

Un groupe peu connu d'ordre 18

Rached Mneimné

Mercredi 5 octobre 2016

INTRODUCTION — Nul n'est ~~X~~encé ignorer la Loi sencé

Le monde mathématique est vaste et varié. On peut y étudier des grandes théories, quand on est jeune et habité par le rêve de parcourir tous les jardins du monde. On peut aussi, quand on devient vieux, s'intéresser à quelques fleurs dans le petit jardin d'à côté.

Jeune, je voulais comprendre la classification des groupes finis simples, la cohomologie, le transfert et fusion... Aujourd'hui, je trouve de la fascination dans l'examen des tout premiers exemples de groupes, par exemple le groupe à deux éléments. Je ne suis pas le seul (more than 800 000 views) :

[https : //www.youtube.com/watch?v = UTbye4 – Rhg](https://www.youtube.com/watch?v=UTbye4-Rhg)

En fait, c'est plutôt d'un groupe d'ordre 18 particulier que je vais vous parler aujourd'hui.

Pour ceux qui s'ennuieraient :

[https : //www.youtube.com/watch ?v=uqwC41RDPyg](https://www.youtube.com/watch?v=uqwC41RDPyg)

Assujétir les corps

- Il y a une seule copie du corps $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ dans $\mathbb{C}$, tout comme une seule copie du corps $\mathbb{Q}(i)$. Cela cesse, en revanche, d'être le cas pour le corps $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$, qui possède quant à lui deux autres copies qui lui sont isomorphes dans $\mathbb{C}$, en l'occurrence $\mathbb{Q}(j\sqrt[3]{2})$ et $\mathbb{Q}(j^2\sqrt[3]{2})$, où j est la racine troisième de l'unité de partie imaginaire > 0 . Le corps $\mathbb{Q}(i\sqrt{3}, \sqrt[3]{2})$, engendré par j et $\sqrt[3]{2}$, n'a qu'une seule copie : c'est une extension galoisienne de $\mathbb{Q}$!

Assujétir les corps

- ▶ Il y a une seule copie du corps $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ dans $\mathbb{C}$, tout comme une seule copie du corps $\mathbb{Q}(i)$. Cela cesse, en revanche, d'être le cas pour le corps $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$, qui possède quant à lui deux autres copies qui lui sont isomorphes dans $\mathbb{C}$, en l'occurrence $\mathbb{Q}(j\sqrt[3]{2})$ et $\mathbb{Q}(j^2\sqrt[3]{2})$, où j est la racine troisième de l'unité de partie imaginaire > 0 . Le corps $\mathbb{Q}(i\sqrt{3}, \sqrt[3]{2})$, engendré par j et $\sqrt[3]{2}$, n'a qu'une seule copie : c'est une extension galoisienne de $\mathbb{Q}$!
- ▶ L'étude de ces extensions et de leurs sous-corps relève de ce que l'on appelle la théorie de Galois, qui, à cet effet, met à son service la théorie des groupes, et offre un magnifique pont entre deux théories a priori distinctes, la théorie des corps et celle des groupes. L'objet de notre exposé concerne essentiellement l'étude d'un groupe particulier de cardinal 18, et sa présence dans une situation particulière en théorie des corps.

Assujettir les corps

- ▶ Il y a une seule copie du corps $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ dans $\mathbb{C}$, tout comme une seule copie du corps $\mathbb{Q}(i)$. Cela cesse, en revanche, d'être le cas pour le corps $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$, qui possède quant à lui deux autres copies qui lui sont isomorphes dans $\mathbb{C}$, en l'occurrence $\mathbb{Q}(j\sqrt[3]{2})$ et $\mathbb{Q}(j^2\sqrt[3]{2})$, où j est la racine troisième de l'unité de partie imaginaire > 0 . Le corps $\mathbb{Q}(i\sqrt{3}, \sqrt[3]{2})$, engendré par j et $\sqrt[3]{2}$, n'a qu'une seule copie : c'est une extension galoisienne de $\mathbb{Q}$!
- ▶ L'étude de ces extensions et de leurs sous-corps relève de ce que l'on appelle la théorie de Galois, qui, à cet effet, met à son service la théorie des groupes, et offre un magnifique pont entre deux théories a priori distinctes, la théorie des corps et celle des groupes. L'objet de notre exposé concerne essentiellement l'étude d'un groupe particulier de cardinal 18, et sa présence dans une situation particulière en théorie des corps.
- ▶ Il y a en fait trois groupes d'ordre 18 non commutatifs. On devine deux tels groupes : le produit direct $\mathfrak{S}_3 \times C_3$ du groupe symétrique $\mathfrak{S}_3$ par le groupe cyclique C_3 et le groupe diédral $\mathcal{D}_9$ des isométries du nanogone régulier. Le troisième est notre groupe ! Ce groupe-ci apparaît comme ... le groupe de Galois du polynôme $X^9 + 3X^6 + 3X^3 - 1$, c'est-à-dire comme le groupe des automorphismes du corps $\mathbb{K}$ engendré par les racines de ce polynôme :

$$\mathbb{K} = \mathbb{Q}\left(\sqrt[3]{\sqrt[3]{2} - 1}, i\sqrt{3}\right) \supset \mathbb{Q}.$$

Srinivasa Ramanujan

- ▶ Tout cela est beau et repose un peu sur les épaules de Galois, de Ramanujan et de votre très humble serviteur (et celles d'Alain Debreil) !!

Je ne dois pas oublier Bernadette Perrin Riou.

P.S. Je demande aux auditeurs une certaine maturité mathématique et surtout de connaître les définitions d'un groupe, d'un corps et d'un espace affine, et l'on prendra le soin de rappeler tout ce qui nécessaire à la compréhension de l'exposé.

Srinivasa Ramanujan

- ▶ Tout cela est beau et repose un peu sur les épaules de Galois, de Ramanujan et de votre très humble serviteur (et celles d'Alain Debreil) !!

Je ne dois pas oublier Bernadette Perrin Riou.

P.S. Je demande aux auditeurs une certaine maturité mathématique et surtout de connaître les définitions d'un groupe, d'un corps et d'un espace affine, et l'on prendra le soin de rappeler tout ce qui nécessaire à la compréhension de l'exposé.

- ▶ La formule suivante, due à Ramanujan, sera notre point de départ :

$$\sqrt[3]{\sqrt[3]{2} - 1} = \sqrt[3]{\frac{1}{9}} - \sqrt[3]{\frac{2}{9}} + \sqrt[3]{\frac{4}{9}}.$$

Nous chercherons à partir de là à déterminer toutes les extensions intermédiaires de l'extension galoisienne $\mathbb{K} \supset \mathbb{Q}$ en question, c'est-à-dire tous les corps coincés entre $\mathbb{Q}$ et $\mathbb{K}$.

Question subsidiaire

Existe-t-il des extensions galoisiennes de $\mathbb{Q}$ qui soient de degré 3 ?

Oui ! par exemple $\mathbb{Q}(\cos(2\pi/9))$.

- Méthode de Cardan pour $x^3 - 3x + 1 = 0$. On écrit $x = U + V$ et l'on obtient alors une nouvelle équation $(U^3 + V^3) + 3UV(U + V) - 3(U + V) + 1 = 0$, de sorte que les deux termes en $(U + V)$ vont s'éliminer si $UV = 1$. On se retrouve alors avec les trois conditions

$$U^3 + V^3 = -1; \quad U^3 V^3 = 1; \quad UV = 1.$$

Des deux premières, U^3 et V^3 sont racines de $z^2 + z + 1 = 0$, soit $U^3 = j$ ou j^2 .

Cela permet de remplacer une équation du troisième degré en $x = U + V$ en une équation du second degré en U^3 et V^3 et donne donc trois valeurs possibles pour U et tout autant pour $V = 1/U$, vu la dernière condition. On en déduit aisément que les trois racines de notre polynôme du troisième degré sont $2 \cos(2\pi/9)$, $2 \cos(8\pi/9)$ et $2 \cos(4\pi/9)$.

Question subsidiaire

Existe-t-il des extensions galoisiennes de $\mathbb{Q}$ qui soient de degré 3 ?

Oui ! par exemple $\mathbb{Q}(\cos(2\pi/9))$.

- Méthode de Cardan pour $x^3 - 3x + 1 = 0$. On écrit $x = U + V$ et l'on obtient alors une nouvelle équation $(U^3 + V^3) + 3UV(U + V) - 3(U + V) + 1 = 0$, de sorte que les deux termes en $(U + V)$ vont s'éliminer si $UV = 1$. On se retrouve alors avec les trois conditions

$$U^3 + V^3 = -1; \quad U^3 V^3 = 1; \quad UV = 1.$$

Des deux premières, U^3 et V^3 sont racines de $z^2 + z + 1 = 0$, soit $U^3 = j$ ou j^2 .

Cela permet de remplacer une équation du troisième degré en $x = U + V$ en une équation du second degré en U^3 et V^3 et donne donc trois valeurs possibles pour U et tout autant pour $V = 1/U$, vu la dernière condition. On en déduit aisément que les trois racines de notre polynôme du troisième degré sont $2 \cos(2\pi/9)$, $2 \cos(8\pi/9)$ et $2 \cos(4\pi/9)$.

- La formule de Moivre. On a en effet, en écrivant $(\cos(x) + i \sin x)^3 = \cos(3x) + i \sin(3x)$ et en passant aux parties réelles, l'identité

$$4 \cos^3(x) - 3 \cos(x) - \cos(3x) = 0,$$

laquelle, particularisée en $\alpha = 2\pi/9$, montre que $\cos(2\pi/9)$ est racine de l'équation $(2z)^3 - 3(2z) + 1 = 0$, qui ne sort plus comme ci-dessus du chapeau.

Géométrie

- Le groupe de Galois en question apparaîtra comme le groupe des homothéties-translations $\text{HoT}(2, \mathbb{F}_3)$ du plan affine sur le corps $\mathbb{F}_3$ à trois éléments. Grâce à cela, on dessinera le « treillis » de ses sous-groupes très simplement, et l'on fera l'unité entre Corps, Groupes et Géométrie.

Ce groupe a aussi d'autres vertus et d'autres avatars, que l'on ne déclinera en fin de notre exposé.

- ▶ Le groupe de Galois en question apparaîtra comme le groupe des homothéties-translations $\text{HoT}(2, \mathbb{F}_3)$ du plan affine sur le corps $\mathbb{F}_3$ à trois éléments. Grâce à cela, on dessinera le « treillis » de ses sous-groupes très simplement, et l'on fera l'unité entre Corps, Groupes et Géométrie.

Ce groupe a aussi d'autres vertus et d'autres avatars, que l'on ne déclinera en fin de notre exposé.

- ▶ La suite exacte fondamentale de la géométrie affine

$$\begin{array}{ccccccc} C_3^2 \simeq \mathcal{T}(\mathcal{E}_2, \mathbb{F}_3) & \hookrightarrow & \text{GA}(\mathcal{E}_2, \mathbb{F}_3) & \twoheadrightarrow & \text{GL}(E_2, \mathbb{F}_3) & \simeq & \text{GL}(2, \mathbb{F}_3) \\ & & & & \cup & & \cup \\ C_3^2 \simeq \mathcal{T}(\mathcal{E}_2, \mathbb{F}_3) & \hookrightarrow & \text{HoT}(2, \mathbb{F}_3) & \twoheadrightarrow & \{\pm \text{Id}_E\} & \simeq & \{\pm I_3\} \end{array}$$

On doit, malgré tout, un peu calculer.

► $\mathbb{Q}(\sqrt[3]{\sqrt[3]{2}-1}) = \mathbb{Q}(\sqrt[3]{9}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}).$

On doit, malgré tout, un peu calculer.

- ▶ $\mathbb{Q}(\sqrt[3]{\sqrt[3]{2}-1}) = \mathbb{Q}(\sqrt[3]{9}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3})$.
- ▶ $P(X) = X^9 + 3X^6 + 3X^3 - 1$ est irréductible

On doit, malgré tout, un peu calculer.

- ▶ $\mathbb{Q}(\sqrt[3]{\sqrt[3]{2}-1}) = \mathbb{Q}(\sqrt[3]{9}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3})$.
- ▶ $P(X) = X^9 + 3X^6 + 3X^3 - 1$ est irréductible
- ▶ $P(X+1) =$
 $X^9 + 9X^8 + 36X^7 + 87X^6 + 144X^5 + 171X^4 + 147X^3 + 90X^2 + 36X + 6$.

On doit, malgré tout, un peu calculer.

- ▶ $\mathbb{Q}(\sqrt[3]{\sqrt{32}-1}) = \mathbb{Q}(\sqrt[3]{9}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3})$.
- ▶ $P(X) = X^9 + 3X^6 + 3X^3 - 1$ est irréductible
- ▶ $P(X+1) =$
 $X^9 + 9X^8 + 36X^7 + 87X^6 + 144X^5 + 171X^4 + 147X^3 + 90X^2 + 36X + 6$.
- ▶ Il s'agit, vu que $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, de démontrer que $\sqrt[3]{9} \notin \mathbb{Q}(\sqrt[3]{2})$, c'est-à-dire que l'écriture, en nombres rationnels a, b, c ,

$$9 = (a + b\sqrt[3]{2} + c\sqrt[3]{4})^3$$

est impossible. Cette écriture est équivalente aux trois lignes L_1, L_2, L_3 qui suivent :

$$a^3 + 2b^3 + 4c^3 + 12abc = 9$$

$$a^2b + 2ac^2 + 2b^2c = 0$$

$$a^2c + ab^2 + 2c^2b = 0.$$

La combinaison $cL_2 - bL_3$ produit un miracle.

► La correspondance de Galois

Notre groupe de Galois $G_0 = \text{Gal}(\mathbb{K}, \mathbb{Q})$ n'est pas commutatif puisque $\mathbb{K}$ contient des sous-corps distincts isomorphes ; il contient par ailleurs neuf éléments d'ordre 2.

Comme le 3-Sylow de G_0 est d'indice 2, il y est donc distingué, si bien que $\mathbb{K}$ ne possède qu'un seul sous-corps de degré 2, en l'occurrence $\mathbb{Q}(i\sqrt{3})$. Ce 3-Sylow est ou bien C_9 ou $C_3 \times C_3$. Il ne peut être un C_9 , car, par la correspondance de Galois, cela forcerait $\mathbb{K}$ à n'avoir qu'un seul sous-corps de dimension 6, et nous avons déjà sous la main les corps $\mathbb{Q}(j, \sqrt[3]{2})$ et $\mathbb{Q}(j, \sqrt[3]{9})$ (sans avoir à compter les deux autres).

► La correspondance de Galois

Notre groupe de Galois $G_0 = \text{Gal}(\mathbb{K}, \mathbb{Q})$ n'est pas commutatif puisque $\mathbb{K}$ contient des sous-corps distincts isomorphes ; il contient par ailleurs neuf éléments d'ordre 2.

Comme le 3-Sylow de G_0 est d'indice 2, il y est donc distingué, si bien que $\mathbb{K}$ ne possède qu'un seul sous-corps de degré 2, en l'occurrence $\mathbb{Q}(i\sqrt{3})$. Ce 3-Sylow est ou bien C_9 ou $C_3 \times C_3$. Il ne peut être un C_9 , car, par la correspondance de Galois, cela forcerait $\mathbb{K}$ à n'avoir qu'un seul sous-corps de dimension 6, et nous avons déjà sous la main les corps $\mathbb{Q}(j, \sqrt[3]{2})$ et $\mathbb{Q}(j, \sqrt[3]{9})$ (sans avoir à compter les deux autres).

- En allant dans [AD], on apprend que parmi les trois groupes non commutatifs d'ordre 18, il y a deux qui admettent comme 3-Sylow $C_3 \times C_3$ et deux qui admettent des sous-groupes d'ordre 2 au nombre de 9. Seul, cependant, notre groupe $\text{HoT}(2, \mathbb{F}_3)$ réunit les deux conditions, si bien que $G \simeq G_0$.

Calculer les racines

Les racines de P sont les racines cubiques des trois nombres complexes

$$\sqrt[3]{2} - 1, \quad j\sqrt[3]{2} - 1, \quad j^2\sqrt[3]{2} - 1.$$

Nous n'avons point besoin de les calculer.

Voudrait-on malgré tout le faire, il n'y aurait pas plus facile : il suffit d'appliquer à $y = \sqrt[3]{\sqrt[3]{2} - 1}$ les neuf automorphismes de $\mathbb{K}$ qui laissent j fixe, ce qui fournit alors les neuf racines de ce polynôme. Ainsi, si l'on prend l'automorphisme Υ de $\mathbb{K}$ qui $\sqrt[3]{2} \rightsquigarrow j\sqrt[3]{2}$, $\sqrt[3]{9} \rightsquigarrow j^2\sqrt[3]{9}$ et $j \rightsquigarrow j$, on a que

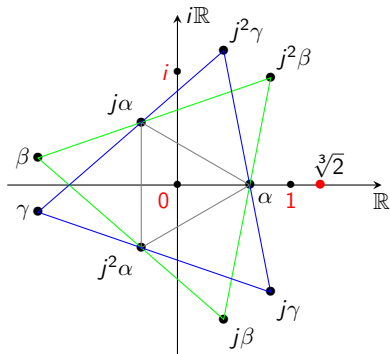
$$\Upsilon(\sqrt[3]{\sqrt[3]{2} - 1}) = \Upsilon\left(\frac{1 - \sqrt[3]{2} + \sqrt[3]{4}}{\sqrt[3]{9}}\right) = \frac{1 - j\sqrt[3]{2} + j^2\sqrt[3]{4}}{j^2\sqrt[3]{9}}$$

vérifie encore l'équation $(X^3 + 1)^3 = 2$, et son cube est égal à

$\Psi(y^3) = \Psi(\sqrt[3]{2} - 1) = j\sqrt[3]{2} - 1$, puisque l'on sait que les neuf corps qu'elles engendrent sont isomorphes à $\mathbb{Q}(y)$, et sont donc engendrés par deux corps choisis l'un parmi les corps $\mathbb{Q}(x)$, $\mathbb{Q}(jx)$, $\mathbb{Q}(j^2x)$ et l'autre parmi $\mathbb{Q}(z)$, $\mathbb{Q}(jz)$, $\mathbb{Q}(j^2z)$, avec $x = \sqrt[3]{2}$ et $z = \sqrt[3]{9}$. Or, tous ces corps sont dans le corps $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{9}, i\sqrt{3})$.

Position des neuf racines de $X^9 + 3X^6 + 3X^3 - 1$ dans $\mathbb{C}$

On note $\beta \approx -1.228 + i 0.245$,
et aussi $\gamma \approx -1.228 - i 0.245$.



$$\alpha = \sqrt[3]{\sqrt[3]{2} - 1} \approx 0.638$$

$$\sqrt[3]{2} \approx 1.260$$

$$|\beta| \approx 1.252$$

Remarquons que si l'on pose $a = \sqrt[3]{2}$ et $b = \sqrt[3]{9}$, alors on a

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

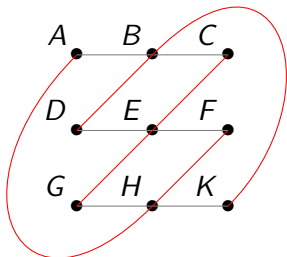
$$\beta = (j^2 - a + ja^2)/b$$

$$\gamma = (j - a + j^2 a^2)/b$$

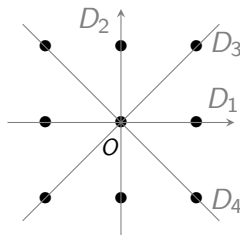
L'espace affine $(\mathcal{E}_2, E_2, \mathbb{F}_3)$

- Neuf points
- Quatre directions de droites
- Douze droites
- Par chaque point passent quatre droites.

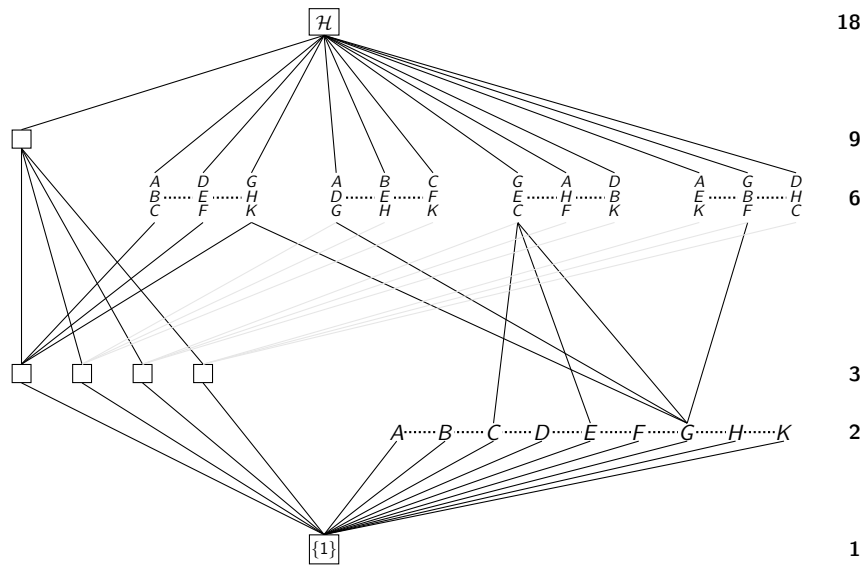
$$\mathcal{E}_2(\mathbb{F}_3)$$



$$E_2 \simeq \mathbb{F}_3^2$$

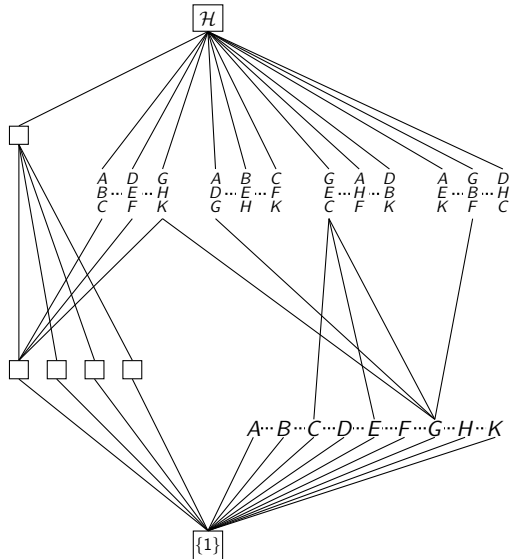


Le treillis des sous-groupes de $\text{HoT}(\mathcal{E}_2, \mathbb{F}_3)$

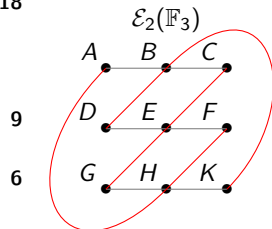


Treillis de $C_3^2 \rtimes_r C_2$, diédral généralisé de C_3^2

Le treillis des sous-groupes de $\text{HoT}(\mathcal{E}_2, \mathbb{F}_3)$



18



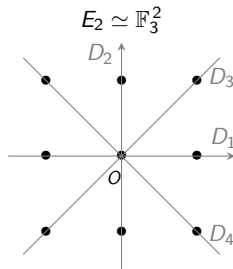
9

6

3

2

1

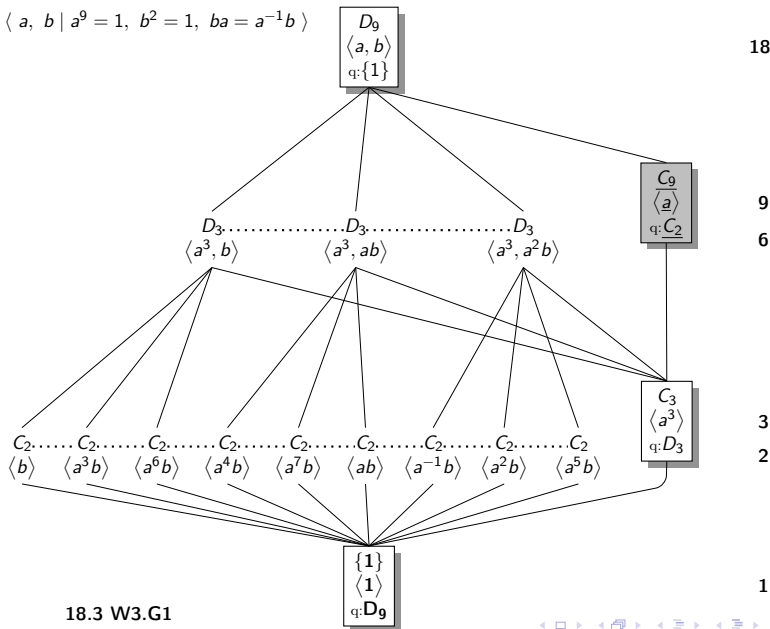


Treillis de $C_3^2 \rtimes_r C_2$, diédral généralisé de C_3^2

Le groupe $\mathcal{D}_9$ des isométries du nonagone régulier

$$\langle a, b \mid a^9 = 1, b^2 = 1, ba = a^{-1}b \rangle$$

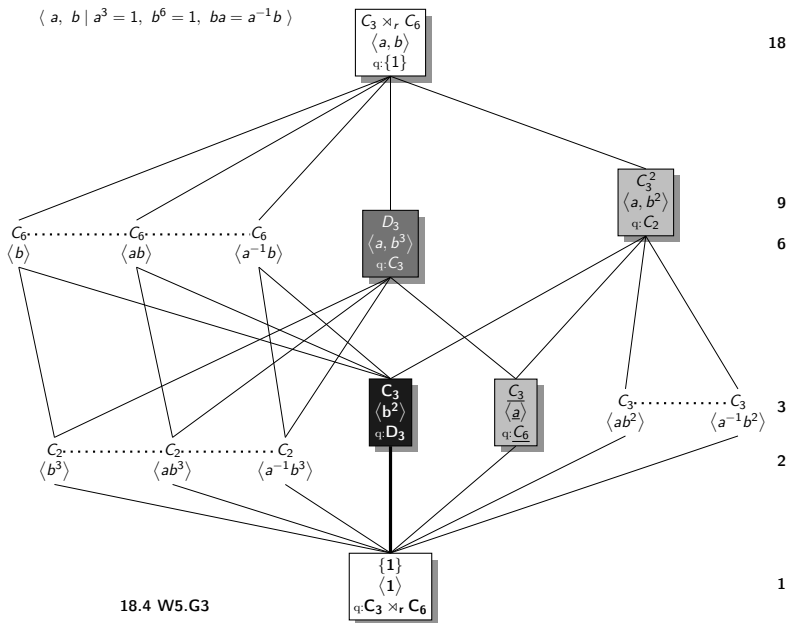
18



Le produit direct $\mathfrak{S}_3 \times C_3$

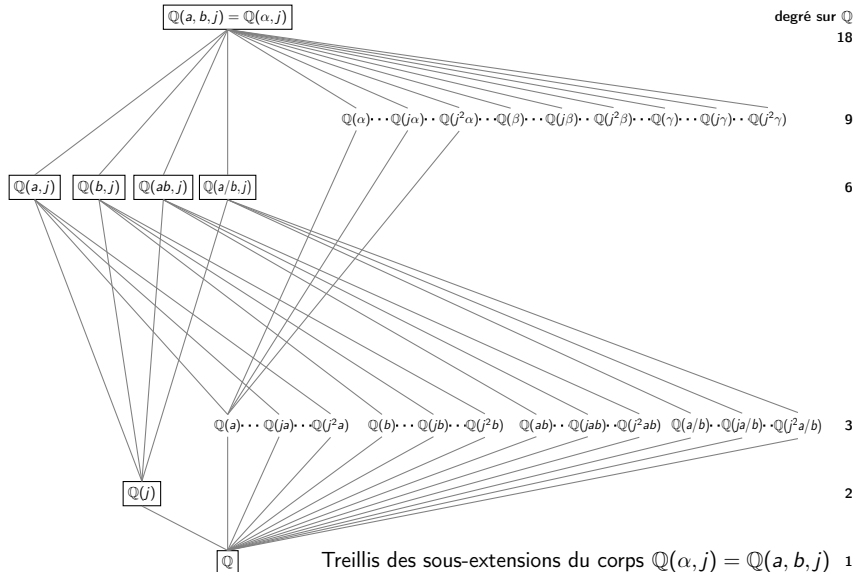
$$\langle a, b \mid a^3 = 1, b^6 = 1, ba = a^{-1}b \rangle$$

18

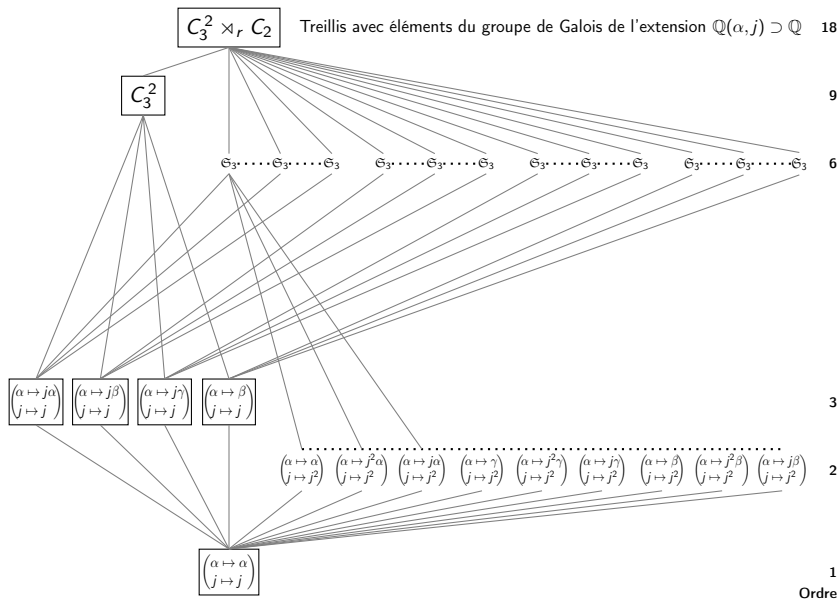


18.4 W5.G3

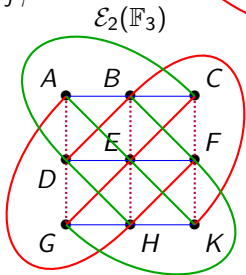
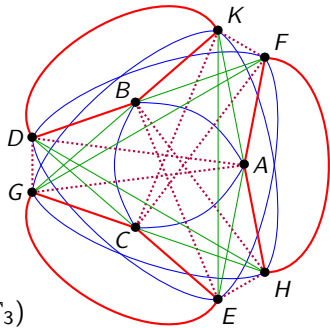
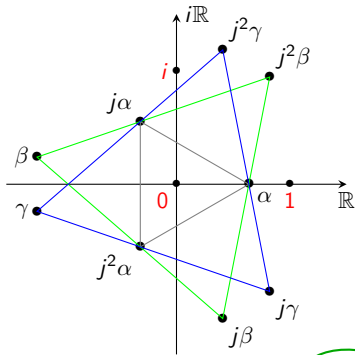
Les extensions intermédiaires



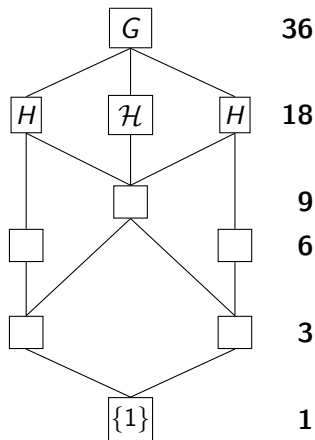
En cadeau, le groupe de Galois



Position des neuf racines de $X^9 + 3X^6 + 3X^3 - 1$ dans $\mathbb{C}$



Le treillis des sous-groupes distingués de $\mathfrak{S}_3 \times \mathfrak{S}_3$



Le treillis distingué de $G = \mathfrak{S}_3 \times \mathfrak{S}_3$

La table des caractères de notre groupe d'ordre 18,
maintenant trop bien connu

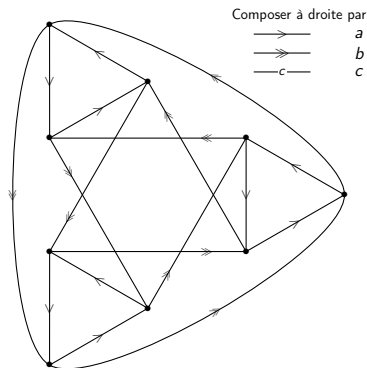
# ordre représ.	1 1 (0, 0), 0	9 2 (0, 0), ϵ	2 3 (1, 0), 0	2 3 (1, 1), 0	2 3 (1, 2), 0	2 3 (0, 1), 0
χ_1	1	1	1	1	1	1
χ_2	1	-1	1	1	1	1
χ_3	2	0	2	-1	-1	-1
χ_4	2	0	-1	2	-1	-1
χ_5	2	0	-1	-1	2	-1
χ_6	2	0	-1	-1	-1	2

Graphes de Cayley

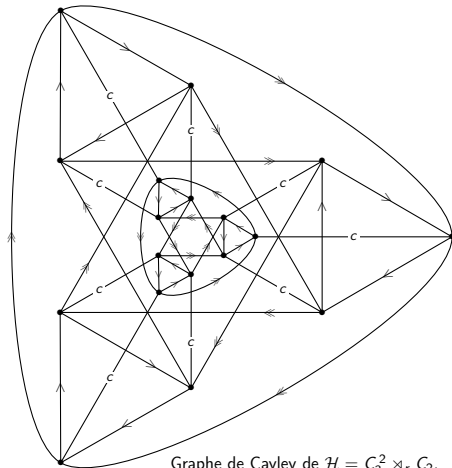
Il admet comme présentation

$$\mathcal{H} = \langle a, b, c \mid a^3 = b^3 = c^2 = 1, ba = ab, cac^{-1} = a^{-1}, cbc^{-1} = b^{-1} \rangle.$$

Son treillis montre qu'il ne peut être engendré par deux seuls de ses éléments



Graphe de Cayley de $C_3 \times C_3$



Graphe de Cayley de $\mathcal{H} = C_3^2 \rtimes_r C_2$,
pour la présentation (1) ci-dessus

Bibliographie.–

[AD]– Alain Debreil. *Groupes finis et treillis de leurs sous-groupes*. Calvage & Mounet, 2016.

[BPR]– Bernadette Perrin-Riou. *Algèbre, Arithmétique et Maple*. Cassini 2000.

[MDE]– Mneimné-Danila-Eiden. *Un bouquet d'exercices pour le M1*. À paraître chez Calvage & Mounet en 2017.

[Mn]– Conférence IREM (Nov. 2011) Rached Mneimné. *Galois ? Prenez la correspondance !* (video en circulation restreinte).

[DP]– Daniel Perrin. Cubes et racines cubiques. PDF attaché. (Orsay, 10 octobre 2016)