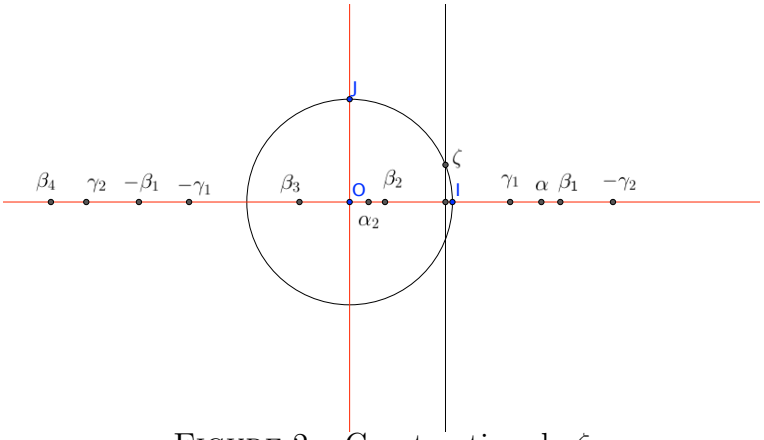

FIGURE 2 – Construction de ζ

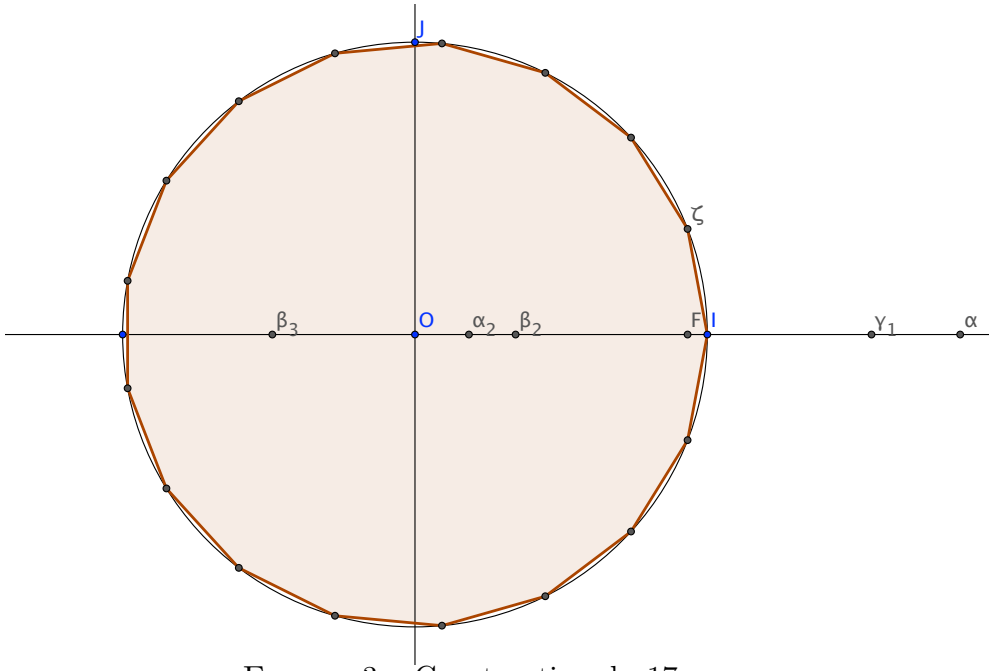

FIGURE 3 – Construction du 17-gone

5 Annexe 1 : un peu de théorie de Galois

Cette annexe vise à rappeler le b-a ba de la théorie de Galois qui est utile, dans ce sujet et dans d'autres. On utilise les notations et les résultats de [DP]. La rédaction en est parfois sommaire. Le lecteur qui souhaiterait en savoir plus ira consulter l'excellent livre de Ian Stewart [S].

5.1 Introduction

La problématique de la théorie de Galois est la suivante. On a une extension finie [5] de corps $K \subset L$ et on s'intéresse aux extensions intermédiaires $K \subset M \subset L$. Il y a plusieurs raisons pour cela :

• Quand on étudie les constructions à la règle et au compas, on doit déterminer s'il existe une "tour" d'extensions $K = K_0 \subset K_1 \subset \cdots \subset K_n = L$ dans laquelle chaque extension intermédiaire est de degré 2.

• Quand on étudie la résolution par radicaux on cherche aussi de telles tours, mais avec des extensions intermédiaires de la forme $K_{i+1} = K_i(\alpha)$ avec $\alpha^r = a$ pour $a \in K_i$ (donc où $\alpha = \sqrt[r]{a}$ est un radical).

L'idée de la théorie de Galois est d'établir un **dictionnaire** entre ces extensions intermédiaires et les sous-groupes d'un groupe fini associé à l'extension initiale et appelé groupe de Galois. Bien entendu, cela repose sur l'idée que la situation est plus simple du côté des groupes que du côté des corps, ce qui est effectivement le cas.

5.2 Le groupe de Galois

5.1 Définition. *Soit $K \subset L$ une extension. Le groupe de Galois de l'extension est le groupe des automorphismes de corps de L qui induisent l'identité sur K. On le note* $\mathrm{Gal}(L/K)$.

Rappelons qu'un automorphisme de corps est une bijection qui conserve addition et multiplication. L'idée intuitive qu'il faut avoir est la suivante :

5.2 Proposition. *Soit $K \subset L$ une extension et soit $\alpha \in L$ un élément algébrique sur K qui annule le polynôme $P \in K[X]$. Alors, si σ est un élément de* $\mathrm{Gal}(L/K)$*, il envoie α sur une (autre) racine du polynôme P.*

Démonstration. On écrit $P(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$, avec $a_i \in K$ et on applique σ. Comme il fixe K et que c'est un automorphisme, on a $\sigma(P(\alpha)) = \sigma(\alpha)^n + a_{n-1}\,\sigma(\alpha)^{n-1} + \cdots + a_1\,\sigma(\alpha) + a_0 = P(\sigma(\alpha)) = 0$.

5. Cela signifie que L est un K-espace vectoriel de dimension finie. Cette dimension s'appelle le degré de l'extension et on la note $[L : K]$

On voit que les éléments du groupe de Galois permutent les racines de P. Cela pose aussitôt deux questions :

• Les racines de P sont-elles toutes dans L ? (Autrement dit, P est-il scindé dans L ?)

• Ces racines sont-elles toutes distinctes ?

Ces questions conduisent à poser les définitions suivantes :

5.3 Définition. *Soit $K \subset L$ une extension finie.*

1) On dit que l'extension est **normale** *si pour tout polynôme irréductible $P \in K[X]$, si P a une racine dans L il est scindé sur L.*

2) On dit que l'extension est **séparable** *si pour tout polynôme irréductible $P \in K[X]$ admettant une racine dans L, ses racines (dans un corps de décomposition) sont toutes distinctes.*

3) On dit que l'extension est **galoisienne** *si elle est à la fois normale et séparable.*

5.4 *Remarques.* 1) La condition de normalité est essentielle. L'exemple type d'une extension non normale est $\mathbf{Q} \subset \mathbf{Q}(\sqrt[3]{2})$. En effet, le polynôme $X^3 - 2$ a une racine dans cette extension (réelle) mais pas les deux autres qui sont $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$.

2) Cette condition peut sembler difficile à vérifier si on veut le faire pour tout polynôme. Heureusement, on a un critère très simple : une extension est normale si et seulement si c'est le corps de décomposition $D_K(P)$ d'un polynôme $P \in K[X]$, voir [S]. Autrement dit, il suffit de vérifier la condition pour un seul polynôme. Cela montre que $\mathbf{Q} \subset \mathbf{Q}(\sqrt[3]{2}, j) = D_{\mathbf{Q}}(X^3 - 2)$ est normale.

3) La condition de séparabilité est plus délicate, mais elle est automatique en caractéristique zéro ou sur un corps fini, voir ci-dessous.

5.3 Séparabilité

5.5 Définition. *Soit $P \in K[X]$ un polynôme de degré n. On dit que P est* **séparable** *si ses n racines, dans un corps de décomposition de P, sont toutes distinctes. Sinon, on dit que P est inséparable.*

L'intérêt de cette notion est dans la proposition suivante, que nous admettrons :

5.6 Proposition. *Soit K un corps, $P \in K[X]$ un polynôme séparable et $L = D_K(P)$. L'extension L/K est séparable (donc galoisienne). On note $\mathrm{Gal}(P)$ son groupe de Galois. Inversement, toute extension galoisienne est de la forme $L = D_K(P)$ avec P séparable.*

La proposition suivante précise les polynômes séparables :

5.7 Proposition. *Soit $P \in K[X]$ un polynôme, $P = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$ sa décomposition en produit d'irréductibles sur K.*

1) Le polynôme P est séparable si et seulement si les P_i le sont et si les exposants α_i sont tous égaux à 1.

2) Si P est irréductible, il est inséparable si et seulement si son polynôme dérivé P' est le polynôme nul.

3) En caractéristique 0 tout polynôme irréductible est séparable.

4) En caractéristique p, un polynôme irréductible non séparable est de la forme $P(X) = Q(X^p)$. Sur un corps fini, tout polynôme irréductible est séparable.

Démonstration. Le point 1) est clair car deux polynômes irréductibles distincts n'ont pas les mêmes racines.

2) Dire que P n'est pas séparable c'est dire qu'il a une racine double α qui est alors racine de P'. Le *pgcd* de P et P', soit δ, est alors divisible par $X - \alpha$, donc de degré > 0. Mais, comme P est irréductible, on a $\delta = P$, donc P divise P', et cela implique $P' = 0$ pour une raison de degré.

3) On écrit $P(X) = a_n X^n + \cdots + a_0$ avec $n > 0$ et $a_n \neq 0$. On a $P'(X) = n a_n X^{n-1} + \cdots$ et ce polynôme n'est pas nul.

4) Il est clair que seuls les polynômes en X^p peuvent être inséparables puisque leur dérivée doit être le polynôme nul. Supposons K fini. Considérons un polynôme en X^p, $P(X) = a_n X^{np} + \cdots + a_1 X^p + a_0$ avec $a_i \in K$. Sur K, l'homomorphisme de Frobenius $x \mapsto x^p$ est surjectif, de sorte qu'il existe b_i tel que $a_i = b_i^p$. Mais alors, si on pose $Q(X) = b_n X^n + \cdots + b_0$, on a $P = Q^p$ (Frobenius encore !), et cela contredit l'irréductibilité de P.

5.8 Corollaire. *Si $K = \mathbf{F}_q$ et $L = \mathbf{F}_{q^n}$ sont des corps finis, l'extension $K \subset L$ est galoisienne.*

Démonstration. En effet, on a $L = D_K(X^{q^n} - X)$, de sorte que l'extension est normale et, comme K est fini, elle est séparable.

5.4 Le théorème de l'élément primitif

Le principal intérêt de la séparabilité réside dans le résultat suivant :

5.9 Théorème. (Théorème de l'élément primitif) *Soit $K \subset L$ une extension séparable. Alors, elle est monogène, autrement dit il existe $\alpha \in L$ tel que $L = K(\alpha)$.*

Par exemple, on vérifie qu'on a $\mathbf{Q}(\sqrt[3]{2}, j) = \mathbf{Q}(\sqrt[3]{2} + j)$. C'est d'ailleurs l'idée de la preuve du théorème, voir [S].

5.10 *Remarque.* On suppose K de caractéristique 0. Le théorème précédent permet de montrer que si $K \subset L$ est une extension finie, il existe une extension M contenant L et normale sur K. En effet, l'extension $K \subset L$ étant séparable, il existe un élément primitif α tel que $L = K(\alpha)$. Si P est le polynôme minimal de α, l'extension $M = D_K(P)$ convient.

5.5 Le théorème de Galois

5.5.1 La correspondance de Galois

Soit $K \subset L$ une extension et $G = \mathrm{Gal}(L/K)$ son groupe de Galois. Notons $\mathcal{K}$ l'ensemble des extensions intermédiaires $K \subset M \subset L$ et $\mathcal{G}$ l'ensemble des sous-groupes de G. On a deux applications $\Phi : \mathcal{K} \to \mathcal{G}$ et $\Psi : \mathcal{G} \to \mathcal{K}$ définies comme suit.

L'application Φ est la plus naturelle. Elle associe à M le groupe de Galois de l'extension **du haut** $H = \mathrm{Gal}(L/M)$. C'est bien un sous-groupe de G (parmi les automorphismes de L fixant K on se limite à ceux qui fixent M). **Attention** en revanche $\mathrm{Gal}(M/K)$ **n'est pas** un sous-groupe de G, voir plus loin. On note que H fixe M et cela nous conduit au point suivant.

L'application Ψ associe à un sous-groupe H de G son **corps fixe** $M = L^H$:

$$L^H = \{x \in L \ \mid \ \forall \sigma \in H,\ \sigma(x) = x\ \}.$$

5.11 *Remarques.* 1) Les applications Φ et Ψ sont décroissantes relativement à l'inclusion.

2) Le théorème de Galois affirme que, dans le cas galoisien, les applications Φ et Ψ sont réciproques l'une de l'autre. Ce qu'on peut dire d'emblée c'est que si M est dans $\mathcal{K}$ et H dans $\mathcal{G}$ on a $M \subset \Psi \circ \Phi(M)$ et $\Phi \circ \Psi(H) \supset H$.

5.5.2 Le théorème

5.12 Théorème. (Galois) *Soit $K \subset L$ une extension finie galoisienne et G son groupe de Galois. On reprend les notations ci-dessus.*

1) Le groupe G est fini et son cardinal est égal au degré de l'extension.

2) Les applications Φ et Ψ sont des bijections décroissantes réciproques l'une de l'autre.

3) Si $K \subset M \subset L$ est une extension intermédiaire, les propriétés suivantes sont équivalentes :

i) L'extension $K \subset M$ est normale.

ii) Le sous-groupe $\mathrm{Gal}(L/M)$ est distingué dans G.

iii) Pour tout $\sigma \in G$ on a $\sigma(M) = M$.

De plus, on a alors un isomorphisme : $\mathrm{Gal}(M/K) \simeq \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M)$.

Démonstration. Comme L/K est séparable, le théorème de l'élément primitif permet de l'écrire $L = K(\alpha)$, avec α de degré n, de polynôme minimal P.

1) Comme l'extension est normale, ce polynôme a n racines (distinctes) dans $L : \alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ et on a une application de G dans l'ensemble des racines qui associe à σ la racine $\sigma(\alpha)$. Comme α_i est de degré n elle engendre L, de sorte que l'application est injective. Elle est aussi surjective : si α_i est une racine de P, il existe $\sigma \in G$ tel que $\sigma(\alpha) = \alpha_i$. C'est une conséquence de l'unicité du corps de rupture, voir [DP].

2) Remarquons d'abord que si M est une extension intermédiaire, l'extension $M \subset L$ est galoisienne. En effet, si on a $L = D_K(P)$, avec P séparable, on a aussi $L = D_M(P)$.

Montrons alors que la composée $\Phi \circ \Psi$ est l'identité de $\mathcal{G}$. Soit H un sous-groupe et $M = L^H$ son corps fixe. On a $L = M(\alpha)$. Je dis que α est algébrique sur M de degré $\leq |H|$. En effet, α est racine du polynôme $Q(X) = \prod_{\sigma \in H} (X - \sigma(\alpha))$ et on voit que ce polynôme est invariant sous H (les éléments de H permutent ses facteurs). Cela montre qu'on a $[L : M] \leq |H|$. Considérons alors $H' = \mathrm{Gal}(L/M)$. On a vu ci-dessus qu'il contient H. Mais on a vu aussi en 1) qu'on a $[L : M] = |H'| \geq |H|$. On en déduit $H = H'$ comme annoncé.

Le fait que $\Psi \circ \Phi$ soit l'identité de $\mathcal{K}$ en résulte facilement.

3) On montre l'équivalence de ii) et iii), qui est facile, puis celle de i) et iii). Pour cela on utilise encore le théorème de l'élément primitif en écrivant $M = K(\beta)$ avec Q comme polynôme minimal. Supposons $K \subset M$ normale. Si on a $\sigma \in G$, comme $\sigma(\beta)$ est une racine de Q, elle est dans M et M est stable. Inversement, si M est stable, les racines de Q sont dans M qui est donc égal à $D_K(Q)$, donc normale.

Enfin, l'isomorphisme s'obtient en restreignant les éléments de G à M (qui est stable). Cela donne un homomorphisme de $\mathrm{Gal}(L/K)$ dans $\mathrm{Gal}(M/K)$, dont le noyau est $\mathrm{Gal}(L/M)$ par définition. On a donc une injection

$$\mathrm{Gal}(L/K)/\mathrm{Gal}(L/M) \subset \mathrm{Gal}(M/K)$$

et c'est une bijection car les cardinaux sont égaux (par le point 1 du théorème de Galois et celui de la base télescopique, voir [DP]).

Une conséquence importante du théorème est la suivante :

5.13 Corollaire. *Soit $K \subset L$ une extension galoisienne de groupe G. Le corps fixe de L sous G est égal à K.*

Démonstration. En effet, on a $\Phi(K) = G$, donc $\Psi(G) = L^G = K$.

5.5.3 Conjugués

Le théorème de Galois permet de préciser 5.1 et d'introduire la notion de conjugué :

5.14 Proposition-Définition. *Soit $K \subset L$ une extension galoisienne finie, $G = \mathrm{Gal}(L/K)$. Soient $\alpha, \beta \in L$. Les propriétés suivantes sont équivalentes :*
1) Les nombres α et β ont même polynôme minimal sur K.
2) Il existe $\sigma \in G$ tel que $\sigma(\alpha) = \beta$.
On dit alors que α et β sont **conjugués** *sur K.*

Démonstration. Seule l'implication $1 \Longrightarrow 2$ mérite une preuve. L'unicité du corps de rupture (voir [DP]) fournit un isomorphisme de $K[\alpha]$ sur $K[\beta]$. Celle du corps de décomposition (*loc. cit.*) permet de le prolonger en un automorphisme de $D_K(P) = M$. Enfin, la surjectivité de la restriction $\mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$ vue en 5.12 permet de conclure.

6 Annexe 2 : Discriminant

6.1 Définition et propriété caractéristique

6.1 Notations. Dans toute cette annexe on désigne par K un corps de caractéristique différente de 2, par P un polynôme de degré $n > 0$ à coefficients dans K et par L son corps de décomposition $L = D_K(P)$. On suppose que le polynôme P est séparable c'est-à-dire qu'il admet n racines distinctes dans L, que l'on note $x_1, \ldots, x_n$. L'extension L/K est alors galoisienne et on note G son groupe de Galois, qui s'injecte dans le groupe symétrique $\mathfrak{S}_n$ par la formule : $g(x_i) = x_{\sigma_g(i)}$ (voir **??**).

6.2 Proposition-Définition. *On pose $\delta = \prod_{1 \le i < j \le n} (x_i - x_j)$ et $\Delta = \delta^2 = \prod_{1 \le i < j \le n} (x_i - x_j)^2$. Le nombre*[6] *$\Delta$ est appelé* **discriminant** *du polynôme P.*
Les nombres δ et Δ sont des éléments de L^* et on a la formule

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

Le signe $(-1)^{n(n-1)/2}$ est égal à 1 si $n \equiv 0, 1 \pmod 4$ et à -1 sinon.

Démonstration. Il suffit de compter les signes $-$, donc les couples (i, j) avec $i > j$, il y en a bien $n(n-1)/2$.

6. On le note $\Delta(P)$ lorsqu'on veut préciser de quel polynôme il est le discriminant.

6.3 *Remarque.* Attention, certains auteurs prennent $\Delta = \prod_{i\neq j}(x_i - x_j)$ comme définition du discriminant, mais la proposition suivante montre que c'est mal adapté à la théorie de Galois.

6.4 Proposition. *Soit g un élément de G et σ_g la permutation associée.*
1) On a les formules $g(\delta) = \epsilon(\sigma_g)\delta$ et $g(\Delta) = \Delta$.
2) Le discriminant Δ est dans K^* (et pas seulement dans L^*).
3) On a les équivalences :

$$\delta \in K^* \iff \Delta \in K^{*2} \iff G \subset \mathfrak{A}_n.$$

Démonstration. La formule avec δ résulte du comptage du nombre d'inversions[7] de σ_g et celle avec Δ est évidente. Le point 2) en résulte car K est le corps fixe de G, voir 5.13. Enfin, le point 3) résulte lui aussi de 1) : si G est formé de permutations paires, les éléments de G fixent δ et inversement.

6.5 *Exemple.* Calculons le discriminant du polynôme du second degré $ax^2 + bx + c$. Ses racines sont x_1 et x_2 et on a $\Delta = (x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = \big(-\frac{b}{a}\big)^2 - 4\frac{c}{a} = \frac{b^2 - 4ac}{a^2}$.

6.2 Calcul du discriminant

6.6 Notations. On reprend les notations précédentes mais on suppose de plus que P est unitaire :

$$P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0.$$

On suppose que la caractéristique du corps ne divise pas n. On considère le polynôme dérivé $P'(x)$ et on note $y_1, \ldots, y_{n-1}$ ses racines. On a donc :

$$P'(X) = nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \cdots + a_1 = n\prod_{j=1}^{n-1}(X - y_j).$$

6.7 Théorème. *Soit Δ le discriminant de P. On a les formules :*

$$\Delta = (-1)^{n(n-1)/2}\prod_{i=1}^{n} P'(x_i) = (-1)^{n(n-1)/2}\prod_{i,j}(x_i - y_j) = (-1)^{n(n-1)/2}n^n\prod_{j=1}^{n-1} P(y_j).$$

7. Voire de la définition de la signature que l'on peut donner par cette formule, vue dans l'anneau de polynômes $K[x_1, \ldots, x_n]$.

Démonstration. On part de la formule $P(X) = \prod_{i=1}^{n}(X - x_i)$ que l'on dérive :

$$P'(X) = \sum_{i=1}^{n}(X - x_1)\cdots(\widehat{X - x_i})\cdots(X - x_n)$$

où le chapeau signifie que le terme correspondant est omis. On calcule alors $P'(x_i)$. Tous les termes de la somme sont nulles sauf celui où l'on a omis x_i et on a donc, pour i fixé, $P'(x_i) = \prod_{j,j\neq i}(x_i - x_j)$. On en déduit la valeur du produit $\prod_{i=1}^{n} P'(x_i) = \prod_{i,j,\,j\neq i}(x_i - x_j)$ et la première formule vient de 6.2. En utilisant l'expression de P' en fonction de ses racines, on a $P'(x_i) = n\prod_{j=1}^{n-1}(x_i - y_j)$ d'où $\prod_{i=1}^{n} P'(x_i) = n^n \prod_{i,j}(x_i - y_j)$ et la seconde formule. Mais on a aussi $P(y_j) = \prod_{i=1}^{n}(y_j - x_i)$ et donc $\prod_{j=1}^{n-1} P(y_j) = \prod_{i,j}(y_j - x_i)$. Par rapport à l'expression précédente, chaque terme $x_i - y_j$ est changé de signe, ce qui fait $n(n-1)$ changements. Comme ce nombre est pair, le signe est le même et on a bien la troisième formule.

Ces formules permettent de calculer le discriminant du polynôme du troisième degré :

6.8 Proposition. *Le discriminant de $P(X) = X^3 + pX + q$ est $\Delta = -4p^3 - 27q^2$.*

Démonstration. On calcule $P'(X) = 3X^2 + p$ dont les racines sont $y_j = \pm\sqrt{-\dfrac{p}{3}}$, $j = 1, 2$, et on vérifie que le produit $P(y_1)P(y_2)$ vaut $A = \dfrac{27q^2 + 4p^3}{27}$. On a alors $\Delta = -27A$ et le résultat.

6.9 *Exercice.* Montrer que le discriminant de $P(X) = X^n + pX + q$ est donné par la formule :

$$\Delta = (-1)^{n(n-1)/2}\left(n^n q^{n-1} + (-1)^{n-1}(n-1)^{n-1}p^n\right).$$

6.3 Le cas cyclotomique

6.10 Proposition. *1) Soit n un entier quelconque premier à la caractéristique de K. On a $\Delta(X^n - 1) = (-1)^{(n-1)(n+2)/2}\, n^n$.*

2) Soit n un nombre premier impair. On a $\Delta(\Phi_n) = (-1)^{n(n-1)/2} n^{n-2}$.

Démonstration. 1) On peut calculer avec la formule utilisant les $P'(x_i)$, mais ici, il est bien plus simple d'utiliser l'autre. Si l'on pose $P(X) = X^n - 1$ on a $P'(X) = nX^{n-1}$ et son unique racine est 0. On a donc $P(y_j) = -1$ pour tout j et la formule en découle (c'est d'ailleurs un cas particulier de $X^n + pX + q$, voir exercice ci-dessus).

2) Ici, on va utiliser la formule avec les $P'(x_i)$. On a $X^n - 1 = (X-1)\Phi_n(X)$ ce qui donne $\Phi_n(X) = X^{n-1} + \cdots + X + 1$ et aussi, en dérivant, $nX^{n-1} = (X-1)\Phi'_n(X) + \Phi_n(X)$ et, si on applique cela avec $X = \zeta^i$, ζ racine n-ième primitive et $i = 1, \ldots, n-1$, on trouve $n\zeta^{i(n-1)} = (\zeta^i - 1)\Phi'_n(\zeta^i)$. On a donc $\Phi'_n(\zeta^i) = \dfrac{n\zeta^{i(n-1)}}{\zeta^i - 1}\cdot$ Comme on a $\zeta^n = 1$, le numérateur est égal à ζ^{-i} et le produit de ces termes est le coefficient constant de Φ_n, soit 1, au signe $(-1)^{n-1}$ près. Les $\zeta^i - 1$, eux, sont les racines du polynôme $\Phi_n(X+1) = (X+1)^{n-1} + \cdots + (X+1) + 1 = X^{n-1} + \cdots + n$ et leur produit est donc $(-1)^{n-1}n$. En définitive, on a $\Delta(\Phi_n) = (-1)^{n(n-1)/2} n^{n-1} \prod_{i=1}^{n-1} \Phi'_n(\zeta^i) = (-1)^{n(n-1)/2} n^{n-2}$.

7 Références

[DP] PERRIN Daniel, *Cours d'Algèbre*, Ellipses, 1996.

[ME] Daniel PERRIN, *Mathématiques d'école*, Cassini, 2011.

[S] STEWART Ian, *Galois theory*, Chapmann-Hall, 1973.

[Serre] SERRE Jean-Pierre, *Cours d'arithmétique*, PUF, 1970.