Équations, des Babyloniens à Abel et Galois

Daniel PERRIN

Maths-Monde, IREM de Paris 7, 13 mars 2019

Équations et mathématiques

- Deux mots synonymes ? L'exemple des problèmes du millenium.

Équations et mathématiques

- Deux mots synonymes ? L'exemple des problèmes du millenium.
- L'hypothèse de Riemann : les solutions de l'équation $\zeta(s) = 0$. La conjecture de Birch et Swinnerton-Dyer : les solutions rationnelles de l'équation $y^2 = x^3 + px + q$. La conjecture de Hodge : un lien entre la topologie algébrique d'une variété algébrique complexe définie par des équations polynomiales et sa géométrie. Les équations de Navier-Stokes. Les équations de Yang-Mills. L'équation ... $P = NP$?

Équations et mathématiques

- Deux mots synonymes ? L'exemple des problèmes du millenium.
- L'hypothèse de Riemann : les solutions de l'équation $\zeta(s) = 0$. La conjecture de Birch et Swinnerton-Dyer : les solutions rationnelles de l'équation $y^2 = x^3 + px + q$. La conjecture de Hodge : un lien entre la topologie algébrique d'une variété algébrique complexe définie par des équations polynomiales et sa géométrie. Les équations de Navier-Stokes. Les équations de Yang-Mills. L'équation ... $P = NP$?
- Sans oublier le raton-laveur : le grand théorème de Fermat et l'équation $x^n + y^n = z^n$.

Équations : soyons modestes

- Dans cet exposé nous nous limiterons aux équations algébriques (i.e. polynomiales) et même à celles données par un polynôme en une seule variable.

Équations : soyons modestes

- Dans cet exposé nous nous limiterons aux équations algébriques (i.e. polynomiales) et même à celles données par un polynôme en une seule variable.
- C'est un problème très simple en apparence, mais qui a tout de même mené à l'introduction à la fois des nombres complexes et de la notion de groupe.

Première partie :

L'histoire ancienne

Les Babyloniens et le second degré

- Traduction du problème 1 de la tablette BM 13901 - 1 (vers 1800 av. J.-C.) par Thureau-Dangin (1936).

Les Babyloniens et le second degré

- Traduction du problème 1 de la tablette BM 13901 - 1 (vers 1800 av. J.-C.) par Thureau-Dangin (1936).
- *J'ai additionné la surface et le côté de mon carré : 45'.*

Les Babyloniens et le second degré

- Traduction du problème 1 de la tablette BM 13901 - 1 (vers 1800 av. J.-C.) par Thureau-Dangin (1936).
- *J'ai additionné la surface et le côté de mon carré : 45'.*
- Traduction : on a x (le côté) tel que $x^2 + x = 45'$ ($ax^2 + bx + c = 0$ avec $a = 1, b = 1, c = -3/4$).

Les Babyloniens et le second degré

- Traduction du problème 1 de la tablette BM 13901 - 1 (vers 1800 av. J.-C.) par Thureau-Dangin (1936).
- *J'ai additionné la surface et le côté de mon carré : 45'.*
- Traduction : on a x (le côté) tel que $x^2 + x = 45'$ ($ax^2 + bx + c = 0$ avec $a = 1, b = 1, c = -3/4$).
- Solution : Tu poseras 1, l'unité. Tu fractionneras en deux 1 : 30'. Tu croiseras 30' et 30' : 15'. Tu ajouteras 15' à 45' : 1. C'est le carré de 1. Tu soustrairas 30', que tu as croisé, de 1 : 30', le côté du carré.

Les Babyloniens et le second degré

- Traduction du problème 1 de la tablette BM 13901 - 1 (vers 1800 av. J.-C.) par Thureau-Dangin (1936).
- *J'ai additionné la surface et le côté de mon carré : 45'.*
- Traduction : on a x (le côté) tel que $x^2 + x = 45'$ ($ax^2 + bx + c = 0$ avec $a = 1, b = 1, c = -3/4$).
- Solution : Tu poseras 1, l'unité. Tu fractionneras en deux 1 : 30'. Tu croiseras 30' et 30' : 15'. Tu ajouteras 15' à 45' : 1. C'est le carré de 1. Tu soustrairas 30', que tu as croisé, de 1 : 30', le côté du carré.
- En clair : $(\frac{b}{2})^2 = \frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$; $(\frac{b}{2})^2 - c = \frac{1}{4} + \frac{3}{4} = 1 = 1^2$; $x = -b + \sqrt{(\frac{b}{2})^2 - c} = -\frac{1}{2} + 1 = \frac{1}{2}$.

Les Babyloniens et le second degré

- Traduction du problème 1 de la tablette BM 13901 - 1 (vers 1800 av. J.-C.) par Thureau-Dangin (1936).
- *J'ai additionné la surface et le côté de mon carré : 45'.*
- Traduction : on a x (le côté) tel que $x^2 + x = 45'$ ($ax^2 + bx + c = 0$ avec $a = 1, b = 1, c = -3/4$).
- Solution : Tu poseras 1, l'unité. Tu fractionneras en deux 1 : 30'. Tu croiseras 30' et 30' : 15'. Tu ajouteras 15' à 45' : 1. C'est le carré de 1. Tu soustrairas 30', que tu as croisé, de 1 : 30', le côté du carré.
- En clair : $(\frac{b}{2})^2 = \frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$; $(\frac{b}{2})^2 - c = \frac{1}{4} + \frac{3}{4} = 1 = 1^2$; $x = -b + \sqrt{(\frac{b}{2})^2 - c} = -\frac{1}{2} + 1 = \frac{1}{2}$.
- Voir une discussion dans l'article de Christine Proust : http ://images.math.cnrs.fr/Mathematiques-en-Mesopotamie.html

Les Grecs et la vision géométrique

- Un problème d'Euclide (livre II, prop. 11) : *Partager une droite donnée de manière que le rectangle compris sous la droite entière et l'un de ses segments soit égal au carré de l'autre segment.*

Les Grecs et la vision géométrique

- Un problème d'Euclide (livre II, prop. 11) : *Partager une droite donnée de manière que le rectangle compris sous la droite entière et l'un de ses segments soit égal au carré de l'autre segment*.
- Autrement dit, une longueur b étant donnée, trouver a telle que $b(b-a) = a^2$.

Les Grecs et la vision géométrique

- Un problème d'Euclide (livre II, prop. 11) : *Partager une droite donnée de manière que le rectangle compris sous la droite entière et l'un de ses segments soit égal au carré de l'autre segment*.
- Autrement dit, une longueur b étant donnée, trouver a telle que $b(b-a) = a^2$.
- Voici la construction* d'Euclide.

Les Grecs et la vision géométrique

- Un problème d'Euclide (livre II, prop. 11) : *Partager une droite donnée de manière que le rectangle compris sous la droite entière et l'un de ses segments soit égal au carré de l'autre segment*.
- Autrement dit, une longueur b étant donnée, trouver a telle que $b(b-a) = a^2$.
- Voici la construction* d'Euclide.
- Le rapport $\phi = \frac{b}{a}$ vérifie $\phi^2 - \phi - 1 = 0$. C'est le nombre d'or. Cette construction mène à celle d'un triangle d'angles $36^\circ, 72^\circ, 72^\circ$ puis à celle du pentagone régulier.

Bilan sur l'équation du second degré au début du XVI-ième siècle

- Sur l'équation $ax^2 + bx + c = 0$, deux résultats bien connus :

Bilan sur l'équation du second degré au début du XVI-ième siècle

- Sur l'équation $ax^2 + bx + c = 0$, deux résultats bien connus :
- La somme et le produit des racines : $x_1 + x_2 = -b/a$, $x_1 x_2 = c/a$.

Bilan sur l'équation du second degré au début du XVI-ième siècle

- Sur l'équation $ax^2 + bx + c = 0$, deux résultats bien connus :
- La somme et le produit des racines : $x_1 + x_2 = -b/a$, $x_1 x_2 = c/a$.
- La méthode pour enlever le terme en bx en rendant la somme des racines nulles, donc en posant $X = x + \frac{b}{2a}$. Cette méthode est connue aussi pour les équations de degré > 2.

Cardan et l'équation de degré 3

- On peut supposer l'équation de la forme $x^3 + px + q = 0$.

Cardan et l'équation de degré 3

- On peut supposer l'équation de la forme $x^3 + px + q = 0$.
- L'astuce (Scipion del Ferro 1515, Tartaglia 1535, publiée par Cardan, 1545) : $x = u + v$.

Cardan et l'équation de degré 3

- On peut supposer l'équation de la forme $x^3 + px + q = 0$.
- L'astuce (Scipion del Ferro 1515, Tartaglia 1535, publiée par Cardan, 1545) : $x = u + v$.
- On impose $uv = -p/3$. Alors u^3, v^3 sont les racines de l'équation du second degré $Y^2 + qY - \dfrac{p^3}{27} = 0$.

Cardan et l'équation de degré 3

- On peut supposer l'équation de la forme $x^3 + px + q = 0$.
- L'astuce (Scipion del Ferro 1515, Tartaglia 1535, publiée par Cardan, 1545) : $x = u + v$.
- On impose $uv = -p/3$. Alors u^3, v^3 sont les racines de l'équation du second degré $Y^2 + qY - \dfrac{p^3}{27} = 0$.
- $$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{4p^3 + 27q^2}{4 \times 27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{4p^3 + 27q^2}{4 \times 27}}}.$$

Cardan et l'équation de degré 3

- On peut supposer l'équation de la forme $x^3 + px + q = 0$.
- L'astuce (Scipion del Ferro 1515, Tartaglia 1535, publiée par Cardan, 1545) : $x = u + v$.
- On impose $uv = -p/3$. Alors u^3, v^3 sont les racines de l'équation du second degré $Y^2 + qY - \frac{p^3}{27} = 0$.
- $$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{4p^3 + 27q^2}{4 \times 27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{4p^3 + 27q^2}{4 \times 27}}}.$$
- L'exemple de Newton : $x^3 - 2x - 5 = 0$.

$$x = \sqrt[3]{\frac{5}{2} + \frac{\sqrt{643}}{6\sqrt{3}}} + \sqrt[3]{\frac{5}{2} - \frac{\sqrt{643}}{6\sqrt{3}}} \sim 2,09455148154.$$

Le cas irréductible et les nombres complexes : Bombelli

- C'est le cas où l'équation $x^3 + px + q = 0$ admet trois racines réelles, par exemple $x^3 - 7x + 6 = 0$, qui admet les racines $1, 2, -3$.

Le cas irréductible et les nombres complexes : Bombelli

- C'est le cas où l'équation $x^3 + px + q = 0$ admet trois racines réelles, par exemple $x^3 - 7x + 6 = 0$, qui admet les racines $1, 2, -3$.
- Dans ce cas, la méthode de Cardan conduit à l'équation $X^2 + qX - \frac{p^3}{27} = 0$ de discriminant $D = \frac{4p^3 + 27q^2}{27} < 0$ ici $D = -\frac{400}{27} < 0$.

Le cas irréductible et les nombres complexes : Bombelli

- C'est le cas où l'équation $x^3 + px + q = 0$ admet trois racines réelles, par exemple $x^3 - 7x + 6 = 0$, qui admet les racines $1, 2, -3$.
- Dans ce cas, la méthode de Cardan conduit à l'équation $X^2 + qX - \frac{p^3}{27} = 0$ de discriminant $D = \frac{4p^3 + 27q^2}{27} < 0$ ici $D = -\frac{400}{27} < 0$.
- En 1560 Bombelli a l'idée de passer outre en introduisant de nouveaux "signes" : *piu, meno, piu de meno, meno de meno*, c'est la naissance des imaginaires.

Bombelli (suite)

- On a alors ici $\sqrt{-\frac{400}{27}} = \frac{20i}{3\sqrt{3}}$, d'où $u^3 = -3 + \frac{10}{3\sqrt{3}}i$ et $v^3 = -3 - \frac{10}{3\sqrt{3}}i$.

Bombelli (suite)

- On a alors ici $\sqrt{-\frac{400}{27}} = \frac{20i}{3\sqrt{3}}$, d'où $u^3 = -3 + \frac{10}{3\sqrt{3}}i$ et $v^3 = -3 - \frac{10}{3\sqrt{3}}i$.
- On calcule une racine cubique de u^3, ici $u = 1 + \frac{2i\sqrt{3}}{3}$, puis v avec $uv = -p/3 = 7/3$, $v = 1 - \frac{2i\sqrt{3}}{3}$.

Bombelli (suite)

- On a alors ici $\sqrt{-\frac{400}{27}} = \frac{20i}{3\sqrt{3}}$, d'où $u^3 = -3 + \frac{10}{3\sqrt{3}}i$ et $v^3 = -3 - \frac{10}{3\sqrt{3}}i$.
- On calcule une racine cubique de u^3, ici $u = 1 + \frac{2i\sqrt{3}}{3}$, puis v avec $uv = -p/3 = 7/3$, $v = 1 - \frac{2i\sqrt{3}}{3}$.
- Les racines de l'équation sont : $x_1 = u + v$, $x_2 = j^2u + jv$, $x_3 = ju + j^2v$, ici $x_1 = (1 + \frac{2i\sqrt{3}}{3}) + (1 - \frac{2i\sqrt{3}}{3}) = 2$, $x_2 = 1$, $x_3 = -3$.

Bombelli (suite)

- On a alors ici $\sqrt{-\frac{400}{27}} = \frac{20i}{3\sqrt{3}}$, d'où $u^3 = -3 + \frac{10}{3\sqrt{3}}i$ et $v^3 = -3 - \frac{10}{3\sqrt{3}}i$.
- On calcule une racine cubique de u^3, ici $u = 1 + \frac{2i\sqrt{3}}{3}$, puis v avec $uv = -p/3 = 7/3$, $v = 1 - \frac{2i\sqrt{3}}{3}$.
- Les racines de l'équation sont : $x_1 = u + v$, $x_2 = j^2u + jv$, $x_3 = ju + j^2v$, ici $x_1 = (1 + \frac{2i\sqrt{3}}{3}) + (1 - \frac{2i\sqrt{3}}{3}) = 2$, $x_2 = 1$, $x_3 = -3$.
- Voir https ://www.math.u-psud.fr/ perrin/CAPES/ algebre /Cardan10.pdf

Bombelli (suite)

- On a alors ici $\sqrt{-\frac{400}{27}} = \frac{20i}{3\sqrt{3}}$, d'où $u^3 = -3 + \frac{10}{3\sqrt{3}}i$ et $v^3 = -3 - \frac{10}{3\sqrt{3}}i$.
- On calcule une racine cubique de u^3, ici $u = 1 + \frac{2i\sqrt{3}}{3}$, puis v avec $uv = -p/3 = 7/3$, $v = 1 - \frac{2i\sqrt{3}}{3}$.
- Les racines de l'équation sont : $x_1 = u + v$, $x_2 = j^2u + jv$, $x_3 = ju + j^2v$, ici $x_1 = (1 + \frac{2i\sqrt{3}}{3}) + (1 - \frac{2i\sqrt{3}}{3}) = 2$, $x_2 = 1$, $x_3 = -3$.
- Voir https ://www.math.u-psud.fr/ perrin/CAPES/ algebre /Cardan10.pdf
- Le degré 4 est traité par Ferrari (1540).

Coefficients et racines, Viète (1540-1603)

- On généralise le cas du second degré. On considère l'équation :

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = 0$$

Coefficients et racines, Viète (1540-1603)

- On généralise le cas du second degré. On considère l'équation :

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = 0$$

- Si $x_1, \ldots, x_n$ sont ses racines, on a les formules :

$$a_1 = -(x_1 + \cdots + x_n), \quad a_2 = x_1 x_2 + x_1 x_3 + \cdots + x_{n-1} x_n, \ldots$$

$$a_k = (-1)^k \sum_{i_1 < \ldots < i_k} x_{i_1} \cdots x_{i_k}, \quad \cdots, \quad a_n = (-1)^n x_1 \cdots x_n.$$

Coefficients et racines, Viète (1540-1603)

- On généralise le cas du second degré. On considère l'équation :

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = 0$$

- Si $x_1, \ldots, x_n$ sont ses racines, on a les formules :

$$a_1 = -(x_1 + \cdots + x_n), \quad a_2 = x_1 x_2 + x_1 x_3 + \cdots + x_{n-1} x_n, \ldots$$

$$a_k = (-1)^k \sum_{i_1 < \ldots < i_k} x_{i_1} \cdots x_{i_k}, \quad \cdots, \quad a_n = (-1)^n x_1 \cdots x_n.$$

- On voit que ces éléments sont invariants par permutation des racines (polynômes symétriques).

Coefficients et racines, Viète (1540-1603)

- On généralise le cas du second degré. On considère l'équation :

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n = 0$$

- Si $x_1, \ldots, x_n$ sont ses racines, on a les formules :

$$a_1 = -(x_1 + \cdots + x_n), \quad a_2 = x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n, \ldots$$

$$a_k = (-1)^k \sum_{i_1 < \ldots < i_k} x_{i_1} \cdots x_{i_k}, \quad \cdots, \quad a_n = (-1)^n x_1 \cdots x_n.$$

- On voit que ces éléments sont invariants par permutation des racines (polynômes symétriques).
- Le théorème fondamental (Newton ?) : *Tout polynôme symétrique en les x_i est un polynôme en les fonctions symétriques élémentaires, donc en les a_i.*

Un résultat important : D'Alembert-Gauss

- Tout polynôme de degré n à coefficients réels admet n racines (complexes), comptées avec multiplicités.

Un résultat important : D'Alembert-Gauss

- Tout polynôme de degré n à coefficients réels admet n racines (complexes), comptées avec multiplicités.
- Il est énoncé par Albert Girard en 1629 : *Toutes les équations d'algèbre reçoivent autant de solutions que la dénomination de la plus haute quantité le démontre.*

Un résultat important : D'Alembert-Gauss

- Tout polynôme de degré n à coefficients réels admet n racines (complexes), comptées avec multiplicités.
- Il est énoncé par Albert Girard en 1629 : *Toutes les équations d'algèbre reçoivent autant de solutions que la dénomination de la plus haute quantité le démontre.*
- Voici ce qu'en dit Descartes : *En chaque équation autant que la quantité inconnue a de dimensions, autant peut-il y avoir de diverses racines : mais souvent il arrive que ces racines soient fausses ou moindres que rien. Comme si on suppose que x désigne aussi le défaut d'une quantité qui soit 5, on a $x+5=0$, qui multipliée par $x^3-9x^2+26x-24=0$ fait $x^4-4x^3-19x^2+106x-120=0$ pour une équation en laquelle il y a quatre racines, à savoir trois vraies qui sont $2,3,4$ et une fausse qui est 5.*

Un résultat important : D'Alembert-Gauss (suite)

- Descartes ajoute, plus loin : *Ces racines sont quelquefois seulement imaginaires c'est-à-dire que l'on peut toujours en imaginer autant que j'ai dit en chaque équation, mais qu'il n'y a quelquefois aucune quantité qui corresponde à celle qu'on imagine...*

Un résultat important : D'Alembert-Gauss (suite)

- Descartes ajoute, plus loin : *Ces racines sont quelquefois seulement imaginaires c'est-à-dire que l'on peut toujours en imaginer autant que j'ai dit en chaque équation, mais qu'il n'y a quelquefois aucune quantité qui corresponde à celle qu'on imagine...*
- D'Alembert en propose une preuve en 1746 (pas tout à fait correcte), puis Euler, Lagrange et enfin Gauss qui en donne quatre démonstrations (1799, 1815, 1816, 1849).

Deuxième partie :

Lagrange et Van der Monde

Lagrange et Van der Monde

- En 1770-1771 paraissent deux articles :
  • Joseph-Louis Lagrange*, *Réflexions sur la résolution algébrique des équations.* Mémoires de l'Académie royale des sciences et Belles-Lettres de Berlin, 1770-1771,
  • Alexandre -Théophile Vandermonde, *Mémoire sur la résolution des équations*, Mémoires de l'Académie des sciences de Paris, 1771.

Lagrange et Van der Monde

- En 1770-1771 paraissent deux articles :
  • Joseph-Louis Lagrange*, *Réflexions sur la résolution algébrique des équations.* Mémoires de l'Académie royale des sciences et Belles-Lettres de Berlin, 1770-1771,
  • Alexandre -Théophile Vandermonde, *Mémoire sur la résolution des équations*, Mémoires de l'Académie des sciences de Paris, 1771.
- Ils portent sur la résolution des équations du troisième et du quatrième degré, mais, par rapport à leurs devanciers, leur but est de donner une explication à des calculs jusque là abscons.

Les objectifs de Lagrange

- *Je me propose dans ce Mémoire d'examiner les différentes méthodes que l'on a trouvées jusqu'à présent pour la résolution algébrique des équations, de les réduire à des principes généraux, et de faire voir a priori pourquoi ces méthodes réussissent pour le troisième et le quatrième degré, et sont en défaut pour les degrés ultérieurs.*

Les objectifs de Lagrange

- *Je me propose dans ce Mémoire d'examiner les différentes méthodes que l'on a trouvées jusqu'à présent pour la résolution algébrique des équations, de les réduire à des principes généraux, et de faire voir a priori pourquoi ces méthodes réussissent pour le troisième et le quatrième degré, et sont en défaut pour les degrés ultérieurs.*
- Et il ajoute :
  ... je donnerai à cette occasion les vrais principes et, pour ainsi dire, la métaphysique de la résolution des équations du troisième et du quatrième degré.

Lagrange et l'équation du troisième degré

- On considère une équation $x^3 + px + q = 0$ et on cherche à calculer ses racines x_1, x_2, x_3 par radicaux. On reprend la méthode de Cardan (avec la version Bombelli).

Lagrange et l'équation du troisième degré

- On considère une équation $x^3 + px + q = 0$ et on cherche à calculer ses racines x_1, x_2, x_3 par radicaux. On reprend la méthode de Cardan (avec la version Bombelli).
- On pose $x = u + v$ et on a vu comment calculer u^3 et v^3.

Lagrange et l'équation du troisième degré

- On considère une équation $x^3 + px + q = 0$ et on cherche à calculer ses racines x_1, x_2, x_3 par radicaux. On reprend la méthode de Cardan (avec la version Bombelli).
- On pose $x = u + v$ et on a vu comment calculer u^3 et v^3.
- Ces éléments jouent un rôle crucial en scindant la résolution de l'équation en deux étapes : l'équation du second degré $Y^2 + qY - \frac{p^3}{27} = 0$ donne u^3, v^3 dont on extrait ensuite les racines cubiques.

Lagrange et l'équation du troisième degré

- On considère une équation $x^3 + px + q = 0$ et on cherche à calculer ses racines x_1, x_2, x_3 par radicaux. On reprend la méthode de Cardan (avec la version Bombelli).
- On pose $x = u + v$ et on a vu comment calculer u^3 et v^3.
- Ces éléments jouent un rôle crucial en scindant la résolution de l'équation en deux étapes : l'équation du second degré $Y^2 + qY - \frac{p^3}{27} = 0$ donne u^3, v^3 dont on extrait ensuite les racines cubiques.
- Ces éléments u^3, v^3 ne sont pas des fonctions rationnelles des coefficients (donc pas des fonctions symétriques des racines) mais $u^3 + v^3 = -q$ et $u^3 v^3 = -p^3/27$ en sont.

Lagrange et l'équation du troisième degré

- On considère une équation $x^3 + px + q = 0$ et on cherche à calculer ses racines x_1, x_2, x_3 par radicaux. On reprend la méthode de Cardan (avec la version Bombelli).
- On pose $x = u + v$ et on a vu comment calculer u^3 et v^3.
- Ces éléments jouent un rôle crucial en scindant la résolution de l'équation en deux étapes : l'équation du second degré $Y^2 + qY - \frac{p^3}{27} = 0$ donne u^3, v^3 dont on extrait ensuite les racines cubiques.
- Ces éléments u^3, v^3 ne sont pas des fonctions rationnelles des coefficients (donc pas des fonctions symétriques des racines) mais $u^3 + v^3 = -q$ et $u^3 v^3 = -p^3/27$ en sont.
- Lagrange va examiner ces éléments avec ce point de vue.

Lagrange et l'équation du troisième degré (suite)

- On a obtenu $x_1 = u + v$, $x_2 = j^2u + jv$, $x_3 = ju + j^2v$.

Lagrange et l'équation du troisième degré (suite)

- On a obtenu $x_1 = u + v$, $x_2 = j^2u + jv$, $x_3 = ju + j^2v$.
- On en tire facilement $3u = x_1 + jx_2 + j^2x_3$ et $3v = x_1 + j^2x_2 + jx_3$.

Lagrange et l'équation du troisième degré (suite)

- On a obtenu $x_1 = u + v$, $x_2 = j^2u + jv$, $x_3 = ju + j^2v$.
- On en tire facilement $3u = x_1 + jx_2 + j^2x_3$ et $3v = x_1 + j^2x_2 + jx_3$.
- Lagrange constate que ces éléments (qu'on appelle résolvantes de Lagrange) ne sont pas symétriques c'est-à-dire invariants par permutation, mais ...

Lagrange et l'équation du troisième degré (suite)

- On a obtenu $x_1 = u + v$, $x_2 = j^2u + jv$, $x_3 = ju + j^2v$.
- On en tire facilement $3u = x_1 + jx_2 + j^2x_3$ et $3v = x_1 + j^2x_2 + jx_3$.
- Lagrange constate que ces éléments (qu'on appelle résolvantes de Lagrange) ne sont pas symétriques c'est-à-dire invariants par permutation, mais ...
- si on pose $\sigma = (123)$, on a $\sigma(u) = j^2u$, $\sigma(v) = jv$, et avec $\tau = (23)$, on a $\tau(u) = v$ et $\tau(v) = u$.

Lagrange et l'équation du troisième degré (suite)

- On a obtenu $x_1 = u + v$, $x_2 = j^2u + jv$, $x_3 = ju + j^2v$.
- On en tire facilement $3u = x_1 + jx_2 + j^2x_3$ et $3v = x_1 + j^2x_2 + jx_3$.
- Lagrange constate que ces éléments (qu'on appelle résolvantes de Lagrange) ne sont pas symétriques c'est-à-dire invariants par permutation, mais ...
- si on pose $\sigma = (123)$, on a $\sigma(u) = j^2u$, $\sigma(v) = jv$, et avec $\tau = (23)$, on a $\tau(u) = v$ et $\tau(v) = u$.
- On en déduit que u^3 et v^3 sont invariants par σ et échangés par τ. Ils sont donc "partiellement symétriques".

La "métaphysique"

- Pour résoudre par radicaux une équation de degré n, il s'agit de trouver des fonctions y des racines qui, par permutation, prennent r valeurs $y_1, \dots y_r$ avec $1 < r < n$, car elles seront racines d'une équation de degré r, $(Y - y_1) \cdots (Y - y_r) = 0$ dont les coefficients seront les fonctions symétriques en ces r valeurs.

La "métaphysique"

- Pour résoudre par radicaux une équation de degré n, il s'agit de trouver des fonctions y des racines qui, par permutation, prennent r valeurs $y_1, \dots y_r$ avec $1 < r < n$, car elles seront racines d'une équation de degré r, $(Y - y_1) \cdots (Y - y_r) = 0$ dont les coefficients seront les fonctions symétriques en ces r valeurs.
- Ici, $u^3 = (x_1 + jx_2 + j^2x_3)^3$ prend deux valeurs u^3 et v^3. Pour $n = 4$, voir Bonus, $u = x_1x_2 + x_3x_4$ prend trois valeurs (donc est solution d'une équation de degré 3).

La "métaphysique"

- Pour résoudre par radicaux une équation de degré n, il s'agit de trouver des fonctions y des racines qui, par permutation, prennent r valeurs $y_1, \dots y_r$ avec $1 < r < n$, car elles seront racines d'une équation de degré r, $(Y - y_1) \cdots (Y - y_r) = 0$ dont les coefficients seront les fonctions symétriques en ces r valeurs.
- Ici, $u^3 = (x_1 + jx_2 + j^2x_3)^3$ prend deux valeurs u^3 et v^3. Pour $n = 4$, voir Bonus, $u = x_1x_2 + x_3x_4$ prend trois valeurs (donc est solution d'une équation de degré 3).
- Lagrange : *Voilà, si je ne me trompe, les vrais principes de la résolution des équations et l'analyse la plus propre à y conduire ; tout se réduit, comme on le voit, à une espèce de calcul des combinaisons, par lequel on trouve a priori les résultats auxquels on doit s'attendre.*

Lagrange et le degré 5

- Lagrange essaie d'appliquer cette méthode aux équations de degré 5 en introduisant la résolvante $r := x_1 + \zeta x_2 + \zeta^2 x_3 + \zeta^3 x_4 + \zeta^4 x_5$ (où ζ est une racine cinquième primitive de l'unité).

Lagrange et le degré 5

- Lagrange essaie d'appliquer cette méthode aux équations de degré 5 en introduisant la résolvante $r := x_1 + \zeta x_2 + \zeta^2 x_3 + \zeta^3 x_4 + \zeta^4 x_5$ (où ζ est une racine cinquième primitive de l'unité).
- Par la permutation circulaire $\sigma = (12345)$ on a $\sigma(r) = \zeta^{-1} r$ donc r^5 est invariant par σ. Si on sait le calculer, on trouve les x_i en résolvant un système de type Vandermonde.

Lagrange et le degré 5

- Lagrange essaie d'appliquer cette méthode aux équations de degré 5 en introduisant la résolvante $r := x_1 + \zeta x_2 + \zeta^2 x_3 + \zeta^3 x_4 + \zeta^4 x_5$ (où ζ est une racine cinquième primitive de l'unité).
- Par la permutation circulaire $\sigma = (12345)$ on a $\sigma(r) = \zeta^{-1} r$ donc r^5 est invariant par σ. Si on sait le calculer, on trouve les x_i en résolvant un système de type Vandermonde.
- Le problème est donc de trouver r^5 et ses comparses comme on a trouvé u^3, v^3 ci-dessus. Malheureusement, l'équation que vérifie r^5 (la résolvante) est de degré 24 en général.

Troisième partie : Abel

Niels Abel (1802-1829)

- Après les travaux de Lagrange et Vandermonde, l'impossibilité de la résolution par radicaux des équations de degré ≥ 5 est dans l'air.

Niels Abel (1802-1829)

- Après les travaux de Lagrange et Vandermonde, l'impossibilité de la résolution par radicaux des équations de degré ≥ 5 est dans l'air.
- Voilà ce que dit Lagrange : *Il résulte de ces réflexions qu'il est très douteux que les méthodes dont nous venons de parler puissent donner la résolution complète des équations du cinquième degré et à plus forte raison celle des degrés supérieurs.*

Niels Abel (1802-1829)

- Après les travaux de Lagrange et Vandermonde, l'impossibilité de la résolution par radicaux des équations de degré ≥ 5 est dans l'air.
- Voilà ce que dit Lagrange : *Il résulte de ces réflexions qu'il est très douteux que les méthodes dont nous venons de parler puissent donner la résolution complète des équations du cinquième degré et à plus forte raison celle des degrés supérieurs.*
- Après une tentative de Ruffini en 1799 c'est au mathématicien norvégien Niels Abel* que revient le mérite de montrer en 1824 que l'équation générale de degré 5 n'est pas résoluble par radicaux.

Abel (suite)

- Dit en termes modernes, voici précisément ce que montre Abel :

Abel (suite)

- Dit en termes modernes, voici précisément ce que montre Abel :
- *Soit K un corps contenant suffisamment de racines de l'unité. On considère le polynôme*

$$P(X) = (X - X_1)(X - X_2) \cdots (X - X_5)$$

dont les racines sont les indéterminées $X_1, \ldots, X_5$ et les coefficients les polynômes symétriques élémentaires $\sigma_1, \ldots, \sigma_5$. Alors, l'équation $P(x) = 0$ n'est pas résoluble par radicaux.

Équation générale ou générique ?

- Voici exactement ce que dit Abel :

Équation générale ou générique ?

- Voici exactement ce que dit Abel :
- *... comme il s'agit de la résolution de l'équation générale du cinquième degré, il est clair qu'on peut considérer* x_1, x_2, x_3, x_4, x_5 *comme des variables indépendantes*

Équation générale ou générique ?

- Voici exactement ce que dit Abel :
- *... comme il s'agit de la résolution de l'équation générale du cinquième degré, il est clair qu'on peut considérer* x_1, x_2, x_3, x_4, x_5 *comme des variables indépendantes*
- et il ajoute :
  Par conséquent on peut échanger les quantités x_i *entre elles ...*

Équation générale ou générique ?

- Voici exactement ce que dit Abel :
- *... comme il s'agit de la résolution de l'équation générale du cinquième degré, il est clair qu'on peut considérer* x_1, x_2, x_3, x_4, x_5 *comme des variables indépendantes*
- et il ajoute :
  Par conséquent on peut échanger les quantités x_i *entre elles ...*
- Traduction moderne : le groupe (de Galois) de l'équation est le groupe symétrique $\mathfrak{S}_5$ tout entier.

Une idée de la preuve d'Abel

- Pour des détails voir ma page web.

Une idée de la preuve d'Abel

- Pour des détails voir ma page web.
- On suppose que l'équation est résoluble, donc que ses racines se calculent par adjonction successives de radicaux.

Une idée de la preuve d'Abel

- Pour des détails voir ma page web.
- On suppose que l'équation est résoluble, donc que ses racines se calculent par adjonction successives de radicaux.
- En termes modernes : le corps $L = K(X_1, \ldots, X_5)$ est contenu dans un corps M qui s'obtient comme sommet d'une "tour" :

$$K = K_0 \subset K_1 \subset \cdots \subset K_r = M$$

chaque K_{i+1} étant obtenu à partir de K_i en lui adjoignant la racine p_i-ième α_i d'un élément $a_i \in K_i$ et on peut supposer p_i premier.

Une idée de la preuve d'Abel

- Pour des détails voir ma page web.
- On suppose que l'équation est résoluble, donc que ses racines se calculent par adjonction successives de radicaux.
- En termes modernes : le corps $L = K(X_1, \ldots, X_5)$ est contenu dans un corps M qui s'obtient comme sommet d'une "tour" :

$$K = K_0 \subset K_1 \subset \cdots \subset K_r = M$$

chaque K_{i+1} étant obtenu à partir de K_i en lui adjoignant la racine p_i-ième α_i d'un élément $a_i \in K_i$ et on peut supposer p_i premier.

- Grâce à la présence des racines de l'unité, Abel montre* que l'on peut supposer que M est égal à L (donc que les α_i sont dans L). Voir mes notes pour des détails.

La preuve d'Abel (suite)

- On considère la première extension $K \subset K_1 = K(\alpha)$ avec $\alpha^p = a \in K$.

La preuve d'Abel (suite)

- On considère la première extension $K \subset K_1 = K(\alpha)$ avec $\alpha^p = a \in K$.
- Comme α est dans L, c'est une fonction rationnelle des X_i.

La preuve d'Abel (suite)

- On considère la première extension $K \subset K_1 = K(\alpha)$ avec $\alpha^p = a \in K$.
- Comme α est dans L, c'est une fonction rationnelle des X_i.
- Comme α^p est dans K, c'est une fonction symétrique des X_i.

La preuve d'Abel (suite)

- On considère la première extension $K \subset K_1 = K(\alpha)$ avec $\alpha^p = a \in K$.
- Comme α est dans L, c'est une fonction rationnelle des X_i.
- Comme α^p est dans K, c'est une fonction symétrique des X_i.
- Quand on permute les X_i, α^p est invariant, donc α prend p valeurs qui sont les $\zeta\alpha$ où ζ est une racine p-ième de l'unité.

La preuve d'Abel (suite)

- On considère la première extension $K \subset K_1 = K(\alpha)$ avec $\alpha^p = a \in K$.
- Comme α est dans L, c'est une fonction rationnelle des X_i.
- Comme α^p est dans K, c'est une fonction symétrique des X_i.
- Quand on permute les X_i, α^p est invariant, donc α prend p valeurs qui sont les $\zeta\alpha$ où ζ est une racine p-ième de l'unité.
- Cela signifie que l'orbite de α sous $\mathfrak{S}_5$ (c'est-à-dire l'ensemble de ses transformés par les permutations) est de cardinal p, ou encore (mais c'est un anachronisme), que le sous-groupe des permutations de $\mathfrak{S}_5$ qui fixent α est d'indice p.

La preuve d'Abel (suite)

- On montre alors les lemmes suivants, que l'on peut voir en termes d'opérations ou de sous-groupes :

La preuve d'Abel (suite)

- On montre alors les lemmes suivants, que l'on peut voir en termes d'opérations ou de sous-groupes :
- Si l'on a une orbite de $\mathfrak{S}_5$ de cardinal p premier, p divise $5! = 120$, donc $p = 2, 3, 5$ ou : un sous-groupe de $\mathfrak{S}_5$ d'indice premier p est d'indice $2, 3$ ou 5 (Lagrange).

La preuve d'Abel (suite)

- On montre alors les lemmes suivants, que l'on peut voir en termes d'opérations ou de sous-groupes :
- Si l'on a une orbite de $\mathfrak{S}_5$ de cardinal p premier, p divise $5! = 120$, donc $p = 2, 3, 5$ ou : un sous-groupe de $\mathfrak{S}_5$ d'indice premier p est d'indice $2, 3$ ou 5 (Lagrange).
- Une orbite de $\mathfrak{S}_5$ de cardinal < 5 est de cardinal 1 ou 2 ou : les seuls sous-groupes de $\mathfrak{S}_5$ d'indices < 5 sont $\mathfrak{S}_5$ et $\mathfrak{A}_5$ (Cauchy, 1815, voir en Bonus la version originale).

La preuve d'Abel (suite)

- On montre alors les lemmes suivants, que l'on peut voir en termes d'opérations ou de sous-groupes :
- Si l'on a une orbite de $\mathfrak{S}_5$ de cardinal p premier, p divise $5! = 120$, donc $p = 2, 3, 5$ ou : un sous-groupe de $\mathfrak{S}_5$ d'indice premier p est d'indice $2, 3$ ou 5 (Lagrange).
- Une orbite de $\mathfrak{S}_5$ de cardinal < 5 est de cardinal 1 ou 2 ou : les seuls sous-groupes de $\mathfrak{S}_5$ d'indices < 5 sont $\mathfrak{S}_5$ et $\mathfrak{A}_5$ (Cauchy, 1815, voir en Bonus la version originale).
- Les seuls sous-groupes de $\mathfrak{S}_5$ (ou de $\mathfrak{A}_5$) d'indice 5 sont les fixateurs des points (Abel).

La preuve d'Abel (suite et fin)

- Si $p = 5$, le fixateur de $K(\alpha)$ est aussi le fixateur d'un X_i et Abel en déduit qu'on a $K(\alpha) = K(X_i)$.

La preuve d'Abel (suite et fin)

- Si $p = 5$, le fixateur de $K(\alpha)$ est aussi le fixateur d'un X_i et Abel en déduit qu'on a $K(\alpha) = K(X_i)$.
- On a donc $X_i = b_0 + b_1\alpha + \cdots + b_4\alpha^4$.

La preuve d'Abel (suite et fin)

- Si $p = 5$, le fixateur de $K(\alpha)$ est aussi le fixateur d'un X_i et Abel en déduit qu'on a $K(\alpha) = K(X_i)$.
- On a donc $X_i = b_0 + b_1\alpha + \cdots + b_4\alpha^4$.
- Si une permutation change X_i en X_j, autre racine de P, on a vu qu'elle transforme α en $\zeta\alpha$ où ζ est une racine 5-ième de l'unité et on a donc $X_j = b_0 + b_1\zeta\alpha + \cdots + b_4\zeta^4\alpha^4$.

La preuve d'Abel (suite et fin)

- Si $p = 5$, le fixateur de $K(\alpha)$ est aussi le fixateur d'un X_i et Abel en déduit qu'on a $K(\alpha) = K(X_i)$.
- On a donc $X_i = b_0 + b_1\alpha + \cdots + b_4\alpha^4$.
- Si une permutation change X_i en X_j, autre racine de P, on a vu qu'elle transforme α en $\zeta\alpha$ où ζ est une racine 5-ième de l'unité et on a donc $X_j = b_0 + b_1\zeta\alpha + \cdots + b_4\zeta^4\alpha^4$.
- On a donc $K(X_1, \ldots, X_5) = K(\alpha)$, mais c'est absurde car les polynômes en α ne prennent que 5 valeurs quand on permute les X_i alors que $X_1 + \zeta X_2 + \cdots + \zeta^4 X_5$ (avec $\zeta^5 = 1$) prend 120 valeurs (car les X_i sont indépendants).

La preuve d'Abel (suite et fin)

- Si $p = 5$, le fixateur de $K(\alpha)$ est aussi le fixateur d'un X_i et Abel en déduit qu'on a $K(\alpha) = K(X_i)$.
- On a donc $X_i = b_0 + b_1\alpha + \cdots + b_4\alpha^4$.
- Si une permutation change X_i en X_j, autre racine de P, on a vu qu'elle transforme α en $\zeta\alpha$ où ζ est une racine 5-ième de l'unité et on a donc $X_j = b_0 + b_1\zeta\alpha + \cdots + b_4\zeta^4\alpha^4$.
- On a donc $K(X_1, \ldots, X_5) = K(\alpha)$, mais c'est absurde car les polynômes en α ne prennent que 5 valeurs quand on permute les X_i alors que $X_1 + \zeta X_2 + \cdots + \zeta^4 X_5$ (avec $\zeta^5 = 1$) prend 120 valeurs (car les X_i sont indépendants).
- Si $p = 2$ la preuve est analogue, mais en deux étapes.

Quatrième partie : Galois

Évariste Galois (1811-1832)

Commençons par une citation, emblématique de la modernité de Galois* :

Depuis Euler les calculs sont devenus de plus en plus nécessaires et aussi de plus en plus difficiles à mesure qu'ils s'appliquaient à des objets de science plus avancés. Dès le commencement de ce siècle, l'algorithme avait atteint un degré de complication tel que tout progrès était devenu impossible par ce moyen, sans l'élégance que les géomètres modernes ont dû imprimer à leurs recherches et au moyen de laquelle l'esprit saisit promptement et d'un seul coup un grand nombre d'opérations.

Évariste Galois, citation (suite)

Or je crois que les simplifications produites par l'élégance des calculs ... ont leurs limites ; je crois que le moment arrivera où les transformations algébriques prévues par les spéculations des analystes ne trouveront ni le temps ni la place de se produire ; à tel point qu'il faudra se contenter de les avoir prévues. Je ne veux pas dire qu'il n'y a plus rien de nouveau pour l'analyse sans ce secours : mais je crois qu'un jour sans cela tout serait épuisé. Sauter à pieds joints sur les calculs ; grouper les opérations, les classer suivant leurs difficultés et non suivant leurs formes ; telle est, suivant moi, la mission des géomètres futurs ; telle est la voie où je suis entré dans cet ouvrage.

Évariste Galois : les outils

- Par rapport à Abel, Galois introduit deux outils essentiels.

Évariste Galois : les outils

- Par rapport à Abel, Galois introduit deux outils essentiels.
- La notion de groupe (de Galois) de l'équation, qui permet de traiter toutes les extensions et pas seulement les génériques.

Évariste Galois : les outils

- Par rapport à Abel, Galois introduit deux outils essentiels.
- La notion de groupe (de Galois) de l'équation, qui permet de traiter toutes les extensions et pas seulement les génériques.
- La notion de sous-groupe distingué, qui rend très facile le résultat d'Abel et permet d'aborder le cas général.

Le groupe de Galois

- Quand on regarde une équation générique, toutes les permutations sont pertinentes. Ce n'est plus le cas, en général, pour une équation quelconque. Regardons deux exemples.

Le groupe de Galois

- Quand on regarde une équation générique, toutes les permutations sont pertinentes. Ce n'est plus le cas, en général, pour une équation quelconque. Regardons deux exemples.
- L'équation $x^4 - x - 1 = 0$ a quatre racines x_1, x_2, x_3, x_4. Ces racines vérifient les relations correspondant aux fonctions symétriques élémentaires :
  $x_1 + x_2 + x_3 + x_4 = x_1x_2 + \cdots + x_3x_4 = 0$,
  $x_1x_2x_3 + \cdots + x_2x_3x_4 = 1$, $x_1x_2x_3x_4 = -1$ et pas d'autres.
  Toutes les permutations sont pertinentes, le groupe de Galois de l'équation est $\mathfrak{S}_4$.

Le groupe de Galois (suite)

- L'équation $x^4 - 2 = 0$. Cette équation a aussi quatre racines x_1, x_2, x_3, x_4 qui vérifient les relations analogues :
  $x_1 + x_2 + x_3 + x_4 = x_1x_2 + \cdots + x_3x_4 =$
  $x_1x_2x_3 + \cdots + x_2x_3x_4 = 0$, $x_1x_2x_3x_4 = -2$.

Le groupe de Galois (suite)

- L'équation $x^4 - 2 = 0$. Cette équation a aussi quatre racines x_1, x_2, x_3, x_4 qui vérifient les relations analogues :
  $x_1 + x_2 + x_3 + x_4 = x_1x_2 + \cdots + x_3x_4 =$
  $x_1x_2x_3 + \cdots + x_2x_3x_4 = 0$, $x_1x_2x_3x_4 = -2$.
- Mais ici, si l'on pose $x_1 = \sqrt[4]{2}$, $x_2 = i\sqrt[4]{2}$, $x_3 = -\sqrt[4]{2}$ et $x_4 = -i\sqrt[4]{2}$, on a les relations supplémentaires $x_1 + x_3 = x_2 + x_4 = 0$ et les permutations de $\{1, 2, 3, 4\}$ qui ne respectent pas ces relations (par exemple la transposition (12)) ne sont pas pertinentes.

Le groupe de Galois (suite)

- L'équation $x^4 - 2 = 0$. Cette équation a aussi quatre racines x_1, x_2, x_3, x_4 qui vérifient les relations analogues :
  $x_1 + x_2 + x_3 + x_4 = x_1x_2 + \cdots + x_3x_4 =$
  $x_1x_2x_3 + \cdots + x_2x_3x_4 = 0$, $x_1x_2x_3x_4 = -2$.
- Mais ici, si l'on pose $x_1 = \sqrt[4]{2}$, $x_2 = i\sqrt[4]{2}$, $x_3 = -\sqrt[4]{2}$ et $x_4 = -i\sqrt[4]{2}$, on a les relations supplémentaires $x_1 + x_3 = x_2 + x_4 = 0$ et les permutations de $\{1, 2, 3, 4\}$ qui ne respectent pas ces relations (par exemple la transposition (12)) ne sont pas pertinentes.
- Ce que dit Galois* : *... que toute fonction des racines, déterminable rationnellement, soit invariable par les substitutions*. Ici $x_1 + x_3$ (qui est nulle, donc rationnelle) n'est pas invariante par (12).

Le groupe de Galois (suite)

- La manière moderne de dire cela est de regarder les automorphismes de corps. On note K le corps de base et L le corps de décomposition du polynôme P, engendré par ses racines $x_1, \ldots, x_n$.

Le groupe de Galois (suite)

- La manière moderne de dire cela est de regarder les automorphismes de corps. On note K le corps de base et L le corps de décomposition du polynôme P, engendré par ses racines $x_1, \ldots, x_n$.
- Alors, le groupe de Galois est le groupe des automorphismes de L qui laissent fixe K. Dans l'exemple précédent, la permutation $\sigma = (12)$ ne définit pas un automorphisme de L car on a $x_1 + x_3 = 0$ mais $x_{\sigma(1)} + x_{\sigma(3)} = x_2 + x_3 \neq 0$.

Le groupe de Galois (suite)

- La manière moderne de dire cela est de regarder les automorphismes de corps. On note K le corps de base et L le corps de décomposition du polynôme P, engendré par ses racines $x_1, \ldots, x_n$.
- Alors, le groupe de Galois est le groupe des automorphismes de L qui laissent fixe K. Dans l'exemple précédent, la permutation $\sigma = (12)$ ne définit pas un automorphisme de L car on a $x_1 + x_3 = 0$ mais $x_{\sigma(1)} + x_{\sigma(3)} = x_2 + x_3 \neq 0$.
- Le groupe de Galois de l'équation $x^4 - 2 = 0$ est le groupe formé de l'identité et des permutations (1234), $(13)(24)$, (1432), $(12)(34)$, $(14)(23)$, (13) et (24). Il est isomorphe au groupe diédral $\mathbf{D}_4$.

Le groupe de Galois (suite)

- Cela permet de mieux comprendre la notion de "valeurs prises par une fonction" utilisée par Abel et Galois. En termes modernes, si $v = f(x_1, \ldots, x_n)$ est une fonction des racines, ses "valeurs" sont les conjugués $\sigma(v) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ où σ est dans le groupe de Galois.

Le groupe de Galois (suite)

- Cela permet de mieux comprendre la notion de "valeurs prises par une fonction" utilisée par Abel et Galois. En termes modernes, si $v = f(x_1, \ldots, x_n)$ est une fonction des racines, ses "valeurs" sont les conjugués $\sigma(v) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ où σ est dans le groupe de Galois.
- L'idée principale de la théorie de Galois (?) est alors d'établir une correspondance entre les corps intermédiaires entre K et L et les sous-groupes du groupe de Galois : si on a $K \subset M \subset L$, le sous-groupe associé à M est l'ensemble des automorphismes qui fixent M.

Le groupe de Galois (suite)

- Cela permet de mieux comprendre la notion de "valeurs prises par une fonction" utilisée par Abel et Galois. En termes modernes, si $v = f(x_1, \ldots, x_n)$ est une fonction des racines, ses "valeurs" sont les conjugués $\sigma(v) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ où σ est dans le groupe de Galois.
- L'idée principale de la théorie de Galois (?) est alors d'établir une correspondance entre les corps intermédiaires entre K et L et les sous-groupes du groupe de Galois : si on a $K \subset M \subset L$, le sous-groupe associé à M est l'ensemble des automorphismes qui fixent M.
- Un exemple : si K contient les racines p-ièmes de l'unité et si $\alpha^p = a \in K$, le groupe de Galois de $K(\alpha)$ sur K est cyclique d'ordre p engendré par $\alpha \mapsto \zeta\alpha$ avec $\zeta^p = 1$.

Les sous-groupes distingués

- On considère une extension $K \subset M \subset L$ et le sous-groupe $H = \mathrm{Gal}(L/M)$ associé à M, formé des automorphismes de L qui fixent M.

Les sous-groupes distingués

- On considère une extension $K \subset M \subset L$ et le sous-groupe $H = \mathrm{Gal}(L/M)$ associé à M, formé des automorphismes de L qui fixent M.
- Si l'extension $K \subset M$ est "normale", c'est-à-dire engendrée par **toutes*** les racines $y_1, \ldots, y_r$ d'un polynôme irréductible sur K, Q, le sous-groupe H est distingué dans G.

Les sous-groupes distingués

- On considère une extension $K \subset M \subset L$ et le sous-groupe $H = \mathrm{Gal}(L/M)$ associé à M, formé des automorphismes de L qui fixent M.
- Si l'extension $K \subset M$ est "normale", c'est-à-dire engendrée par **toutes*** les racines $y_1, \ldots, y_r$ d'un polynôme irréductible sur K, Q, le sous-groupe H est distingué dans G.
- En effet, M est stable par G car G permute les racines de Q.

Les sous-groupes distingués

- On considère une extension $K \subset M \subset L$ et le sous-groupe $H = \mathrm{Gal}(L/M)$ associé à M, formé des automorphismes de L qui fixent M.
- Si l'extension $K \subset M$ est "normale", c'est-à-dire engendrée par **toutes*** les racines $y_1, \ldots, y_r$ d'un polynôme irréductible sur K, Q, le sous-groupe H est distingué dans G.
- En effet, M est stable par G car G permute les racines de Q.
- Si $\sigma \in \mathrm{Gal}(L/M)$ et $g \in \mathrm{Gal}(L/K)$, σ fixe M, donc, par le principe de conjugaison, $g\sigma g^{-1}$ fixe $g(M)$, c'est-à-dire M !

Les sous-groupes distingués

- On considère une extension $K \subset M \subset L$ et le sous-groupe $H = \mathrm{Gal}(L/M)$ associé à M, formé des automorphismes de L qui fixent M.
- Si l'extension $K \subset M$ est "normale", c'est-à-dire engendrée par **toutes*** les racines $y_1, \ldots, y_r$ d'un polynôme irréductible sur K, Q, le sous-groupe H est distingué dans G.
- En effet, M est stable par G car G permute les racines de Q.
- Si $\sigma \in \mathrm{Gal}(L/M)$ et $g \in \mathrm{Gal}(L/K)$, σ fixe M, donc, par le principe de conjugaison, $g\sigma g^{-1}$ fixe $g(M)$, c'est-à-dire M !
- Dans le cas étudié par Abel on a $K \subset K(\sqrt[p]{a})$ et cette extension est normale car les racines p-ièmes de l'unité sont dans K. Cela permet de simplifier notablement la preuve d'Abel.

Le premier mémoire de Galois, le théorème principal

- Dans le premier mémoire (envoyé à l'Académie mais refusé), Galois montre le théorème suivant.

Le premier mémoire de Galois, le théorème principal

- Dans le premier mémoire (envoyé à l'Académie mais refusé), Galois montre le théorème suivant.
- *Pour qu'une équation de degré premier, qui n'a pas de diviseurs commensurables, soit soluble par radicaux, il faut et il suffit que toutes les racines soient des fonctions rationnelles de deux quelconques d'entre elles.*

Le premier mémoire de Galois, le théorème principal

- Dans le premier mémoire (envoyé à l'Académie mais refusé), Galois montre le théorème suivant.
- *Pour qu'une équation de degré premier, qui n'a pas de diviseurs commensurables, soit soluble par radicaux, il faut et il suffit que toutes les racines soient des fonctions rationnelles de deux quelconques d'entre elles.*
- En termes modernes : *si $P \in K[X]$ est un polynôme irréductible de degré premier, et si $x_1, \ldots, x_p$ sont ses racines, l'équation $P(x) = 0$ est résoluble par radicaux si et seulement si, quelles que soient les racines x_i, x_j, toutes les racines de P sont dans $K(x_i, x_j)$.*

Exemples

- Si P est un polynôme irréductible de degré premier $p \geq 3$ à coefficients rationnels et si l'équation $P(x) = 0$ est résoluble par radicaux, P a soit une seule racine réelle, soit toutes ses racines réelles.

Exemples

- Si P est un polynôme irréductible de degré premier $p \geq 3$ à coefficients rationnels et si l'équation $P(x) = 0$ est résoluble par radicaux, P a soit une seule racine réelle, soit toutes ses racines réelles.
- Soit p un nombre premier ≥ 5 et soit $P(X) = X^p - p^2X + p$. Alors, P est irréductible sur $\mathbf{Q}$ et l'équation $P(x) = 0$ n'est pas résoluble par radicaux.

Exemples

- Si P est un polynôme irréductible de degré premier $p \geq 3$ à coefficients rationnels et si l'équation $P(x) = 0$ est résoluble par radicaux, P a soit une seule racine réelle, soit toutes ses racines réelles.
- Soit p un nombre premier ≥ 5 et soit $P(X) = X^p - p^2X + p$. Alors, P est irréductible sur $\mathbf{Q}$ et l'équation $P(x) = 0$ n'est pas résoluble par radicaux.
- En effet, le polynôme P a exactement trois racines réelles*.

Une idée de la preuve du théorème de Galois

- Comme dans le cas d'Abel, on a une tour :

$$K = K_0 \subset K_1 \subset \cdots \subset K_{r-1} \subset K_r = L = D_K(P) = K(x_0, x_1, \ldots, x_{p-1})$$

avec $K_{i+1} = K_i(\alpha_i)$ et $\alpha_i^{p_i} = a_i \in K_i$ où p_i est premier, les x_i étant les racines de P.

Une idée de la preuve du théorème de Galois

- Comme dans le cas d'Abel, on a une tour :

$$K = K_0 \subset K_1 \subset \cdots \subset K_{r-1} \subset K_r = L = D_K(P) = K(x_0, x_1, \ldots, x_{p-1})$$

avec $K_{i+1} = K_i(\alpha_i)$ et $\alpha_i^{p_i} = a_i \in K_i$ où p_i est premier, les x_i étant les racines de P.

- Comme on suppose la présence de racines de l'unité, l'extension $K_i \subset K_{i+1}$ est normale.

Une idée de la preuve du théorème de Galois

- Comme dans le cas d'Abel, on a une tour :

$$K = K_0 \subset K_1 \subset \cdots \subset K_{r-1} \subset K_r = L = D_K(P) = K(x_0, x_1, \ldots, x_{p-1})$$

avec $K_{i+1} = K_i(\alpha_i)$ et $\alpha_i^{p_i} = a_i \in K_i$ où p_i est premier, les x_i étant les racines de P.

- Comme on suppose la présence de racines de l'unité, l'extension $K_i \subset K_{i+1}$ est normale.
- On pose $G = \mathrm{Gal}(L/K)$ et $H_i = \mathrm{Gal}(L/K_i)$ et on a :

$$H_r = \{1\} \subset H_{r-1} \subset \cdots \subset H_{i+1} \subset H_i \subset \cdots \subset H_1 \subset G,$$

H_{i+1} est un sous-groupe distingué de H_i et on a $H_{r-1} \simeq \mathbf{Z}/p_{r-1}\mathbf{Z}$ (groupe des racines p_{r-1}-ièmes de l'unité).

La preuve du théorème de Galois (suite)

- Comme P est irréductible, l'un des p_i est nécessairement* égal à p ce qui assure la présence d'un élément d'ordre p (donc un p-cycle) dans le groupe de Galois G et implique la transitivité.

La preuve du théorème de Galois (suite)

- Comme P est irréductible, l'un des p_i est nécessairement* égal à p ce qui assure la présence d'un élément d'ordre p (donc un p-cycle) dans le groupe de Galois G et implique la transitivité.
- *Soit G un sous-groupe de $\mathfrak{S}_p$, p premier, transitif sur $X = \{0, 1, 2, \ldots, p-1\}$ et soit N un sous-groupe distingué de G, distinct de $\{1\}$. Alors N opère transitivement sur X.*

La preuve du théorème de Galois (suite)

- Comme P est irréductible, l'un des p_i est nécessairement* égal à p ce qui assure la présence d'un élément d'ordre p (donc un p-cycle) dans le groupe de Galois G et implique la transitivité.
- *Soit G un sous-groupe de $\mathfrak{S}_p$, p premier, transitif sur $X = \{0, 1, 2, \ldots, p-1\}$ et soit N un sous-groupe distingué de G, distinct de $\{1\}$. Alors N opère transitivement sur X.*
- Conséquences : chaque H_i est transitif sur $\{0, 1, 2, \ldots, p-1\}$. On en déduit que H_{r-1} est de cardinal p.

La preuve du théorème de Galois (suite et fin)

On a le lemme suivant :

- Soient p un nombre premier et G un sous-groupe de $\mathfrak{S}_p$ qui opère sur $\{0, 1, \ldots, p-1\}$ identifié à $\mathbf{Z}/p\mathbf{Z}$. On suppose que G contient un sous-groupe distingué N d'ordre p engendré par $\sigma = (0, 1, \ldots, p-1)$. Soit $g \in G$, on a les propriétés suivantes :
  1) g est une application affine de $\mathbf{Z}/p\mathbf{Z}$, $g(s) = a + ks$ avec $a, k \in \mathbf{Z}/p\mathbf{Z}$ et $k \neq 0$.
  2) Si $g \neq \mathrm{Id}$, g admet au plus un point fixe.
  3) Si g n'est pas dans N, g est d'ordre diviseur de $p-1$. Il en résulte que N est l'unique sous-groupe d'ordre p de G.

La preuve du théorème de Galois (suite et fin)

On a le lemme suivant :

- Soient p un nombre premier et G un sous-groupe de $\mathfrak{S}_p$ qui opère sur $\{0, 1, \ldots, p-1\}$ identifié à $\mathbf{Z}/p\mathbf{Z}$. On suppose que G contient un sous-groupe distingué N d'ordre p engendré par $\sigma = (0, 1, \ldots, p-1)$. Soit $g \in G$, on a les propriétés suivantes :
  1) g est une application affine de $\mathbf{Z}/p\mathbf{Z}$, $g(s) = a + ks$ avec $a, k \in \mathbf{Z}/p\mathbf{Z}$ et $k \neq 0$.
  2) Si $g \neq \mathrm{Id}$, g admet au plus un point fixe.
  3) Si g n'est pas dans N, g est d'ordre diviseur de $p-1$. Il en résulte que N est l'unique sous-groupe d'ordre p de G.
- On en déduit que $G = \mathrm{Gal}(L/K)$ admet H_{r-1} comme sous-groupe distingué d'ordre p.

La preuve du théorème de Galois (suite et fin)

On a le lemme suivant :

- Soient p un nombre premier et G un sous-groupe de $\mathfrak{S}_p$ qui opère sur $\{0, 1, \ldots, p-1\}$ identifié à $\mathbf{Z}/p\mathbf{Z}$. On suppose que G contient un sous-groupe distingué N d'ordre p engendré par $\sigma = (0, 1, \ldots, p-1)$. Soit $g \in G$, on a les propriétés suivantes :
  1) g est une application affine de $\mathbf{Z}/p\mathbf{Z}$, $g(s) = a + ks$ avec $a, k \in \mathbf{Z}/p\mathbf{Z}$ et $k \neq 0$.
  2) Si $g \neq \mathrm{Id}$, g admet au plus un point fixe.
  3) Si g n'est pas dans N, g est d'ordre diviseur de $p-1$. Il en résulte que N est l'unique sous-groupe d'ordre p de G.
- On en déduit que $G = \mathrm{Gal}(L/K)$ admet H_{r-1} comme sous-groupe distingué d'ordre p.
- Conclusion*.

Abel et Galois : le jeu des différences

- Il y a plusieurs différences entre les textes d'Abel et Galois.

Abel et Galois : le jeu des différences

- Il y a plusieurs différences entre les textes d'Abel et Galois.
- La principale est que Galois considère des équations qui ne sont pas nécessairement génériques. C'est là qu'intervient la notion de groupe de Galois.

Abel et Galois : le jeu des différences

- Il y a plusieurs différences entre les textes d'Abel et Galois.
- La principale est que Galois considère des équations qui ne sont pas nécessairement génériques. C'est là qu'intervient la notion de groupe de Galois.
- Il y a aussi une différence importante au niveau des preuves : Abel utilise un sous-groupe d'indice premier (qui correspond à une extension située en bas de la tour), Galois un sous-groupe d'ordre premier (une extension en haut de la tour).

La dernière lettre

- Il s'agit de la lettre écrite par Galois à son ami Auguste Chevalier le 29 mai 1832, c'est-à-dire la veille de sa mort tragique en duel.

La dernière lettre

- Il s'agit de la lettre écrite par Galois à son ami Auguste Chevalier le 29 mai 1832, c'est-à-dire la veille de sa mort tragique en duel.
- C'est un texte absolument extraordinaire.

La dernière lettre

- Il s'agit de la lettre écrite par Galois à son ami Auguste Chevalier le 29 mai 1832, c'est-à-dire la veille de sa mort tragique en duel.
- C'est un texte absolument extraordinaire.
- En substance, il énonce qu'une équation est résoluble par radicaux si et seulement si son groupe peut se dévisser avec des sous-groupes distingués à quotients premiers, c'est-à-dire s'il est résoluble*.

Et maintenant ...

- La théorie de Galois est maintenant un sujet central en algèbre, mais il y reste nombre de questions ouvertes.

Et maintenant ...

- La théorie de Galois est maintenant un sujet central en algèbre, mais il y reste nombre de questions ouvertes.
- Par exemple, une extension finie de $\mathbf{Q}$ étant donnée, on a des moyens de calculer son groupe de Galois. En revanche, on ignore toujours si, un groupe fini étant donné, il existe une extension de $\mathbf{Q}$ admettant ce groupe comme groupe de Galois.

Et maintenant ...

- La théorie de Galois est maintenant un sujet central en algèbre, mais il y reste nombre de questions ouvertes.
- Par exemple, une extension finie de $\mathbf{Q}$ étant donnée, on a des moyens de calculer son groupe de Galois. En revanche, on ignore toujours si, un groupe fini étant donné, il existe une extension de $\mathbf{Q}$ admettant ce groupe comme groupe de Galois.
- Ce problème est lié à une question plus fondamentale, celle de la description du groupe de Galois $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ de la clôture algébrique $\overline{\mathbf{Q}}$ de $\mathbf{Q}$, qui touche à une multitude de domaines des mathématiques actuelles. Mais ceci est une autre histoire ...

Et maintenant ...

- La théorie de Galois est maintenant un sujet central en algèbre, mais il y reste nombre de questions ouvertes.
- Par exemple, une extension finie de $\mathbf{Q}$ étant donnée, on a des moyens de calculer son groupe de Galois. En revanche, on ignore toujours si, un groupe fini étant donné, il existe une extension de $\mathbf{Q}$ admettant ce groupe comme groupe de Galois.
- Ce problème est lié à une question plus fondamentale, celle de la description du groupe de Galois $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ de la clôture algébrique $\overline{\mathbf{Q}}$ de $\mathbf{Q}$, qui touche à une multitude de domaines des mathématiques actuelles. Mais ceci est une autre histoire ...
- Je vous remercie de votre attention.

Références

- Lagrange Joseph-Louis, *Réflexions sur la résolution algébrique des équations*

https://gallica.bnf.fr/ark:/12148/bpt6k229222d/f206

Références

- Lagrange Joseph-Louis, *Réflexions sur la résolution algébrique des équations*

https://gallica.bnf.fr/ark:/12148/bpt6k229222d/f206

- Abel Niels, *Démonstration de l'impossibilité de la résolution algébrique des équations générales qui passent le quatrième degré.* Journal für die reine und angewandte Mathematik, Band 1, Berlin, 1826.
  https://books.google.fr/books?id=4TEPAAAAIAAJ&hl=fr&pg=PR4#v=onepage&q&f=false

Références

- Lagrange Joseph-Louis, *Réflexions sur la résolution algébrique des équations*

https://gallica.bnf.fr/ark:/12148/bpt6k229222d/f206

- Abel Niels, *Démonstration de l'impossibilité de la résolution algébrique des équations générales qui passent le quatrième degré.* Journal für die reine und angewandte Mathematik, Band 1, Berlin, 1826.
https://books.google.fr/books?id=4TEPAAAAIAAJ&hl=fr&pg=PR4#v=onepage&q&f=false
- Galois Evariste, *Œuvres*,
https://www.irphe.fr/~clanet/otherpaperfile/articles/Galois/N0029062_PDF_1_84.pdf

Références (suite)

- Perrin Daniel *Cours d'algèbre*, Ellipses, 1996

Références (suite)

- Perrin Daniel *Cours d'algèbre*, Ellipses, 1996
- Perrin Daniel *Résolution par radicaux*
  `https://www.math.u-psud.fr/~perrin/TER/radicaux.pdf`

Références (suite)

- Perrin Daniel *Cours d'algèbre*, Ellipses, 1996
- Perrin Daniel *Résolution par radicaux*
  `https://www.math.u-psud.fr/~perrin/TER/radicaux.pdf`
- Et bientôt sur ma page web : *Équations, des Babyloniens à Abel et Galois*.

BONUS

Les Arabes et la naissance de l'algèbre

- Un exemple d'Al-Kwarizmi :

  Un homme meurt et laisse quatre fils et il fait, à un homme, une donation égale à la part d'un de ses fils et, à un autre, le quart de la différence entre le tiers de l'héritage et la première donation. Quelle est la part de chacun ?

Les Arabes et la naissance de l'algèbre

- Un exemple d'Al-Kwarizmi :

  Un homme meurt et laisse quatre fils et il fait, à un homme, une donation égale à la part d'un de ses fils et, à un autre, le quart de la différence entre le tiers de l'héritage et la première donation. Quelle est la part de chacun ?

- Traduction : h l'héritage, x la part de chaque fils, $5x + \frac{1}{4}\left(\frac{h}{3} - x\right) = h$ et $x = \dfrac{11h}{57}$.

Retour sur Lagrange et l'équation du troisième degré

Notons qu'inversement, pour trouver les x_i, on résout le système :

$$\begin{cases} x_1 + x_2 + x_3 = 0 \\ x_1 + jx_2 + j^2x_3 = 3u \\ x_1 + j^2x_2 + jx_3 = 3v \end{cases}$$

et on retrouve $x_1 = u + v$. (Le déterminant du système est un Vandermonde !).

Le quatrième degré : l'algèbre

- Elle est résolue par un disciple de Cardan : Ferrari (1540).

Le quatrième degré : l'algèbre

- Elle est résolue par un disciple de Cardan : Ferrari (1540).
- Méthode algébrique. On a $P(x) = x^4 + px^2 + qx + r$, on écrit :

$$x^4 = (x^2 + \lambda)^2 - 2\lambda x^2 - \lambda^2$$

Le quatrième degré : l'algèbre

- Elle est résolue par un disciple de Cardan : Ferrari (1540).
- Méthode algébrique. On a $P(x) = x^4 + px^2 + qx + r$, on écrit :

$$x^4 = (x^2 + \lambda)^2 - 2\lambda x^2 - \lambda^2$$

- On en déduit :

$$P(x) = (x^2 + \lambda)^2 - [(2\lambda - p)x^2 - qx + \lambda^2 - r]$$

et on impose que le deuxième terme soit un carré (on a alors $P = Q^2 - R^2 = (Q - R)(Q + R)$) en écrivant que son discriminant est nul, ce qui donne une équation de degré 3 (la résolvante) :

$$R(\lambda) = 8\lambda^3 - 4p\lambda^2 - 8r\lambda + 4rp - q^2 = 0.$$

Le quatrième degré : la géométrie

- Méthode géométrique : on considère l'équation $F(x) = x^4 + mx^3 + px^2 + qx + r$ et on l'interprète comme l'équation aux x de l'intersection de deux coniques du plan affine, $f(x, y) = y - x^2 = 0$ et $g(x, y) = y^2 + mxy + py + qx + r = 0$.

Le quatrième degré : la géométrie

- Méthode géométrique : on considère l'équation $F(x) = x^4 + mx^3 + px^2 + qx + r$ et on l'interprète comme l'équation aux x de l'intersection de deux coniques du plan affine, $f(x, y) = y - x^2 = 0$ et $g(x, y) = y^2 + mxy + py + qx + r = 0$.
- En pensant au pinceau défini par f, g et à ses coniques dégénérées, on se ramène à résoudre une équation de degré 3 et deux de degré 2. Figure.

Le quatrième degré : la géométrie

- Méthode géométrique : on considère l'équation $F(x) = x^4 + mx^3 + px^2 + qx + r$ et on l'interprète comme l'équation aux x de l'intersection de deux coniques du plan affine, $f(x, y) = y - x^2 = 0$ et $g(x, y) = y^2 + mxy + py + qx + r = 0$.
- En pensant au pinceau défini par f, g et à ses coniques dégénérées, on se ramène à résoudre une équation de degré 3 et deux de degré 2. Figure.
- Voici l'équation dans le cas de $P(x) = x^4 + px^2 + qx + r$:

$$R^*(\lambda) = \lambda^3 + 2p\lambda^2 + \lambda(p^2 - 4r) - q^2.$$

Ce n'est pas exactement celle donnée par Ferrari mais elles sont liées par la formule $R(\lambda) = R^*(2\lambda - p)$.

Le quatrième degré : Lagrange

- Lagrange montre que les racines de l'équation auxiliaire $R(\lambda) = 8\lambda^3 - 4p\lambda^2 - 8r\lambda + 4rp - q^2 = 0$ sont égales à $\lambda = (x_1x_2 + x_3x_4)/2$ et ses permutées, où les x_i sont les racines de $P(x) = x^4 + px^2 + qx + r$.

Le quatrième degré : Lagrange

- Lagrange montre que les racines de l'équation auxiliaire $R(\lambda) = 8\lambda^3 - 4p\lambda^2 - 8r\lambda + 4rp - q^2 = 0$ sont égales à $\lambda = (x_1x_2 + x_3x_4)/2$ et ses permutées, où les x_i sont les racines de $P(x) = x^4 + px^2 + qx + r$.
- Ce qui explique que λ soit racine d'une équation de degré 3 c'est qu'elle est invariante par un sous-groupe d'ordre 8 de $\mathfrak{S}_4$ (engendré par (1324) et (12)).

Le quatrième degré : Lagrange

- Lagrange montre que les racines de l'équation auxiliaire $R(\lambda) = 8\lambda^3 - 4p\lambda^2 - 8r\lambda + 4rp - q^2 = 0$ sont égales à $\lambda = (x_1x_2 + x_3x_4)/2$ et ses permutées, où les x_i sont les racines de $P(x) = x^4 + px^2 + qx + r$.
- Ce qui explique que λ soit racine d'une équation de degré 3 c'est qu'elle est invariante par un sous-groupe d'ordre 8 de $\mathfrak{S}_4$ (engendré par (1324) et (12)).
- On peut aussi utiliser la résolvante de Lagrange $r = x_1 + ix_2 - x_3 - ix_4$ et sa transformée s par la permutation (24). On voit que rs, à un élément du corps de base près, n'est autre que $2(x_1x_3 + x_2x_4)$.

Le théorème de Lagrange

- On attribue à Lagrange le fait que le cardinal d'un sous-groupe d'un groupe fini divise le cardinal du groupe.

Le théorème de Lagrange

- On attribue à Lagrange le fait que le cardinal d'un sous-groupe d'un groupe fini divise le cardinal du groupe.
- En réalité le théorème porte plutôt sur les orbites (dans le cas du groupe symétrique $\mathfrak{S}_n$) :

Le théorème de Lagrange

- On attribue à Lagrange le fait que le cardinal d'un sous-groupe d'un groupe fini divise le cardinal du groupe.
- En réalité le théorème porte plutôt sur les orbites (dans le cas du groupe symétrique $\mathfrak{S}_n$) :
- *On démontrera de même que, si la fonction $f(x', x'', x''', ...)$ est de sa propre nature telle, qu'elle conserve la même valeur en faisant, deux, ou trois, ou un plus grand nombre de permutations différentes entre les racines $x', x'', ...$ les racines de l'équation $\Theta = 0$ seront égales trois à trois, ou quatre à quatre, ... en sorte que la quantité sera égale à un cube ou à un carré-carré etc. et que par conséquent l'équation $\Theta = 0$ se réduira à celle-ci $\theta = 0$ dont le degré sera égal à $n!/3$ ou $n!/4$, etc.*

Et celui de Cauchy

- Version moderne : *Soit n un entier, p le plus grand diviseur premier de n et soit H un sous-groupe de $\mathfrak{S}_n$. Alors H est d'indice 1, 2 ou $\geq p$.*

Et celui de Cauchy

- Version moderne : *Soit n un entier, p le plus grand diviseur premier de n et soit H un sous-groupe de $\mathfrak{S}_n$. Alors H est d'indice 1, 2 ou $\geq p$.*
- Version originale : *Le nombre de valeurs différentes d'une fonction non symétrique de n quantités ne peut s'abaisser au-dessous du plus grand nombre premier p contenu dans n sans devenir égal à 2.*

La définition du groupe de Galois

- On considère une équation $P(x) = 0$, de racines $x_1, \ldots, x_n$ et le corps engendré $L = K(x_1, \ldots, x_n)$.

La définition du groupe de Galois

- On considère une équation $P(x) = 0$, de racines $x_1, \ldots, x_n$ et le corps engendré $L = K(x_1, \ldots, x_n)$.
- Version moderne : *Le groupe de Galois de L sur K est formé des automorphismes de L qui fxent K.*

La définition du groupe de Galois

- On considère une équation $P(x) = 0$, de racines $x_1, \ldots, x_n$ et le corps engendré $L = K(x_1, \ldots, x_n)$.
- Version moderne : *Le groupe de Galois de L sur K est formé des automorphismes de L qui fxent K.*
- Version originale : *Il y aura toujours un groupe de permutations des lettres $x_1, \ldots, x_n$ qui jouira de la propriété suivante :*
  1) Que toute fonction des racines, invariable par les substitutions de ce groupe, soit rationnellement connue ;
  2) Réciproquement, que toute fonction des racines, déterminable rationnellement, soit invariable par les substitutions.

Un exemple de la pensée de Galois : le théorème de l'élément primitif

- Galois énonce ce théorème : si $L = K(x_1, \ldots, x_n)$ est le corps de décomposition de P, il existe $x \in L$ tel que $L = K(x)$.

Un exemple de la pensée de Galois : le théorème de l'élément primitif

- Galois énonce ce théorème : si $L = K(x_1, \ldots, x_n)$ est le corps de décomposition de P, il existe $x \in L$ tel que $L = K(x)$.
- *Il est remarquable que, de cette proposition, on peut conclure que toute équation dépend d'une équation auxiliaire telle que toutes les racines de cette nouvelle équation soient des fonctions rationnelles les unes des autres ... Au surplus, cette remarque est purement curieuse. En effet, une équation qui a cette propriété n'est pas, en général, plus facile à résoudre qu'une autre.*

Un exemple de la pensée de Galois : le théorème de l'élément primitif

- Galois énonce ce théorème : si $L = K(x_1, \ldots, x_n)$ est le corps de décomposition de P, il existe $x \in L$ tel que $L = K(x)$.
- *Il est remarquable que, de cette proposition, on peut conclure que toute équation dépend d'une équation auxiliaire telle que toutes les racines de cette nouvelle équation soient des fonctions rationnelles les unes des autres ... Au surplus, cette remarque est purement curieuse. En effet, une équation qui a cette propriété n'est pas, en général, plus facile à résoudre qu'une autre.*
- Exemple : $D_{\mathbf{Q}}(X^4 - 2) = \mathbf{Q}(\sqrt[4]{2} + i)$, mais l'équation minimale de cet élément est $x^8 + 4x^6 + 2x^4 + 28x^2 + 1 = 0$ et on est bien avancé ...

Le second mémoire (1830)

- Il porte sur les équations dont le groupe est primitif (c'est-à-dire qu'il ne laisse invariante aucune partition des racines).

Le second mémoire (1830)

- Il porte sur les équations dont le groupe est primitif (c'est-à-dire qu'il ne laisse invariante aucune partition des racines).
- Le résultat principal est qu'alors le degré de l'équation est une puissance de nombre premier.

Ah, si Galois et Abel avaient connu l'algèbre linéaire ...

- Une lecture attentive d'Abel et de Galois montre combien les notions modernes (et notamment celle d'espace vectoriel) permettent de simplifier certaines démonstrations. Voici deux exemples.

Ah, si Galois et Abel avaient connu l'algèbre linéaire ...

- Une lecture attentive d'Abel et de Galois montre combien les notions modernes (et notamment celle d'espace vectoriel) permettent de simplifier certaines démonstrations. Voici deux exemples.
- Exemple 1. Soit K un corps, $a \in K$ et α tel que $\alpha^p = a$ avec p premier. Alors toute fraction rationnelle en α est un polynôme en α.

Ah, si Galois et Abel avaient connu l'algèbre linéaire ...

- Une lecture attentive d'Abel et de Galois montre combien les notions modernes (et notamment celle d'espace vectoriel) permettent de simplifier certaines démonstrations. Voici deux exemples.
- Exemple 1. Soit K un corps, $a \in K$ et α tel que $\alpha^p = a$ avec p premier. Alors toute fraction rationnelle en α est un polynôme en α.
- Exemple 2. Avec les notations de l'exemple 1, si on a $x = a_0 + a_1\alpha + \cdots + a_{p-1}\alpha^{p-1}$ et si x n'est pas dans K, on a $\alpha = b_0 + b_1 x + \cdots + b_{p-1}x^{p-1}$.