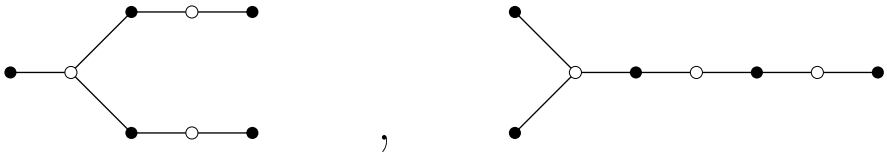
Groupe de travail pour élèves de lycée



et $\sqrt{21}$

par

Dimitri Zvonkine

(Texte produit et tapé par Xavier Caruso)

Le 25 mai 2003

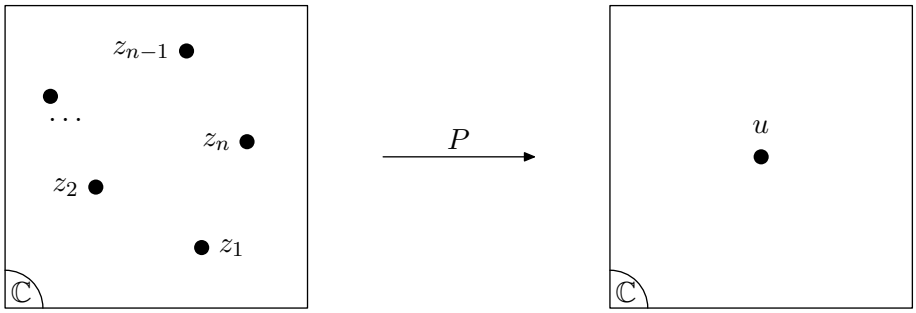
Table des matières

1 Dessins d'enfants

1.1 Image réciproque d'un point par un polynôme

Dans tout ce qui suit, tous les polynômes P que nous considérons sont à coefficients dans le corps des nombres complexes, $\mathbb{C}$.

Soient un polynôme P et un nombre complexe u. On s'intéresse aux antécédents de u, c'est-à-dire aux nombres complexes z vérifiant $P(z) = u$. La situation générique est dans ce cas la suivante :



où n désigne le degré du polynôme P. Cependant, il n'y a pas toujours n antécédents, il peut y en avoir moins. Il se peut que pour certaines valeurs particulières de u, deux antécédents se confondent.

Pour illustrer ce point, prenons l'exemple simple du polynôme $P(z) = z^2$. Il est de degré 2 et de fait l'équation $z^2 = u$ a toujours deux racines, disons δ et $-\delta$. Cependant en 0, ces deux racines 0 et -0 se regroupent et n'en forment plus qu'une. On a ce que l'on appelle une *racine double*.

De fait, la situation générale est exactement celle-ci. Il se peut que pour certains u, des racines qui étaient auparavant distinctes se confondent et n'en forment plus qu'une seule. Le phénomène peut mettre en jeu plus de deux racines, bien entendu. On parle alors, selon le nombre, de racines triples, quadruples, *etc.*

Un antécédent multiple se voit très bien déjà sur le polynôme : z_0 est un antécédent de u d'ordre k si $P(z) - u$ est divisible par $(z - z_0)^k$ (et pas plus). On peut considérer un nouvel exemple, celui du polynôme $P(z) = z^3(z-1)^2$. Il est de degré 5, donc il y a génériquement cinq antécédents, mais si on prend $u = 0$, on constate que les deux seules racines sont 0 et 1, 0 étant racine triple et 1 racine double.

Une autre remarque importante à faire est qu'il existe une façon de lire la présence ou l'absence de racines doubles en regardant la dérivée. Plus précisément, supposons que z_0 soit racine (au moins) double de P. On a alors vu que P pouvait s'écrire :

$$P(z) = (z - z_0)^2 Q(z)$$

où Q est un nouveau polynôme. Mais alors il suffit de dériver pour trouver :

$$P'(z) = 2(z - z_0) Q(z) + (z - z_0)^2 Q'(z) = (z - z_0)\left[2Q(z) + (z - z_0) Q'(z)\right]$$

et donc constater que z_0 est encore racine de P' simple cette fois-ci. De façon générale, on voit que si z_0 est une racine d'ordre k de P, alors c'est aussi une racine d'ordre $k-1$ de P'.

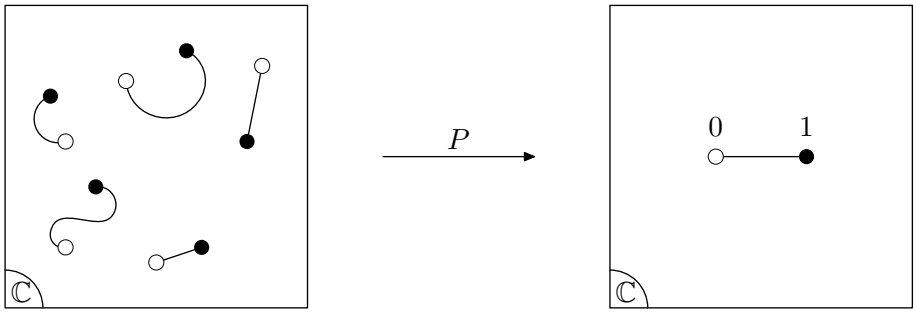
Outre cette dernière remarque qui est intéressante en soi et que l'on réutilisera par la suite, on est maintenant en mesure de donner un critère sur le nombre complexe u pour qu'il admette des antécédents multiples. Cela se produit si, et seulement si les polynômes $P(z) - u$ et $P'(z)$ ont une racine commune ou, ce que revient au même, si ces polynômes ne sont pas premiers entre eux. Cette dernière condition se caractérise par l'annulation de ce que l'on appelle leur *résultant*[1]. Retenons ici simplement que ce résultant s'exprime comme un polynôme en u.

Fixons finalement un peu de terminologie. Un complexe z est un *point critique* du polynôme P si $P'(z) = 0$. Si z est un point critique de P, le nombre $u = P(z)$ s'appelle une *valeur critique* de P. Une définition équivalente : un nombre complexe u est valeur critique de P si et seulement si u admet des antécédents multiples par P.

Un polynôme P de degré n a au plus $n-1$ points critiques distincts et au plus $n-1$ valeurs critiques distinctes.

1.2 Image réciproque d'un segment par un polynôme

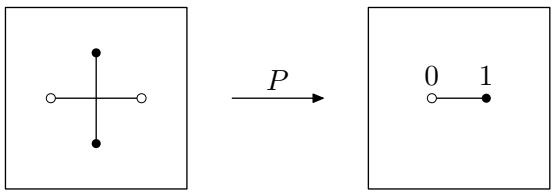
Si maintenant, on ne cherche plus les antécédents d'un complexe u mais les antécédents de tout un segment, on va avoir le dessin générique suivant :



où les extrémités du segment sont repérées par des gros points de deux couleurs différentes qui nous nommerons *vide* et *plein*[2]. Bien sûr, les points vides (resp. pleins) à gauche correspondent respectivement aux antécédents du point vide (resp. plein) de droite.

On supposera dans toute la suite que le point vide se trouve en 0 et le point plein en 1. Ce n'est pas forcément nécessaire mais cela simplifiera la présentation. En contrepartie, il se peut que certaines expressions deviennent un peu plus compliquées.

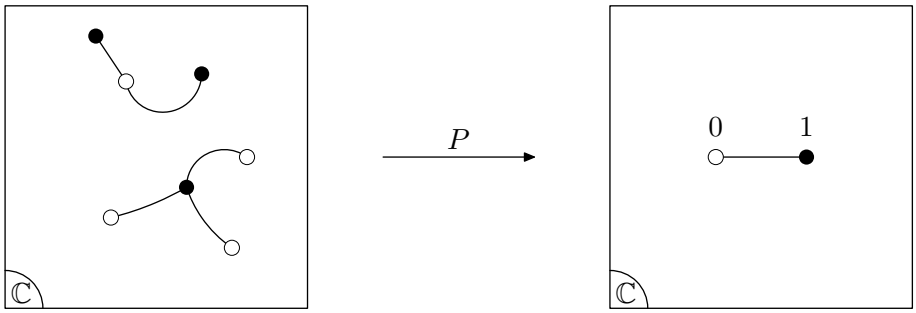
Ceci était le cas le plus général, mais il nous intéressera peu dans cet exposé. Étudions plutôt la situation lorsque une (ou plusieurs) valeur critique entre en jeu. Soit celle-ci est située sur l'intervalle ouvert $]0,1[$, soit elle est à l'une des deux extrémités. La première possibilité correspond au dessin suivant :



[1] Voir l'annexe pour plus de détails.

[2] On n'utilise pas blanc et noir afin de ne pas être soumis à l'encre que l'on utilise. En particulier, cela devient souvent troublant lorsque l'on utilise un tableau sur lequel on écrit en blanc sur vert.

La seconde possibilité peut-être illustrée par le dessin suivant :



Ici 0 admet un antécédent double et 1 un antécédent triple, ce que l'on constate facilement en regardant le nombre de branches qui partent du point vide ou plein correspondant.

On constate aussi que pour déterminer le degré du polynôme, il suffit de compter le nombre de segments, puisque l'on suppose que les points de l'intervalle ouvert $]0,1[$ ne sont pas des valeurs critiques. Cette dernière hypothèse assure que les segments dessinés à gauche ne peuvent ni être confondus, ni même se croiser.

Si l'on connaît un peu les graphes, on reconnaît sur le dessin de gauche un graphe planaire[3] et bipartite[4], pas forcément connexe[5].

Montrons que le graphe antécédent du segment $[0,1]$ ne peut pas avoir de cycles[6]. En effet, supposons que ce graphe possède un cycle, et soit $x \in \mathbb{C}$ un point du plan complexe encerclé par ce cycle. Considérons son image $u = P(x)$. Soit γ une courbe continue dans $\mathbb{C}$ qui part de u et s'en va à l'infini sans couper le segment $[0,1]$. Il est évident qu'une courbe comme cela existe toujours. La courbe γ a n antécédents par P. Un de ces antécédents, disons β, part du point x. (Plus précidément, si x est un antécédent de u de multiplicité k, alors il y a k antécédents de γ partant de x.) Nous avons donc construit une courbe β qui part de x et s'en va à l'infini. De plus, cette courbe ne coupe pas le graphe $P^{-1}([0,1])$ (sinon γ couperait le segment $[0,1]$). L'existence d'une telle courbe β contredit la supposition selon laquelle x est encerclé par le graphe. Par conséquent, le graphe ne peut pas avoir de cycles.

1.3 Le cas le plus dégénéré

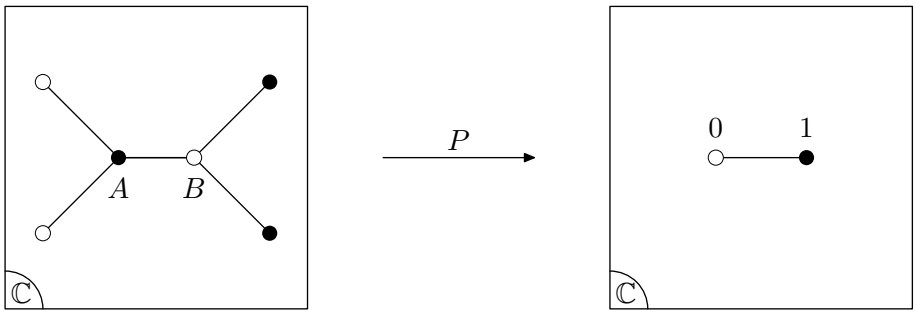
Nous allons nous intéresser à présent au cas encore plus particulier où l'antécédent du segment par le polynôme P est un graphe connexe. Un graphe connexe sans cycle s'appelle un *arbre*. Par exemple on peut avoir :

[3] Cela signifie que l'on peut le représenter dans le plan sans que deux arêtes ne se croisent.

[4] Cela signifie que les sommets sont coloriés en deux couleurs, en l'occurrence vide et plein, de telle sorte que deux sommets reliés par une arête soient toujours de couleurs distinctes.

[5] Un graphe connexe est un graphe en un seul morceau, ou, plus formellement, tel que l'on peut, pour tout couple de sommets, trouver un chemin les reliant.

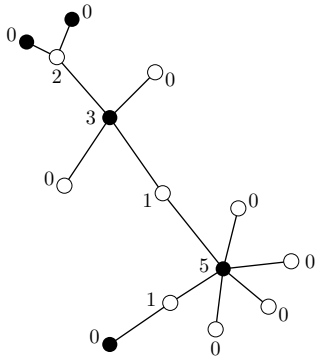
[6] Un cycle est un chemin fermé dans le graphe, non réduit à un sommet.



On remarque dans un premier temps que le degré du polynôme P est donné par le nombre d'arêtes de l'arbre. Ici P est donc de degré 5.

D'autre part, on constate sur le dessin précédent que le point A correspond ici à un antécédent triple de 1, le point B à un antécédent triple de 0. En particulier, ces deux points correspondent à des racines doubles de $P'(z)$. Mais P' est un polynôme de degré 4 ; on a donc déjà toutes ses racines.

Ceci est en réalité un fait général. Considérons par exemple l'arbre suivant et supposons qu'il corresponde à un certain polynôme que l'on ne donnera certainement pas.



Reportons maintenant à côté de chaque sommet, le nombre de racines de la dérivée que le sommet en question fournit. Et maintenant comptons. D'une part, l'arbre a 13 arêtes, ce qui prouve que le polynôme associé est de degré 13. Et d'autre part, on a trouvé $2+3+1+5+1 = 12$ racines de la dérivée. Le compte est bon : on les a toutes.

On laisse en exercice au lecteur de montrer (par récurrence sur le nombre de sommets) que ce résultat reste vrai pour tout arbre.

1.4 À tout arbre correspond un polynôme

Avant d'énoncer le théorème qui précise le titre de cette section, il nous faut faire une remarque. L'arbre que l'on construit, comme expliqué précédemment, à partir d'un polynôme P ne vient pas tout nu mais au contraire avec des données supplémentaires.

Tout d'abord, on a en plus de l'arbre une coloration des sommets en deux couleurs, et ce, de telle façon qu'une arête relie toujours deux sommets de couleurs différentes. Autrement dit, on ne récupère pas seulement un arbre mais un arbre bipartite.

En outre, cet arbre est dessiné dans le plan complexe. Il n'est pas très difficile de se convaincre que si l'on se donne un arbre abstrait (qu'il soit bipartite ou pas ne change rien à l'affaire), il existe souvent plusieurs façons de le représenter dans le plan, possibilités que

l'on ne peut en général pas déduire l'une de l'autre en déplaçant l'arbre sur le plan. En fait, pour que cette représentation soit unique, il faut se donner ce que l'on appelle un *arbre plan*. Un arbre plan est un arbre accompagné de la donnée supplémentaire pour chaque sommet d'un *ordre cyclique* sur l'ensemble des arêtes adjacentes. Cet ordre correspond à l'ordre trigonométrique dans lequel les arêtes adjacentes apparaissent autour du sommet.

Bref, tout cela pour dire qu'à un polynôme, il correspond bien plus qu'un arbre, il correspond un arbre plan bipartite. Il faut peut-être tout de suite mettre le doigt sur une erreur à ne pas commettre : il ne faut pas croire qu'à tout polynôme correspond un arbre. Comme on l'a déjà dit, dans le cas générique, l'image réciproque du segment $[0, 1]$ ressemble plutôt à une union disjointe de courbes qu'à autre chose. De fait, les polynômes qui correspondent à des arbres sont « rares » (pour n'importe quel sens raisonnable qu'on pourrait être tenté de donner à ce mot) mais il n'empêche que ce sont ces polynômes qui nous intéressent.

Le théorème tant attendu est le suivant :

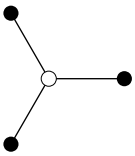
Théorème 1. *À tout arbre plan bipartite correspond un polynôme. Ce polynôme est unique à la transformation $P(z) \mapsto P(az + b)$ près, $a \neq 0$ et b étant des nombres complexes.*

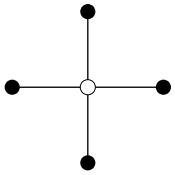
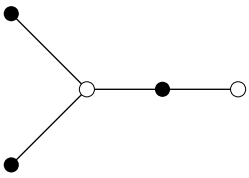
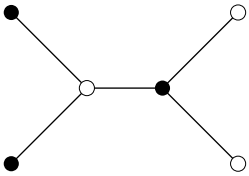
Il est intéressant de remarquer que la transformation précédente correspond simplement à une similitude directe dans le plan de départ, celui de gauche si l'on se rappelle des dessins précédents.

Nous n'allons pas prouver ce théorème. Il s'appuie sur le théorème d'existence de Riemann dont il serait bien difficile de donner une formulation et une preuve accessibles.

1.5 Les premiers arbres et les polynômes correspondants

On se propose, plus modestement, de déterminer les polynômes qui correspondent aux premiers arbres, en fait jusqu'à quatre arêtes. Le résultat est résumé ci-après :

Arbre	Polynôme
	$z \mapsto z$
	$z \mapsto z^2$
	$z \mapsto z^3$
	$z \mapsto cz^2(z-1)$

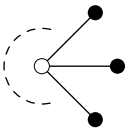
Arbre	Polynôme
	$z \mapsto z^4$
	$z \mapsto cz^3(z-1)$
	$z \mapsto cz^2(z-1)^2$
	$z \mapsto c\left(\frac{z^5}{5} - \frac{z^4}{2} + \frac{z^3}{3}\right)$

Il s'agit maintenant d'expliquer comment l'on aboutit au tableau précédent. Comme le stipule le théorème 1, il n'y a pas un unique polynôme convenable à chaque fois. Et plus précisément, on peut avant de commencer à déterminer le polynôme fixer les coordonnées de deux sommets quelconques du graphe.

Pour le premier graphe par exemple, on peut commencer par demander au point vide d'être à la position 0 et au point plein d'être à la position 1. Il reste à trouver un polynôme P de degré 1 tel que $P(0) = 0$ et $P(1) = 1$. C'est évidemment $P(z) = z$.

On fait de même pour le deuxième : on demande au point vide d'être en 0 et au point plein de droite d'être en 1. Il s'agit alors de trouver un polynôme P de degré 2 admettant 0 pour racine double et tel que $P(1) = 1$. C'est $P(z) = z^2$.

On peut, dès à présent, généraliser le raisonnement précédent à l'arbre suivant composé de n arêtes.



En effet, si on place le point vide en 0 et le point plein de droite en 1, on voit que le polynôme P que l'on cherche devra satisfaire aux conditions suivantes :

- P est de degré n,
- P admet une racine de multiplicité n en 0,
- $P(1) = 1$.

Cela impose directement $P(z) = z^n$.

On remarque finalement que dans la représentation « véritable » de l'arbre dans $\mathbb{C}$, tous les points pleins sont également espacés sur le cercle unité et les arêtes les reliant au point vide sont des segments de droite.

On comprend alors comment sont obtenus les polynômes z^3 et z^4 dans le tableau précédent. Expliquons maintenant comment on détermine le polynôme associé à l'arbre tout en bas à gauche : on commence par placer les deux points vides en 0 et en 1, mettant par exemple le point qui correspond à une racine double en 0. Le polynôme recherché est donc de degré 3, admet une racine double en 0 et une racine simple en 1. Il est de la forme $P(z) = cz^2(z-1)$. Il reste, si on veut être complet à déterminer la constante c. Pour cela, on impose que P vaille 1 sur un point plein, ce qui nous amène naturellement à déterminer la position des points pleins.

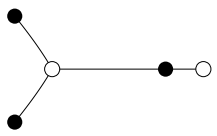
Le point plein situé entre les deux points vides correspond à un antécédent double, c'est donc une racine simple de la dérivée P' donnée par $P'(z) = c\left(3z^2 - 2z\right)$. Ce point plein est donc situé à la position $\frac{2}{3}$ et il nous faut imposer $P\left(\frac{2}{3}\right) = 1$, ce qui détermine $c = -\frac{27}{4}$.

Il est alors possible de calculer la position du second point plein. Il correspond à l'autre solution de $P(z) = 1$. On trouve $-\frac{1}{3}$. On aurait pu également utiliser un argument de symétrie prouvant que la figure était invariante par la symétrie centrale de centre $\frac{1}{3}$ (au changement de couleur près), ce qui fournit le résultat plus rapidement.

On observe finalement que comme le polynôme est à coefficients réels, les courbes reliant les sommets dont on vient de calculer les positions sont des segments de droite. Finalement, la représentation « véritable » de notre arbre dans $\mathbb{C}$ est la suivante :

Sautons l'arbre suivant puisqu'il a déjà été traité et passons donc au cinquième. Comme précédemment, on demande aux points vides d'être situés en 0 et en 1 et on obtient la forme du polynôme $P(z) = cz^3(z-1)$. Le point plein situé entre les deux points vides correspond à une racine de la dérivée $P'(z) = c\left(4z^3 - 3z^2\right)$. Il est donc situé en $\frac{3}{4}$. En écrivant $P\left(\frac{3}{4}\right) = 1$, on obtient $c = -\frac{256}{27}$.

On peut alors déterminer la position des autres sommets. Il s'agit de résoudre $P(z) = 1$ et on sait déjà que $\frac{3}{4}$ est une racine double. On calcule donc ; les solutions sont $\frac{-1 \pm i\sqrt{2}}{4}$. Finalement, si les traits horizontaux restent des segments pour des raisons de symétrie, il n'en est pas de même des autres arêtes. Pour information, la représentation « véritable » de cet arbre dans $\mathbb{C}$ est :



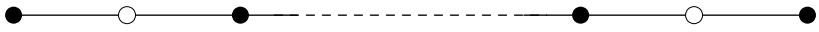
Passons à l'arbre suivant. Encore une fois, en positionnant en 0 et en 1 les points vides, on voit que P est de la forme $P(z) = cz^2(z-1)^2$. Le point plein du milieu correspond encore à une racine de la dérivée, $\frac{1}{2}$ en fait pour des raisons de symétrie. La constante c vaut donc 16 ici. Pour trouver la position des points pleins restants, il s'agit de résoudre $z^2(z-1)^2 = \frac{1}{16}$, soit $z(z-1) = \pm\frac{1}{4}$. Avec le signe « $-$ », on retrouve la racine double $\frac{1}{2}$. Avec le signe « $+$ », on trouve $z = \frac{1 \pm \sqrt{2}}{2}$. L'arbre plongé dans $\mathbb{C}$ correctement se dessine donc :

Pour le dernier arbre, il est plus simple de changer de stratégie car on ne peut pas fixer la position des trois points vides. On s'intéresse donc plutôt aux racines de la dérivée. Les points vide et plein centraux correspondent à deux racines doubles de la dérivée. Ainsi, si l'on fixe leur position respectivement en 0 et en 1, on a nécessairement $P'(z) = c\left(z^2 - z\right)^2$. Finalement en intégrant, on trouve $P(z) = c\left(\frac{z^5}{5} - \frac{z^4}{2} + \frac{z^3}{3} + k\right)$. Il reste donc à déterminer les constantes c et k à l'aide des conditions $P(0) = 0$ et $P(1) = 1$, qui fournissent $k = 0$ et $c = 30$.

On pourrait terminer en déterminant la position des sommets restants, mais, pour une fois, nous laissons ce plaisir au lecteur. Voici toutefois la représentation « véritable » de cet arbre plongé dans $\mathbb{C}$.

1.6 Les polynômes de [7]

Il est une famille d'arbres pour laquelle on sait déterminer les polynômes correspondants. Il s'agit des arbres de la forme suivante :



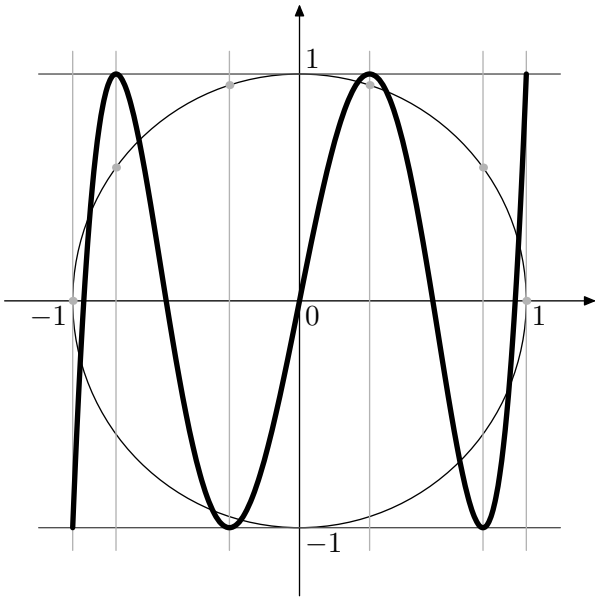
où le nombre de sommets est $n+1$ (les sommets aux extrémités ne sont pas forcément de la même couleur).

Cet arbre correspond au n-ième polynôme de (à une transformation près). On rappelle que les polynômes de sont définis par la relation $P_n(\cos\alpha) = \cos(n\alpha)$, qui doit être vérifiée pour tout réel α.

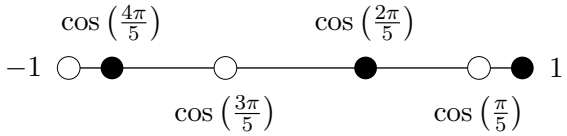
Par exemple comme $\cos(2\alpha) = 2\cos^2\alpha - 1$. le deuxième polynôme de est $P_2(z) = 2z^2 - 1$. De même, comme $\cos(2\alpha) = 4\cos^3\alpha - 3\cos\alpha$, le troisième polynôme de est $P_3(z) = 4z^3 - 3z$. Plus généralement, on vérifie simplement en développant qu'il existe de telles formules pour tout entier n.

Essayons de comprendre maintenant pourquoi ces polynômes correspondent aux arbres précédemment cités. Une première étape consiste à dessiner la courbe $y = P_n(z)$. Grâce à un changement de variable judicieux, on constate que ce n'est autre que la courbe définie paramétriquement par $x(\alpha) = \cos\alpha$ et $y(\alpha) = \cos n\alpha$. Pour $n = 5$, on obtient donc le graphe suivant :

[7] Évidemment, ceci est l'écriture russe de Tchebychev. Dimitri, en bon russe, tient à cette orthographe.

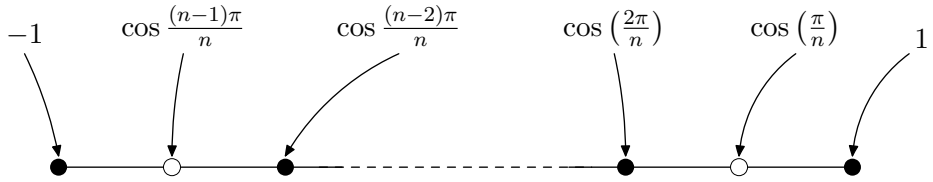


les traits verticaux fins coupant le cercle aux sommets d'un 10-gone régulier. On voit alors avec les yeux quels sont les antécédents du segment $[-1,1]$. C'est :



et les arêtes sont véritablement des segments.

Le cas général est exactement identique ; l'image réciproque du segment $[-1,1]$ par le polynôme P_n est représentée par le graphe :

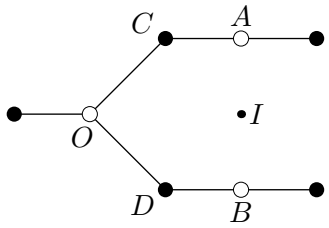


Remarquons finalement que dans ce qui précède le segment image considéré est $[-1,1]$ et non $[0,1]$ comme on le voudrait. Cependant, pour palier à ce problème, il suffit de remplacer le polynôme P_n par $Q_n = \frac{P_n+1}{2}$.

1.7 Le premier arbre irrationnel

Jusqu'à présent, tous les polynômes que l'on a déterminés étaient à coefficients rationnels, mais ce n'est pas forcément le cas : il se peut que l'on ait des équations à résoudre nécessitant l'extraction de racines carrées, voire pire.

Le plus petit exemple pour cela est l'arbre suivant :



On remarque tout d'abord que cet arbre a 7 arêtes et donc le polynôme P qui lui correspond est de degré 7. Notons maintenant, comme sur le dessin précédent, O, A et B les sommets vides et I le milieu de $[AB]$. Positionnons O en 0 et I en 1. Le nombre 0 est alors racine triple de P. Par ailleurs, P admet deux autres racines doubles que l'on ne connaît pas *a priori* mais dont on connait la demi-somme : c'est 1. Ainsi P s'écrit sous la forme suivante :

$$P(z) = cz^3\left(z^2 - 2z + a\right)^2,$$

où a est un nombre complexe à déterminer.

Pour se faire, calculons les positions des points C et D. Ces points correspondent à des racines simples de la dérivée qui s'écrit :

$$P'(z) = cz^2\left(z^2 - 2z + a\right)\underbrace{\left(7z^2 - 10z + 3a\right)}_{Q(z)}$$

Ainsi, avec des notations évidentes, z_C et z_D sont les solutions de l'équation $Q(z) = 0$. On veut imposer $P(z_C) = P(z_D)$ $(= 1)$. On remarque alors astucieusement que $Q(z_C) = Q(z_D) = 0$. Si R est le reste de la division euclidienne de P par Q, la condition $P(z_C) = P(z_D)$ est équivalente à $R(z_C) = R(z_D)$. Après calcul, on obtient l'expression suivante pour R :

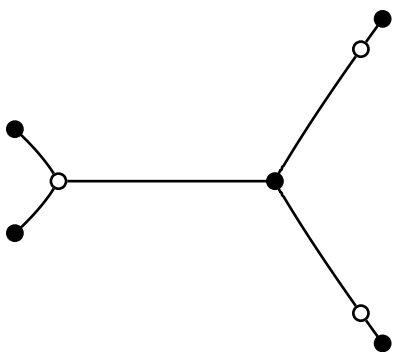
$$R(z) = -\frac{16}{7^6}\left[(21a - 25)\left(49a^2 - 476a + 400\right)z + 12a\,(28a - 25)\,(7a - 10)\right]$$

qui est un polynôme de degré 1 ; pour qu'il prenne la même valeur en z_C et z_D, il faut et il suffit que son terme en z soit nul. On est donc ramené à résoudre l'équation :

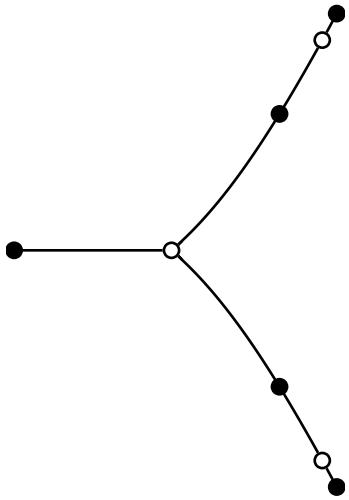
$$(21a - 25)\left(49a^2 - 476a + 400\right) = 0,$$

qui admet trois solutions : $\frac{25}{21}$, $\frac{34+6\sqrt{21}}{7}$ et $\frac{34-6\sqrt{21}}{7}$. Il ne reste plus qu'à déterminer parmi ces trois solutions laquelle est la bonne. Pour cela, on dessine simplement les arbres correspondant aux trois hypothétiques solutions, et on procède par élimination.

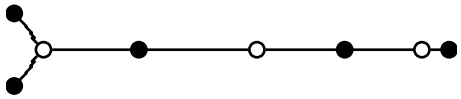
Pour $a = \frac{25}{21}$, on obtient :



Pour $a = \frac{34+6\sqrt{21}}{7}$, on obtient :



Pour $a = \frac{34-6\sqrt{21}}{7}$, on obtient :



Finalement $a = \frac{34+6\sqrt{21}}{7}$. Reste à déterminer c. Cela est pénible et n'a en fait aucun intérêt. Un exercice intéressant par contre, que le lecteur peut vouloir faire, est de reconnaître sur chacun des trois dessins précédents les points O, A, B, C et D.

Terminons par une remarque. Il aurait été possible de discréditer d'office $a = \frac{25}{21}$. En effet, ce cas correspond à $z_C = z_D$, alors que les points C et D sont supposés distincts. Par contre, il est bien plus délicat de choisir entre les deux autres arbres. Plus précisément, et dans un sens qui sera rendu précis par la suite, il n'est pas possible d'écrire une quelconque équation algébrique qui permette de trouver le polynôme de l'un des arbres sans trouver celui de l'autre. Il est nécessaire de parler d'inégalités, d'approximations ou de choses équivalentes pour pouvoir discréditer $a = \frac{34-6\sqrt{21}}{7}$

2 Un peu de théorie de Galois

2.1 Qu'est-ce qu'un corps ?

Nous n'allons pas à proprement parler définir la notion de corps, nous préférons nous restreindre aux sous-corps de $\mathbb{C}$. Cela est amplement suffisant pour notre propos, et demande un effort d'abstraction infiniment inférieur, ce qui a pour conséquence de faciliter grandement la compréhension.

Un *sous-corps de* $\mathbb{C}$ est une partie de $\mathbb{C}$ contenant 0 et 1 et stable par les quatre opérations usuelles (qui sont addition, soustraction, multiplication et division[8]).

Remarquons que tout sous-corps de $\mathbb{C}$ contient au moins les nombres rationnels. En effet, comme par hypothèse, il contient 1, il contient également $2 = 1 + 1$ puis $3 = 2 + 1$,

[8]Bien sûr pour la division, on suppose en outre que l'on ne divise pas par 0.

et ainsi de suite, il contient tous les entiers positifs. La stabilité par soustraction assure que $0-n=-n$ est aussi élément du corps. Alors la stabilité par quotient prouve que tous les rationnels sont présents. On remarque également que l'on ne peut pas faire mieux : l'ensemble des nombres rationnels forme un sous-corps de $\mathbb{C}$.

Il y a cependant d'autres sous-corps de $\mathbb{C}$. Il y a par exemple $\mathbb{C}$ lui-même, ou $\mathbb{R}$, l'ensemble des nombres réels, ou des constructions un peu plus farfelues comme :

$$\mathbb{Q}(\sqrt{21})=\left\{a+b\sqrt{21},\quad a,b\in\mathbb{Q}\right\}$$

Il est clair que ce dernier ensemble contient 0 et 1 et est stable par addition, soustraction et multiplication. Le seul point délicat est la stabilité par quotient, mais l'astuce de la quantité conjuguée permet de conclure :

$$\frac{a+b\sqrt{21}}{c+d\sqrt{21}}=\frac{\left(a+b\sqrt{21}\right)\left(c-d\sqrt{21}\right)}{c^2-21d^2}$$

Soit K un sous-corps de $\mathbb{C}$. Un *automorphisme* de K est, par définition, une bijection $\varphi : K\to K$ qui respecte l'addition et la multiplication, c'est-à-dire telle que :

$$\begin{aligned}\varphi(x+y) &= \varphi(x)+\varphi(y)\\ \varphi(xy) &= \varphi(x)\,\varphi(y)\end{aligned}$$

Bien sûr, l'identité de K est toujours un automorphisme mais il y en a parfois d'autres. Par exemple, si $K=\mathbb{Q}\left(\sqrt{21}\right)$, on peut vérifier que la conjugaison $a+b\sqrt{21}\mapsto a-b\sqrt{21}$ est un automorphisme.

Avant d'étudier plus en détails ces automorphismes, il convient de dégager au moins les propriétés suivantes, essentielles.

Propriété 1. *Soit K un sous-corps de $\mathbb{C}$. Alors tout automorphisme φ de K agit trivialement sur les rationnels, (c'est-à-dire $\varphi(x)=x$ pour tout rationnel x).*

Si, en outre, $\alpha\in K$ est une racine d'un polynôme P à coefficients rationnels, alors tout automorphisme φ de K envoie α sur une racine de P, qui peut éventuellement être encore α.

Ces propriétés ne sont pas difficiles mais donnons quand même leur preuve pour familiariser le lecteur avec la notion. Pour le premier point, considérons φ un automorphisme de K. Il vérifie $\varphi(0)+\varphi(0)=\varphi(0)$. On en déduit immédiatement que $\varphi(0)=0$. De même, on a $\varphi(1)\,\varphi(1)=\varphi(1)$ et donc $\varphi(1)$ vaut 0 ou 1. Mais $\varphi(1)$ ne peut valoir 0 puisque φ est supposé bijectif. Donc $\varphi(1)=1$.

On calcule $\varphi(2)=\varphi(1)+\varphi(1)=2$, puis $\varphi(3)=\varphi(2)+\varphi(1)=3$ et ainsi de suite, on obtient $\varphi(n)=n$ pour tout entier naturel n. En écrivant $\varphi(-n)+\varphi(n)=\varphi(0)=0$, on déduit $\varphi(-n)=-n$ encore pour n entier naturel. Si, pour finir, p et q sont deux entiers relatifs et q est non nul, on a $\varphi\left(\frac{p}{q}\right)\varphi(q)=\varphi(p)$ et donc $\varphi\left(\frac{p}{q}\right)=\frac{p}{q}$.

Expliquons maintenant la preuve de la seconde assertion. Supposons que P s'écrive $P(z)=a_nz^n+\ldots+a_1z+a_0$, les a_i étant des nombres rationnels. On a par hypothèse :

$$a_n\alpha^n+\ldots+a_1\alpha+a_0=0$$

En appliquant φ à l'égalité ci-dessus, on obtient directement

$$a_n\varphi(\alpha)^n + \ldots + a_1\varphi(\alpha) + a_0 = 0,$$

puisque, d'une part, φ respecte les opérations et, d'autre part, φ ne modifie pas les rationnels d'après le premier point. La dernière équation écrite assure que $\varphi(\alpha)$ est encore une racine de P.

On est maintenant en mesure de déterminer complètement les automorphismes du corps $\mathbb{Q}\left(\sqrt{21}\right)$. D'après la propriété précédente, un tel automorphisme envoie forcément $\sqrt{21}$ sur une racine du polynôme $z^2 - 21$, et les seules racines de ce polynôme sont $\sqrt{21}$ et $-\sqrt{21}$. Il suffit alors de constater qu'une fois que l'on a fixé l'image de $\sqrt{21}$, l'image de tout élément de $\mathbb{Q}\left(\sqrt{21}\right)$ est *ipso facto* fixée, du fait de la formule :

$$\varphi(a + b\sqrt{21}) = a + b\varphi(\sqrt{21})$$

On déduit de tout cela que les seuls automorphismes de $\mathbb{Q}\left(\sqrt{21}\right)$ sont l'identité et la conjugaison.

2.2 Qu'est-ce que le groupe de Galois d'un corps ?

Si K est un sous-corps de $\mathbb{C}$, on appelle *groupe de Galois* de K l'ensemble des automorphismes de K. (En général, on définit le groupe de Galois d'une extension plutôt que celui d'un corps, et on se garde bien de le faire lorsque l'extension n'est pas galoisienne, mais peu importe pour cet exposé). On note cet ensemble $\mathrm{Gal}(K)$.

Précédemment, on a donc prouvé que $\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{21}\right)\right)$ est un ensemble réduit à deux éléments : l'identité et la conjugaison.

Si φ et ψ sont deux automorphismes de K, leur composée $\varphi \circ \psi$, qui consiste à appliquer ψ, puis φ, est également un automorphisme. On peut donc introduire sur l'ensemble des automorphismes une *loi de composition* associative, qui à φ et ψ associe $\varphi \circ \psi$. De plus, l'identité est un automorphisme de n'importe quel corps. Et, finalement, si φ est un automorphisme, alors φ^{-1} en est un aussi. On dit que les automorphismes de K forment un *groupe*.

Il est facile de décrire la loi de composition sur $\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{21}\right)\right)$: l'identité composée avec n'importe quel élément de $\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{21}\right)\right)$ ne modifie pas cet élément, et lorsque l'on applique deux fois la conjugaison successivement, on obtient l'identité. Si on connait un peu de théorie des groupes, cela signifie $\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{21}\right)\right)$ est isomorphe au groupe $\mathbb{Z}/2\mathbb{Z}$.

Prenons un nouvel exemple. Considérons :

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \left\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}, \quad a, b, c, d \in \mathbb{Q}\right\}$$

Comme avant, pour déterminer le groupe de Galois de ce corps, il suffit de déterminer les images possibles de $\sqrt{2}$, $\sqrt{3}$ et $\sqrt{6}$. On remarque en outre que $\sqrt{6} = \sqrt{2} \times \sqrt{3}$, de sorte qu'il suffit de déterminer les images possibles de $\sqrt{2}$ et $\sqrt{3}$. Mais $\sqrt{2}$ s'envoie nécessairement sur $\sqrt{2}$ ou sur $-\sqrt{2}$ et on a une condition analogue pour $\sqrt{3}$. Il y a donc au plus quatre possibilités. Autrement dit le groupe $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ est de cardinal au plus 4.

Définissons par ailleurs la 2-conjugaison par :

$$c_2\left(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}\right) = a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$$

et la 3-conjugaison par :

$$c_3\left(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\right)=a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6}$$

On vérifie sans peine que ces deux applications sont des automorphismes de notre corps, ainsi d'ailleurs que $c_2 \circ c_3$. On a ainsi trouvé quatre éléments de $Gal(\mathbb{Q}(\sqrt{2},\sqrt{3}))$ deux à deux distincts, et donc d'après ce qui précède, on a complètement décrit ce groupe. On vérifie en outre que $c_2 \circ c_2 = c_3 \circ c_3 = \mathrm{id}$ et que $c_2 \circ c_3 = c_3 \circ c_2$ (*i.e.* c_2 et c_3 commutent). Pour ceux qui connaissent la théorie des groupes, le groupe $Gal(\mathbb{Q}(\sqrt{2},\sqrt{3}))$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$.

Problème ouvert. Un problème encore ouvert à ce jour est ce que l'on appelle le *problème de Galois inverse*. Il consiste à déterminer si tous les groupes finis[9] peuvent être réalisés comme de tels groupes de Galois. Autrement dit, étant donné un groupe abstrait, peut-on trouver un corps dont c'est le groupe de Galois ? Bien que l'on conjecture que cela soit vrai, on est encore loin de savoir le prouver complètement.

2.3 La clôture algébrique de $\mathbb{Q}$

Nous allons nous intéresser tout particulièrement par la suite à un certain sous-corps de $\mathbb{C}$ que l'on définit sans plus tarder. Il s'agit du corps des nombres algébriques que l'on note traditionnellement $\overline{\mathbb{Q}}$.

Un nombre complexe z est dit *algébrique* s'il existe un polynôme à coefficients rationnels P tel que $P(z)=0$. Par exemple, $\sqrt{21}$ est algébrique comme solution de $z^2-21=0$. De même i ou $\sqrt[3]{7}$ le sont. Tous les nombres ne sont toutefois pas algébriques, ces derniers formant même un ridicule ensemble dénombrable. Le premier nombre non algébrique à avoir été exhibé est celui de Liouville défini par :

$$\sum_{i=0}^{\infty}\frac{1}{10^{i!}}$$

Plus récemment, il a été prouvé que ni π, ni e ne sont algébriques.

Avant de continuer il nous reste à voir que $\overline{\mathbb{Q}}$ est un sous-corps de $\mathbb{C}$. Bien sûr, 0 et 1 sont algébriques, le point plus délicat est de prouver que $\overline{\mathbb{Q}}$ est stable par les quatre opérations classiques. Nous n'allons en fait traiter que l'addition, les autres cas étant similaires. Et nous allons pour cela présenter pas moins de trois méthodes.

Commençons par un exemple : comment pourrait-on prouver que $x=\sqrt{2}+\sqrt{3}$ est algébrique ? On peut commencer par calculer $x^2=5+2\sqrt{6}$ afin d'obtenir $\left(x^2-5\right)^2=24$, ce qui fournit bien une preuve. Cependant, cette méthode ne s'applique pas si bien lorsque x vaut, par exemple, $\sqrt[3]{2}+\sqrt[3]{5}$. Lorsque l'on élève au carré ou au cube, le nombre de termes génant croît plutôt que de diminuer. Mais ne nous effrayons pas : calculons quand même

[9] Il est connu que les groupes infinis ne peuvent pas tous se réaliser comme groupes de Galois.

ces termes et dressons un tableau pour marquer les résultats.

	1	$\sqrt[3]{2}$	$\sqrt[3]{4}$	$\sqrt[3]{5}$	$\sqrt[3]{10}$	$\sqrt[3]{20}$	$\sqrt[3]{25}$	$\sqrt[3]{50}$	$\sqrt[3]{100}$
x^0	1								
x^1		1		1					
x^2			1		2		1		
x^3	7					3		3	
$\vdots$					$\vdots$				

Comme dirait Dimitri[10], il n'y a maintenant même pas besoin de connaître de l'algèbre linéaire pour être convaincu que, lorsque l'on aura rempli les dix premières lignes du tableau, une des lignes pourra être exprimée comme combinaison linéaire des autres. Ceci fournit un polynôme à coefficients rationnels, dont $\sqrt[3]{2}+\sqrt[3]{5}$ est solution. Voici notre première méthode, dont on peut se convaincre qu'elle aboutit à coup sûr.

La seconde méthode est celle des conjugués. Voyons comment on procède pour $x = \sqrt[3]{2}+\sqrt[3]{5}$. On sait que $\sqrt[3]{2}$ est solution d'une équation polynomiale, en l'occurence $z^3-2=0$, les autres solutions étant $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$, où j est $\frac{-1+i\sqrt{3}}{2}$. De même, $\sqrt[3]{5}$ est solution de l'équation polynomiale $z^3-5=0$, les autres solutions étant $j\sqrt[3]{5}$ et $j^2\sqrt[3]{5}$. On considère alors le polynôme dont les racines sont les diverses sommes que l'on peut former à partir des nombres précédents. Précisement, on regarde le polynôme

$$\begin{aligned} P(z) &= \left(z-\sqrt[3]{2}-\sqrt[3]{5}\right)\left(z-j\sqrt[3]{2}-\sqrt[3]{5}\right)\left(z-j^2\sqrt[3]{2}-\sqrt[3]{5}\right) \\ &\quad \left(z-\sqrt[3]{2}-j\sqrt[3]{5}\right)\left(z-j\sqrt[3]{2}-j\sqrt[3]{5}\right)\left(z-j^2\sqrt[3]{2}-j\sqrt[3]{5}\right) \\ &\quad \left(z-\sqrt[3]{2}-j^2\sqrt[3]{5}\right)\left(z-j\sqrt[3]{2}-j^2\sqrt[3]{5}\right)\left(z-j^2\sqrt[3]{2}-j^2\sqrt[3]{5}\right) \end{aligned}$$

La somme $\sqrt[3]{2}+\sqrt[3]{5}$ en est évidemment une racine, et ce dernier polynôme est à coefficients rationnels comme le lecteur pourra s'en apercevoir s'il s'amuse à le développer. En réalité, un théorème de la théorie de Galois assure que cette construction convient en toutes circonstances.

Nous allons finalement présenter la troisième méthode, et ce dans le cas général. Supposons donc que l'on dispose de deux polynômes P et Q tels que $P(\alpha)=Q(\beta)=0$ et que l'on cherche à construire un nouveau polynôme R vérifiant, lui, $R(\alpha+\beta)=0$. L'idée consiste à introduire deux nouveaux polynômes à deux variables, définis par :

$$\begin{aligned} \widetilde{P}(X,Y) &= P(X) \\ \widetilde{Q}(X,Y) &= Q(Y-X) \end{aligned}$$

Ces deux derniers polynômes vérifient $\widetilde{P}(\alpha,\alpha+\beta)=\widetilde{Q}(\alpha,\alpha+\beta)$. En particulier, les polynômes en une variable (en l'occurrence X) $\widetilde{P}(X,\alpha+\beta)$ et $\widetilde{Q}(X,\alpha+\beta)$ ont une racine commune (en l'occurrence α), et donc ne sont pas premiers entre eux.

[10] Il ne l'a pas dit mais il était pas loin de « Même sans avoir fait d'algèbre linéaire, tout le monde sait que dans un espace de dimension 9, une famille de cardinal 10 est forcément liée ».

Mais le résultant[11] fournit un critère pour déterminer si deux polynômes sont premiers entre eux. Ici le résultant des polynômes (vus comme polynômes en X) $\widetilde{P}(X,t)$ et $\widetilde{Q}(X,t)$ où t est une nouvelle variable s'exprime comme un polynôme en t et s'annule lorsque ces polynômes (en X) ne sont pas premiers entre eux, ce qui arrive lorsqu'ils ont une racine commune, et en particulier lorsque $t = \alpha + \beta$ (la racine commune est alors $X = \alpha$). Le résultant fournit donc au final un polynôme qui s'annule en $\alpha + \beta$ comme on le voulait.

2.4 Gal $(\bar{\mathbb{Q}})$ et son action sur les arbres

On s'intéresse ici au groupe de Galois de $\overline{\mathbb{Q}}$. Le comprendre, le décrire, ou même l'appréhender, est une question très difficile au cœur de nombreuses théories mathématiques actuelles qui sont parmi les plus florissantes.

Remarquons modestement que ce groupe est infini, mais que l'on ne peut exhiber de façon simple que deux de ses éléments qui sont l'identité et la conjugaison complexe. Notons que la conjugaison définie précédemment sur $\mathbb{Q}(\sqrt{21})$ qui envoyait $\sqrt{21}$ sur $-\sqrt{21}$ se prolonge d'une infinité de façons en un élément de Gal $\left(\overline{\mathbb{Q}}\right)$, mais trouver un prolongement est loin d'être simple.

Peu importe. Ce qui nous intéresse ici, c'est de faire *agir* ce groupe de Galois compliqué sur les arbres plans bipartites. Précisément, étant donnés un automorphisme de $\overline{\mathbb{Q}}$ et un arbre plan bipartite, on veut montrer comment l'on '« applique »cet automorphisme à cet arbre pour obtenir un nouvel arbre (plan bipartite).

On aimerait en outre que deux conditions naturelles soient respectées : d'une part, si l'on fait agir l'identité sur n'importe quel arbre, celui-ci ne doit pas être modifié, et d'autre part, faire agir d'abord l'automorphisme φ puis l'automorphisme ψ doit revenir à faire agir la seule composée $\psi \circ \varphi$.

Expliquons à présent comment est définie cette action. Soit donc un arbre plan bipartite. D'après le théorème 1, il existe un polynôme à coefficients complexes qui correspond à cet arbre. En fait, on peut raffiner ce théorème 1 et montrer que l'on peut toujours choisir un polynôme à coefficients dans $\overline{\mathbb{Q}}$. Précisément, on a le théorème suivant, version améliorée du théorème 1.

Théorème 2. *À tout arbre plan bipartite correspond un polynôme à coefficients dans* $\overline{\mathbb{Q}}$. *Ce polynôme est unique à la transformation* $P(z) \mapsto P(az+b)$ *près,* a *et* b *étant des éléments de* $\overline{\mathbb{Q}}$.

On choisit un tel polynôme associé à l'arbre plan bipartite considéré. On applique alors φ à ce polynôme, simplement en appliquant φ à chacun des coefficients. À ce nouveau polynôme, il correspond un nouvel arbre plan bipartite[12] que l'on définit finalement comme le résultat de l'action de φ sur l'arbre de départ.

Il faut quand même vérifier que l'arbre que l'on obtient à l'arrivée ne dépend pas du choix du polynôme, mais c'est immédiat : si au lieu de $P(z)$, on avait choisi $P(az+b)$ pour a et b des éléments de $\overline{\mathbb{Q}}$, on aurait obtenu au final $\varphi(P)(\varphi(a)z + \varphi(b))$ qui correspond bien au même arbre que le polynôme $\varphi(P)$, image de P par φ.

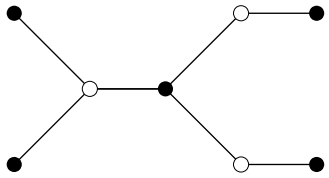
[11] Voir l'annexe pour plus de détails.

[12] Bien que totalement passé sous silence pendant l'exposé, ce point n'est pas totalement clair. Il s'agit de voir que le polynôme obtenu donne bien naissance à un arbre et non pas à quelconque autre graphe, et pour cela il s'agit de voir que ce nouveau polynôme admet exactement deux valeurs critiques qui doivent être 0 et 1 (voir l'annexe pour plus de détails). Mais cela n'est pas difficile puisque l'on peut voir que les valeurs critique du polynôme d'arrivée sont les images par φ de celles du polynôme de départ et φ fixe évidemment les nombres 0 et 1.

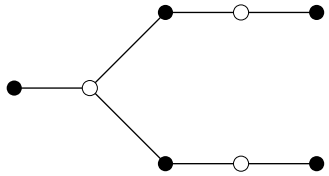
2.5 Des arbres conjugués et d'autres pas

Reprenons les trois arbres que l'on avait déterminés à la fin de la première partie. Rappelons qu'il y avait :

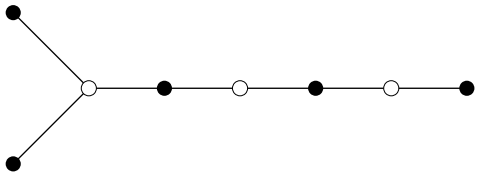
· pour $a = \frac{25}{21}$



· pour $a = \frac{34+6\sqrt{21}}{7}$



· pour $a = \frac{34-6\sqrt{21}}{7}$



Il existe un élément de $\mathrm{Gal}\left(\overline{\mathbb{Q}}\right)$ qui permet d'aller du deuxième arbre au troisième. En fait, tout élément de $\mathrm{Gal}\left(\overline{\mathbb{Q}}\right)$ qui envoie $\sqrt{21}$ sur $-\sqrt{21}$ convient, et on a dit qu'un tel élément existait, bien qu'il soit difficile d'en déterminer explicitement un.

Par contre, le premier arbre est « rationnel » (*i.e.* défini par un polynôme à coefficients rationnels) et donc l'action de n'importe quel élément $\varphi \in \mathrm{Gal}\left(\overline{\mathbb{Q}}\right)$ laisse cet arbre invariant. En conclusion, il n'est pas lié aux deux autres comme précédemment.

Rappelons-nous qu'à la fin de la première partie, nous avions dit qu'il était plus délicat de distinguer les deux derniers arbres que de distinguer par exemple le premier du troisième. Cette heuristique se traduit mathématiquement exactement par l'assertion que nous venons de prouver : il n'est pas possible de passer du premier arbre au troisième par l'action d'un élément de $\mathrm{Gal}\left(()\,\bar{Q}\right)$, mais il est par contre possible de passer du second au troisième par un tel procédé.

Pour formaliser un peu les choses qui précèdent, introduisons un peu de terminologie : deux arbres sont dits *conjugués* lorsqu'il existe un élément $\varphi \in \mathrm{Gal}\left(\overline{\mathbb{Q}}\right)$ qui envoie l'un de ces arbres sur l'autre. L'*orbite* d'un arbre est l'ensemble des arbres qui lui sont conjugués. Ainsi on vient de provuer que les deux derniers arbres dessinés sont conjugués et que le premier arbre dessiné est seul dans son orbite. On laisse au lecteur le soin de prouver qu'en fait les deux derniers arbres sont également seuls dans leur orbite.

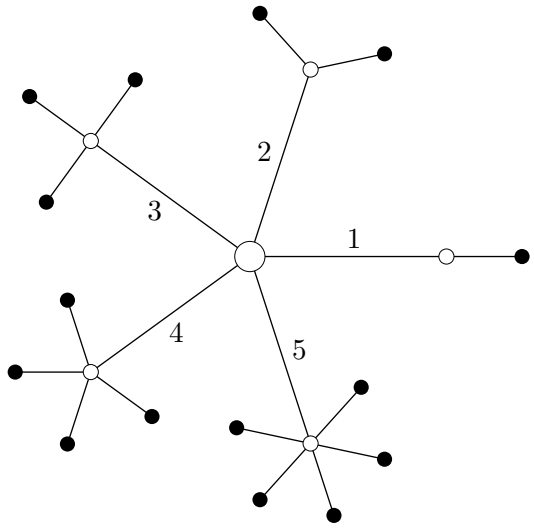
Désormais, la question naturelle est de savoir comment reconnaître deux arbres conjugués. Il n'y a pas de réponse claire et définitive mais on peut toutefois exhiber des invariants simples qui permettent de répondre dans plus d'un cas. Deux arbres conjugués ont :

1. même nombre d'arêtes.
2. même (multi-)ensemble des degrés des sommets vides (resp. pleins). En particulier, ils ont même nombre de sommets vides (resp. pleins).
3. mêmes symétries[13].

Ces invariants ne permettent pas de prouver que deux arbres sont conjugués mais permettent de voir que deux arbres ne le sont pas. En particulier, la deuxième condition prouve directement que les arbres correspondant respectivement à $a = \frac{25}{21}$ et $a = \frac{34+6\sqrt{21}}{7}$ ne sont pas conjugués : le multi-ensemble des sommets pleins du premier arbre est $\{1, 1, 1, 1, 3\}$, celui du second arbre est $\{1, 1, 1, 2, 2\}$.

2.6 La fleur de Leila

Il est hélas possible que deux arbres non conjugués ne puissent être distingués par les méthodes précédentes. L'exemple est celui de la fleur de Leila, représentée ci-dessous ;



On constate en premier lieu que cet arbre n'a aucune symétrie. D'autre part, chaque fois que l'on dispose d'une permutation de l'ensemble $\{1, 2, 3, 4\}$ on peut construire un nouvel arbre, simplement en permutant les branches marquées 1, 2, 3 et 4 sur le dessin comme le veut la permutation.

On obtient ainsi 24 arbres tous distincts qui ont tous même nombre d'arêtes, même ensemble de degrés des sommets pleins (resp. vides) et mêmes symétries. Cependant, on peut montrer que tous ces arbres ne sont pas conjugués. Précisément, ils se répartissent en deux orbites, correspondant respectivement aux permutations paires et aux permutations impaires.

3 Quelques compléments

3.1 La correspondance de Galois

On considère ici K un sous-corps de $\mathbb{C}$ inclus dans $\overline{\mathbb{Q}}$ (on dit encore un sous-corps de $\overline{\mathbb{Q}}$). Soit $\alpha \in K$ et soit P le polynôme unitaire à coefficients rationnels de plus bas degré

[13] Une symétrie étant un automorphisme de l'arbre plan bipartite. Nous laissons au lecteur le soin de donner une définition claire de cette notion.

qui annule α. Les *conjugués* de α sont par définition les autres racines complexes de P ; ils appartiennent encore à $\overline{\mathbb{Q}}$. On dit que K est une *extension galoisienne* de $\mathbb{Q}$ si pour tout élément $x \in K$, tous les conjugués de x sont aussi dans K.

Regardons des exemples. Considérons en premier lieu le corps $K = \mathbb{Q}\left(\sqrt{2}\right)$. Un élément $x \in K$ s'écrit $x = a + b\sqrt{2}$, où a et b sont des nombres rationnels. Le polynôme de plus bas degré annulant x, est :

$$P(z) = z^2 - 2az + \left(a^2 - 2b^2\right).$$

L'autre racine de ce polynôme est $a - b\sqrt{2}$, qui est élément de $\mathbb{Q}\left(\sqrt{2}\right)$. Le corps $\mathbb{Q}\left(\sqrt{2}\right)$ est donc une extension galoisienne de $\mathbb{Q}$.

Toutefois, le corps $K = \mathbb{Q}\left(\sqrt[3]{2}\right)$ n'est pas une extension galoisienne de $\mathbb{Q}$. En effet, le polynôme à coefficients rationnels de plus bas degré annulant $\sqrt[3]{2}$ est $z^3 - 2$ et ses autres racines sont $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$ qui ne sont pas des éléments de K.

Soient K une extension galoisienne de $\mathbb{Q}$ et G son groupe de galois. Si H est un sous-groupe de G (c'est-à-dire un sous-ensemble de G stable pour la composition), notons K^H l'ensemble des éléments de K stables par tous les automorphismes de H. On montre facilement (et on laisse l'exercice au lecteur) que K^H est un sous-corps de K. Si L est un sous-corps de K, notons G^L l'ensemble des éléments du groupe G qui laissent tous les éléments de L invariants. C'est un sous-groupe de G, (exercice laissé au lecteur).

Théorème 3. *Soient K une extension galoisienne de $\mathbb{Q}$ et G son groupe de Galois. On suppose que G est fini.*

Les correspondances $H \mapsto K^H$ et $L \mapsto G^L$ sont des bijections inverses l'une de l'autre entre l'ensemble des sous-corps de K et l'ensemble des sous-groupes de G.

Notons que, dans cette correspondance, plus le sous-corps est grand, plus le sous-groupe est petit et vice-versa. Par exemple, au groupe G lui-même correspond le corps $\mathbb{Q}$, tandis qu'au groupe $\{id\}$ correspond le corps K.

3.2 Le corps de définition d'un arbre

Reprenant les idées précédentes qui sont vraiment celles qu'il faut avoir en tête lorsque l'on fait de la théorie de Galois, on peut définir ce qu'est le *corps de définition* d'un arbre.

Soit un arbre plan bipartite. On considère le sous-groupe de $\mathrm{Gal}\left(\overline{\mathbb{Q}}\right)$ formé des éléments qui agissent sur cet arbre sans le modifier. Comme il est passablement évident que $\overline{\mathbb{Q}}$ est une extension galoisienne de $\mathbb{Q}$, d'après la correspondance précédente[14], à ce sous-groupe, il correspond un sous-corps de $\overline{\mathbb{Q}}$ qui est par définition le *corps de définition de l'arbre*[15]

On dispose alors d'un théorème qui permet de calculer ce corps simplement à partir d'un polynôme définissant l'arbre en question.

[14] Il n'est pas vrai ici que G est fini. Cependant il existe une variante de la correspondance de Galois, plus difficile à énoncer pour le cas infini qui s'applique à cette situation.

[15] En déroulant les définitions, on constate que le corps de définition de l'arbre est formé exactement des éléments de $\bar{Q}$ fixés par tous les éléments de $\mathrm{Gal}\left(()\,\bar{Q}\right)$ qui n'agissent pas sur l'arbre. L'intérêt de cette reformulation est qu'elle ne fait appel à aucune correspondance de Galois... et donc n'a pas besoin d'un théorème que l'on n'a ni prouvé ni énoncé pour fonctionner.

Théorème 4. *Soit P un polynôme à coefficients dans $\overline{\mathbb{Q}}$ correspondant à un certain arbre plan bipartite A. Soient K_A le corps de définition de A et K_P le plus petit corps contenant tous les coefficients de P.*

Alors on a $K_A \subset K_P$. De plus, en appliquant à P une transformation $P(z) \mapsto P(az+b)$, il est toujours possible d'obtenir un nouveau polynôme P tel que $K_A = K_P$.

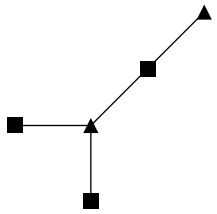
Il est laissé en exercice au lecteur le soin de trouver les corps de définition de tous les arbres que l'on a pu rencontrer jusqu'à maintenant (sauf peut-être celui de la fleur de Leila qui demande une quantité non négligeable de calculs).

3.3 Composition des polynômes et des arbres

Il est possible de décrire une construction qui, à partir d'un arbre associé à un polynôme P et d'un arbre associé à un polynôme Q, fournisse un nouvel arbre associé à peu de choses près au polynôme composé $Q \circ P$.

C'est en fait légèrement plus compliqué car à partir de deux arbres on peut former de nombreaux nouveaux arbres. Il faut se donner en outre pour la construction une *donnée de recollement*.

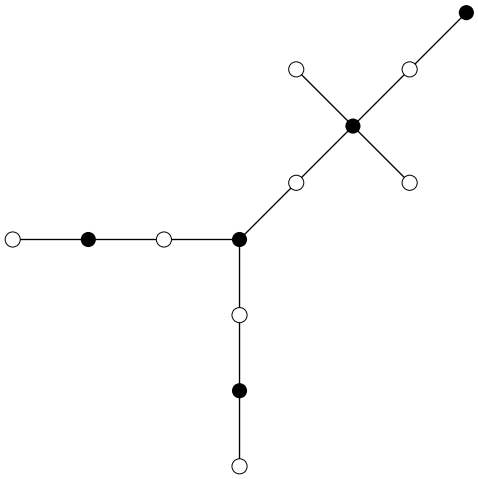
Expliquons cette construction sur un exemple. Supposons que l'on dispose de l'arbre suivant associé au polynôme P :



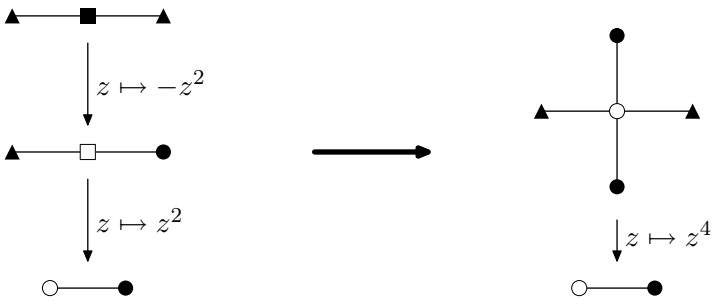
Les couleurs des sommets sont ici indiquées par des carrés et des triangles, plutôt que par des sommets vides et pleins. On considère également l'arbre suivant associé au polynôme Q :

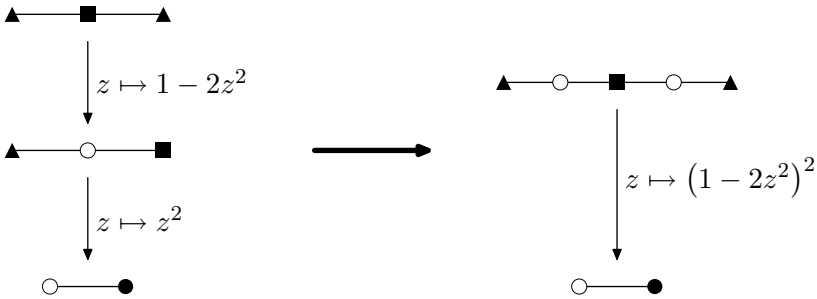
Cette fois les couleurs des sommets sont, comme d'habitude, vide et plein. Cependant deux sommets sont en plus marqués par un carré et un triangle. C'est le marquage de ces deux sommets qui correspond à la « donnée de recollement ». Nous disposons cet arbre sur le plan de sorte à avoir le carré en 0 et le triangle en 1 (cela nous détermine uniquement le polynôme Q associé).

La composition consiste à remplacer chaque arête du premier arbre par tout le second arbre, les carrés venant sur les carrés et les triangles sur les triangles. Notons que les sommets qui, dans le deuxième arbre, ne se trouvent pas entre le carré et le triangle, ne sont pas du tout perdus. Avec les deux arbres précédents, on obtient le résultat suivant :



On peut finalement donner d'autres exemples de composition (plus simples que le précédent). Nous laissons les illustrations parler d'elles-mêmes.





Annexe : notion de résultant

Définition

On considère deux polynômes P et Q à coefficients complexes de degré p et q respectivement. On cherche à déterminer un critère portant sur les coefficients pour que P et Q soient premiers entre eux.

Pour cela, on se rappelle que l'on dispose en premier lieu du théorème de Bézout qui stipule que P et Q sont premiers entre eux si et seulement s'il existe deux polynômes U et V tels que $\deg U < q$, $\deg V < p$ et $PU + QV = 1$.

Si l'on désigne par $\mathbb{C}_k[X]$ l'ensemble des polynômes à coefficients complexes dont le degré est inférieur ou égal à k, il est facile de voir, grâce au théorème de Bézout, que l'application :

$$\varphi : \left(\begin{array}{ccc} \mathbb{C}_{q-1}[X] \times \mathbb{C}_{p-1}[X] & \to & \mathbb{C}_{p+q-1}[X] \\ (U, V) & \mapsto & PU + QV \end{array} \right)$$

est surjective si et seulement si P et Q sont premiers entre eux. Pour ceux qui connaissent l'algèbre linéaire : le résultant de P et Q est, par définition, le déterminant de l'application φ. Ci-dessous, nous donnons une explication un peu plus détaillée.

Déjà, on remarque que l'application φ n'est autre qu'une fonction qui prend en entrée $p + q$ complexes (qui sont les coefficients des polynômes U et V), multiplie chacun de ces nombres par le bon coefficient de P ou de Q et additionne certains des résultats obtenus pour donner au final à nouveau $p + q$ complexes (qui seront les coefficients du polynôme $PU + QV$).

Dire que l'application φ est surjective signifie simplement que, quel que soit ce que l'on met à droite, on est capable de résoudre un gros système à $p + q$ équations et $p + q$ inconnus. Mais il y a une condition portant sur les coefficients « à gauche » qui précise quand cela est ou n'est pas le cas. Si l'on se rappelle la résolution de Cramer, on se rappelle que les solutions d'un système (2×2, mais pas forcément) sont données par un quotient de deux déterminants et qu'il y a donc toujours une unique solution si le déterminant au dénominateur est non nul.

De fait, cela fonctionne exactement de la même façon dans le cas d'un système $(p + q) \times (p + q)$: on calcule le déterminant des nombres qui apparaissent à gauche. S'il est nul, cela signifie que, pour certaines valeurs de droite, il n'y a pas de solution. Sinon, cela signifie qu'il y aura toujours une unique solution quel que soit ce que l'on met à droite.

Le point important est que la relative primalité de P et de Q est conditionnée par la nullité ou la non nullité d'un nombre qui s'obtient par de simples opérations arithmétiques (addition, soustraction, multiplication) et de façon totalement explicite à partir des coefficients de P et de Q. En particulier, si les coefficients de P et de Q dépendent de façon polynomiale d'un certain paramètre t, la condition de relative primalité s'exprime par l'annulation d'un certain polynôme en t.

Bibliographie commentée

L'article [1] a attiré l'attention des mathématiciens sur les dessins d'enfant. L'article [2] est un des premiers consacrés à ce sujet. Ce sont des références plutôt historiques, car difficilement compréhensibles par un non spécialiste.

Les deux premiers chapitres de [3] constituent une introduction patiente et presque élémentaire à la théorie des dessins d'enfant.

Le livre [4] constitue un catalogue des polynômes associés aux arbres plans avec des explications détaillées sur la façon dont on les calcule. Malheureusement, la seule façon de se le procurer est de demander une copie à l'un des auteurs.

Références

[1] A. Grothendieck, *Esquisse d'un programme* (1984) in *Geometric Galois Action* (par L. Schneps, P. Lochak), **1**, London Mathematical Society Lecture Notes Series, Cambridge University Press, 1997, **242**, pp 5–48

[2] G.B. Shabat, V. A. Voevodsky, *Drawing curves over number fields* in *The Grothedieck Festschrift* (par P. Cartier, L. Illusie, N.M. Kats, Yu. Manin, K.A. Ribet), Birkhäuser, 1990, **3**, pp 199-227

[3] S. K. Lando, A. K. Zvonkin, *Graphs on surfaces and their applications*, Springer-Verlag, 2004

[4] J. Bétréma, D. Péré, A. K. Zvonkin, *Plane trees and their Shabat polynomials. Catalog.* Rapport interne du Laboratoire Bordelais de Recherche en Informatique, 1992