

A too little known group of order 18

Rached Mneimné

Lahore

Friday and Saturday, December 9th and 10th – 2016

INTRODUCTION.—

The mathematical world is vast and varied. One can study great theories, when young and inhabited by the dream of traversing all the gardens of the world. When becoming old, one can also, take an interest in some flowers in the small garden next door.

Young, I wanted to understand the classification of Simple Finite Groups, Cohomology, Transfer and Fusion... Today, I find fascination in examining the very first examples of groups, for example the two-element group. I'm not the only one (more than 800 000 views).

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

In fact, it's more of a particular group of order 18 that I will talk about today, and the day after.

For those who would soon be bored:

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

Controlling Fields

- There is only one copy of the field $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ in $\mathbb{C}$, as much as the number of copies of $\mathbb{Q}(i)$. On the other hand, it ceases to be the case for the field $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$, which has two other isomorphic copies inside $\mathbb{C}$, more specifically the fields $\mathbb{Q}(j\sqrt[3]{2})$ et $\mathbb{Q}(j^2\sqrt[3]{2})$, where $j = e^{2i\pi/3}$.

The field $\mathbb{Q}(i\sqrt{3}, \sqrt[3]{2})$, generated by j et $\sqrt[3]{2}$, has only one copy: It is a Galois-extension of $\mathbb{Q}$!

Controlling Fields

- ▶ There is only one copy of the field $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ in $\mathbb{C}$, as much as the number of copies of $\mathbb{Q}(i)$. On the other hand, it ceases to be the case for the field $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$, which has two other isomorphic copies inside $\mathbb{C}$, more specifically the fields $\mathbb{Q}(j\sqrt[3]{2})$ et $\mathbb{Q}(j^2\sqrt[3]{2})$, where $j = e^{2i\pi/3}$.

The field $\mathbb{Q}(i\sqrt{3}, \sqrt[3]{2})$, generated by j et $\sqrt[3]{2}$, has only one copy: It is a Galois-extension of $\mathbb{Q}$!

- ▶ The study of these extensions and their subfields falls within the so-called Galois Theory, which for this purpose puts at its favor Group Theory, and offers a magnificent bridge between two *a priori* distinct theories: the Theory of Fields and that of Groups.

The subject of my talk essentially concerns the study of a particular group of order 18, and its presence in a particular situation in Field Theory.

Controlling Fields

- There is only one copy of the field $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ in $\mathbb{C}$, as much as the number of copies of $\mathbb{Q}(i)$. On the other hand, it ceases to be the case for the field $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$, which has two other isomorphic copies inside $\mathbb{C}$, more specifically the fields $\mathbb{Q}(j\sqrt[3]{2})$ et $\mathbb{Q}(j^2\sqrt[3]{2})$, where $j = e^{2i\pi/3}$.

The field $\mathbb{Q}(i\sqrt{3}, \sqrt[3]{2})$, generated by j et $\sqrt[3]{2}$, has only one copy: It is a Galois-extension of $\mathbb{Q}$!

- The study of these extensions and their subfields falls within the so-called Galois Theory, which for this purpose puts at its favor Group Theory, and offers a magnificent bridge between two *a priori* distinct theories: the Theory of Fields and that of Groups.

The subject of my talk essentially concerns the study of a particular group of order 18, and its presence in a particular situation in Field Theory.

- There are actually three non-commutative groups of order 18. One guesses easily two such groups: On one hand, the direct product $\mathfrak{S}_3 \times C_3$ of the symmetric group $\mathfrak{S}_3$ with the cyclic group C_3 , and on the other hand the dihedral group $\mathcal{D}_9$ of the isometries of the regular 9-gone. The third is our group! This group appears as the Galois group of the polynomial $X^9 + 3X^6 + 3X^3 - 1$, that is to say as the automorphism Group of the field $\mathbb{K}$ generated by the roots of that polynomial:

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

Our friend Srinivasa Ramanujan

- ▶ All this is beautiful and rests on the shoulders of Galois and Ramanujan, and much little on those of your very humble servant.

Great thanks to Alain Debreil and Bernadette Perrin-Riou

Our friend Srinivasa Ramanujan

- ▶ All this is beautiful and rests on the shoulders of Galois and Ramanujan, and much little on those of your very humble servant.

Great thanks to Alain Debreil and Bernadette Perrin-Riou

- ▶ The following formula, due to Ramanujan, will be our starting point:

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

We shall then try to determine all the intermediate extensions of our Galois extension $\mathbb{K} \supset \mathbb{Q}$, i.e. all fields wedged between $\mathbb{Q}$ and $\mathbb{K}$.

Subsidiary question

Are there 3-degrees Galois extensions of $\mathbb{Q}$?

Yes! For example, $\mathbb{Q}(\cos(2\pi/9))$.

- ▶ Cardan method for $x^3 - 3x + 1 = 0$. We write $x = U + V$, and obtain a new equation $(U^3 + V^3) + 3UV(U + V) - 3(U + V) + 1 = 0$, so that the two terms in $(U + V)$ will be eliminated if $UV = 1$. We then find ourselves with the three conditions :

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

Of the first two, U^3 et V^3 are roots of $z^2 + z + 1 = 0$, soit $U^3 = j$ ou j^2 . This allows to replace a third degree equation in $x = U + V$ by a second degree equation in U^3 et V^3 , and thus gives three possible values for U and equally for $V = 1/U$, given the last condition. It is now easy to deduce that the three roots of our third degree polynomial are $2 \cos(2\pi/9)$, $2 \cos(8\pi/9)$ et $2 \cos(4\pi/9)$.

Subsidiary question

Are there 3-degrees Galois extensions of $\mathbb{Q}$?

Yes! For example, $\mathbb{Q}(\cos(2\pi/9))$.

- ▶ Cardan method for $x^3 - 3x + 1 = 0$. We write $x = U + V$, and obtain a new equation $(U^3 + V^3) + 3UV(U + V) - 3(U + V) + 1 = 0$, so that the two terms in $(U + V)$ will be eliminated if $UV = 1$. We then find ourselves with the three conditions :

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

Of the first two, U^3 et V^3 are roots of $z^2 + z + 1 = 0$, soit $U^3 = j$ ou j^2 . This allows to replace a third degree equation in $x = U + V$ by a second degree equation in U^3 et V^3 , and thus gives three possible values for U and equally for $V = 1/U$, given the last condition. It is now easy to deduce that the three roots of our third degree polynomial are $2 \cos(2\pi/9)$, $2 \cos(8\pi/9)$ et $2 \cos(4\pi/9)$.

- ▶ Moivre's Formula. In fact, by writing $(\cos(x) + i \sin x)^3 = \cos(3x) + i \sin(3x)$ and passing to the real parts, one gets the well known identity

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

which, specialized at $\alpha = 2\pi/9$, shows that $\cos(2\pi/9)$ is root of the equation $(2z)^3 - 3(2z) + 1 = 0$, which no longer comes out as above like a rabbit out of one's hat.

Geometry

- ▶ The Galois group in question will appear as the group of homotheties-translations $G := \text{HoT}(2, \mathbb{F}_3)$ of the affine Plane over the field $\mathbb{F}_3$ with three elements. Thanks to this, we will draw the lattice of its subgroups very simply, and we will make Unity between Fields, Groups et Geometry.

This group also has other virtues and other avatars, which will be declined at the end of my talk.

Geometry

- ▶ The Galois group in question will appear as the group of homotheties-translations $G := \text{HoT}(2, \mathbb{F}_3)$ of the affine Plane over the field $\mathbb{F}_3$ with three elements. Thanks to this, we will draw the lattice of its subgroups very simply, and we will make Unity between Fields, Groups et Geometry.

This group also has other virtues and other avatars, which will be declined at the end of my talk.

- ▶ The Fundamental Exact Sequence of affine Geometry

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

One must accept to do, after all, some little calculations.

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

One must accept to do, after all, some little calculations.

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

One must accept to do, after all, some little calculations.

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

► $P(X) = X^9 + 3X^6 + 3X^3 - 1$ is irreducible

► $P(X+1) =$

$$X^9 + 9X^8 + 36X^7 + 87X^6 + 144X^5 + 171X^4 + 147X^3 + 90X^2 + 36X + 6.$$

One must accept to do, after all, some little calculations.

- ▶ $\mathbb{Q}(\sqrt[3]{\sqrt[3]{2}-1}) = \mathbb{Q}(\sqrt[3]{9}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3})$.
- ▶ $P(X) = X^9 + 3X^6 + 3X^3 - 1$ is irreducible
- ▶ $P(X+1) =$
 $X^9 + 9X^8 + 36X^7 + 87X^6 + 144X^5 + 171X^4 + 147X^3 + 90X^2 + 36X + 6$.
- ▶ Taking in account the fact that $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, we must prove that $\sqrt[3]{9} \notin \mathbb{Q}(\sqrt[3]{2})$, that is to say that the writing, in rational numbers α, β, γ ,

$$9 = (\alpha + \beta\sqrt[3]{2} + \gamma\sqrt[3]{4})^3$$

is impossible. This equation is equivalent to the following three lines L_1, L_2, L_3 :

$$\alpha^3 + 2\beta^3 + 4\gamma^3 + 12\alpha\beta\gamma = 9$$

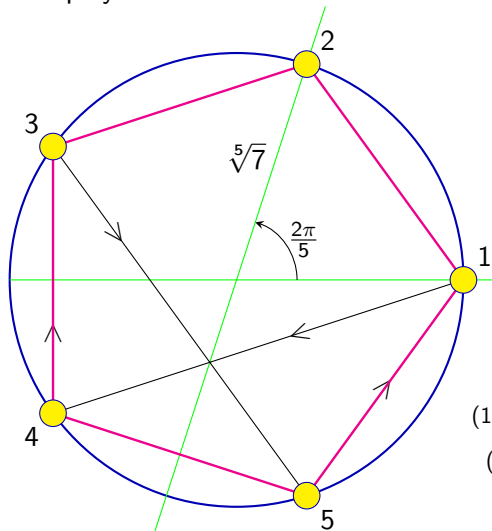
$$\alpha^2\beta + 2\beta^2\gamma + 2\gamma^2\alpha = 0$$

$$\alpha^2\gamma + \beta^2\alpha + 2\gamma^2\beta = 0.$$

The $\gamma L_2 - \beta L_3$ combination produces a miracle.

The Galois correspondance – Aperitif

The polynomial $X^5 - 7$ and the Frobenius group F_{20}



Elements of the normalizer in $\mathfrak{S}_5$ of the 5-Sylow generated by $\sigma = (12345)$ could be seen on this picture.

$$(13)(45) \circ \sigma \circ (13)(45) = (32154) = \sigma^{-1}$$

$$(1534) \circ \sigma \circ (1534)^{-1} = (52413) = \sigma^2$$

Do not eat too many appetizers, as you will not be hungry anymore!

The Galois correspondance

- Our Galois group $G_0 = \text{Gal}(\mathbb{K}, \mathbb{Q})$ is not commutative, since $\mathbb{K}$ contains isomorphic subfields! It contains otherwise nine elements of order 2 (these are the automorphisms which do not fix j).

Being of index 2 in G_0 , therefore normal in G_0 , a 3-Sylow subgroup G_0 is necessarily unique, so that $\mathbb{K}$ contains a unique subfield of degree 2, which is as it happens $\mathbb{Q}(i\sqrt{3})$.

This 3-Sylow is either C_9 or $C_3 \times C_3$. In fact, it cannot be C_9 , since, by Galois correspondance, our field $\mathbb{K}$ should have only one subfield of degree 6, and we have already at hand the fields $\mathbb{Q}(j, \sqrt[3]{2})$ et $\mathbb{Q}(j, \sqrt[3]{9}) = \mathbb{Q}(j, \sqrt[3]{3})$ (without having to count the other two).

The Galois correspondance

- ▶ Our Galois group $G_0 = \text{Gal}(\mathbb{K}, \mathbb{Q})$ is not commutative, since $\mathbb{K}$ contains isomorphic subfields! It contains otherwise nine elements of order 2 (these are the automorphismes which do not fix j).

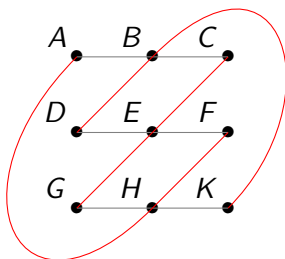
Being of index 2 in G_0 , therefore normal in G_0 , a 3-Sylow subgroup G_0 is necessarily unique, so that $\mathbb{K}$ contains a unique subfield of degree 2, which is as it happens $\mathbb{Q}(i\sqrt{3})$. This 3-Sylow is either C_9 or $C_3 \times C_3$. In fact, it cannot be C_9 , since, by Galois correspondance, our field $\mathbb{K}$ should have only one subfield of degree 6, and we have already at hand the fields $\mathbb{Q}(j, \sqrt[3]{2})$ et $\mathbb{Q}(j, \sqrt[3]{9}) = \mathbb{Q}(j, \sqrt[3]{3})$ (without having to count the other two).

- ▶ By going to [AD], we learn that among the three non-commutative groups of order 18, there are two that admit as 3-Sylow $C_3 \times C_3$ and two that admit nine subgroups of order 2. Only, however, our $G = \text{HoT}(2, \mathbb{F}_3)$ group meets the two conditions, so $G \simeq G_0$.

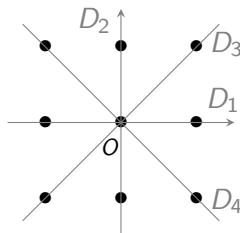
The Affine Space $(\mathcal{E}_2, E_2, \mathbb{F}_3)$

- Nine points
- Four line directions
- Twelve lines
- By each point pass four straight lines.

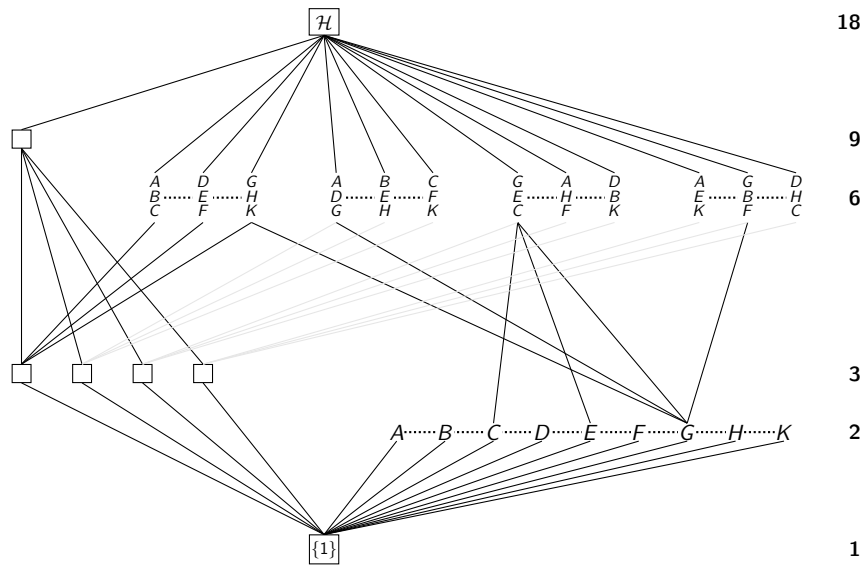
$$\mathcal{E}_2(\mathbb{F}_3)$$



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

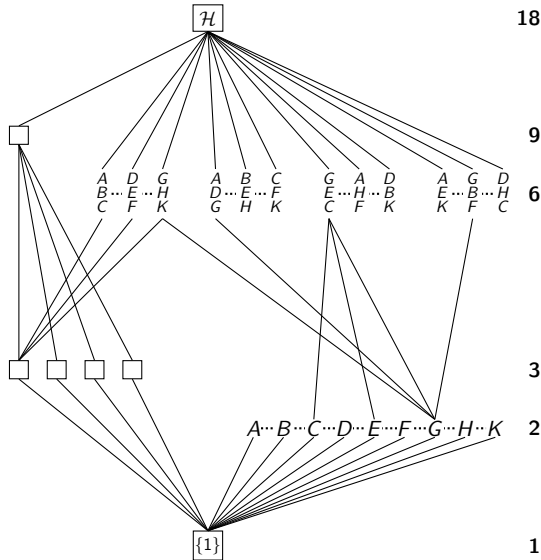


The lattice of subgroups $\text{HoT}(\mathcal{E}_2, \mathbb{F}_3)$

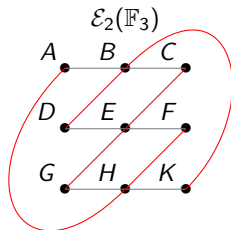


Lattice of subgroups of $C_3^2 \rtimes_r C_2$, the generalised dihedral group of C_3^2

The lattice of Subgroups of $\text{HoT}(\mathcal{E}_2, \mathbb{F}_3)$ – A better view



18



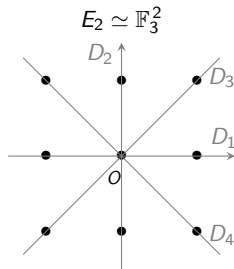
9

6

3

2

1

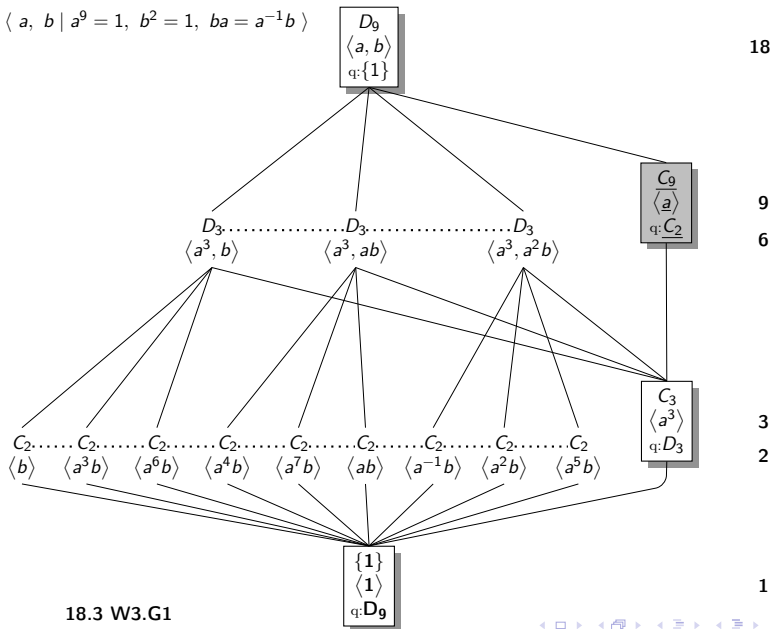


Lattice of subgroups of $C_3^2 \rtimes_r C_2$, the generalised dihedral of C_3^2

Dihedral group $\mathcal{D}_9$ of isometries of the regular nonagone

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

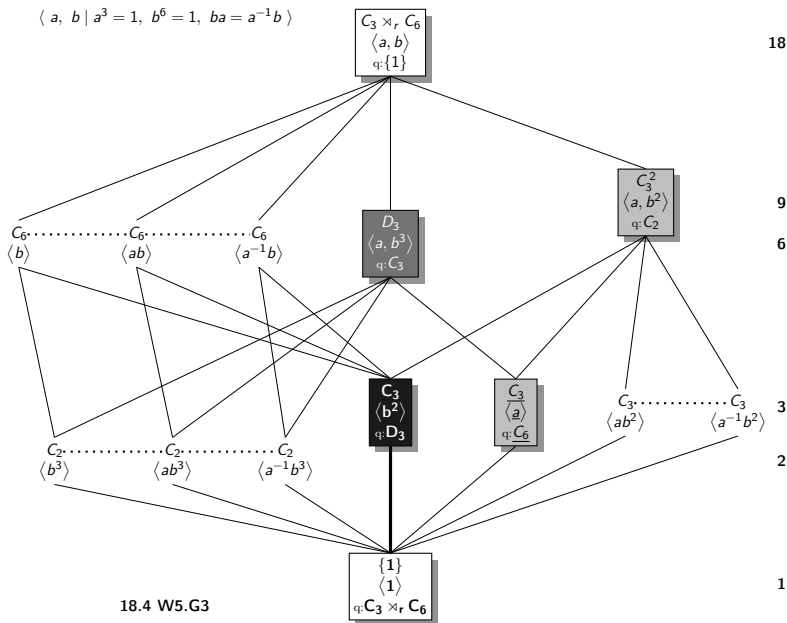
18



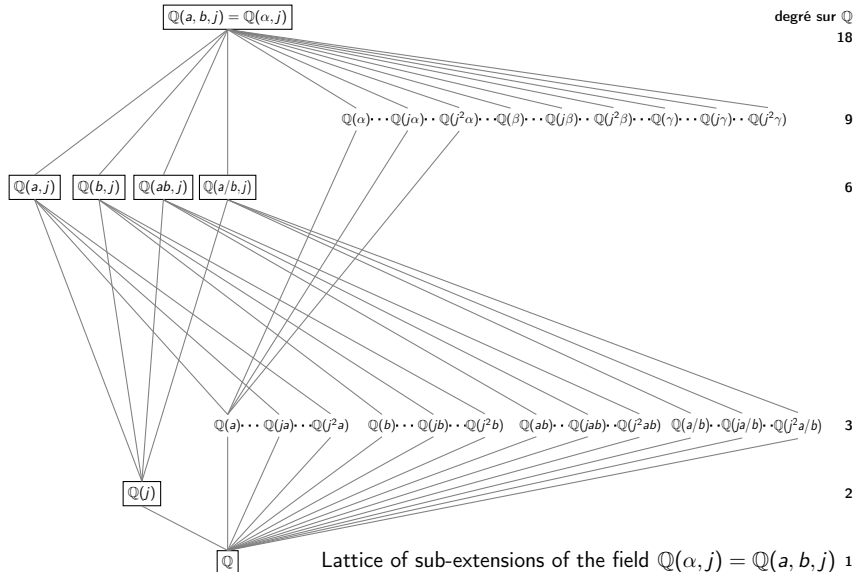
The direct product $\mathfrak{S}_3 \times C_3 \simeq C_3 \wr C_2$

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

18



The intermediate extensions



Computing the roots

The roots of P are the cubic roots of the three complex numbers

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

We do not need to calculate them.

Would you still do it, there would not be easier : It is enough to apply to

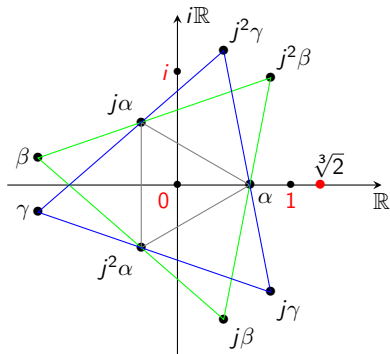
$y = \sqrt[3]{\sqrt[3]{2} - 1}$ the nine automorphisms of $\mathbb{K}$ which leave j fixed, which then provides the nine roots of this polynomial. Thus, if we take automorphism Υ of $\mathbb{K}$ which $\sqrt[3]{2} \rightsquigarrow j\sqrt[3]{2}$, $\sqrt[3]{9} \rightsquigarrow j^2\sqrt[3]{9}$ et $j \rightsquigarrow j$, we get that

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

still satisfies the equation $(X^3+1)^3=2$, and its cube is equal to $\Psi(y^3)=\Psi(\sqrt[3]{2}-1)=j\sqrt[3]{2}-1$, since we know that the nine fields they generate are isomorphic to $\mathbb{Q}(y)$, and are thus generated by two fields chosen one among the fields $\mathbb{Q}(a)$, $\mathbb{Q}(ja)$, $\mathbb{Q}(j^2a)$ and the other among $\mathbb{Q}(b)$, $\mathbb{Q}(jb)$, $\mathbb{Q}(j^2b)$, with $a = \sqrt[3]{2}$ and $b = \sqrt[3]{9}$. Now, all these fields are in the field $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{9}, i\sqrt{3})$.

Position in $\mathbb{C}$ of the nine roots of $X^9 + 3X^6 + 3X^3 - 1$

Let $\beta \approx -1.228 + i0.245$,
and let also $\gamma \approx -1.228 - i0.245$.



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

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

$$|\beta| \approx 1.252$$

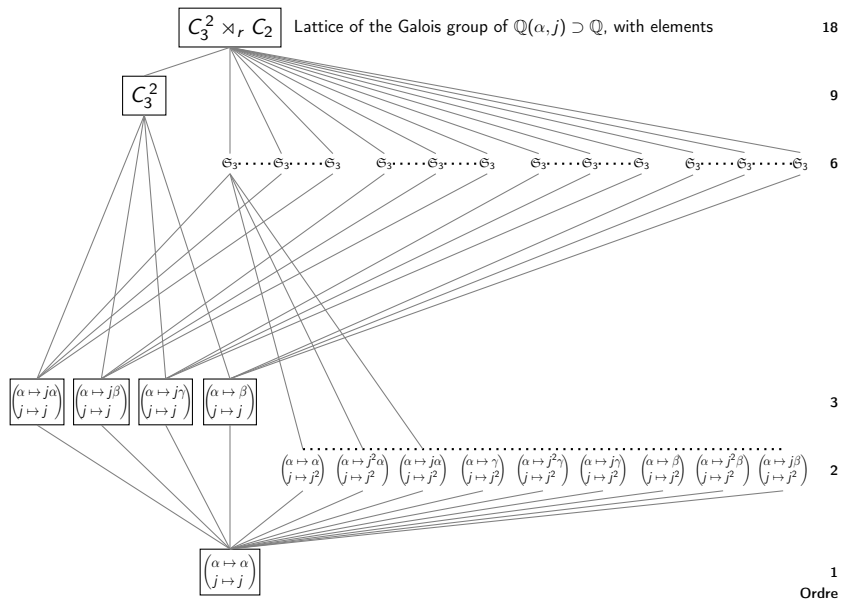
Note that if one puts $a = \sqrt[3]{2}$ et $b = \sqrt[3]{9}$, then we have

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

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

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

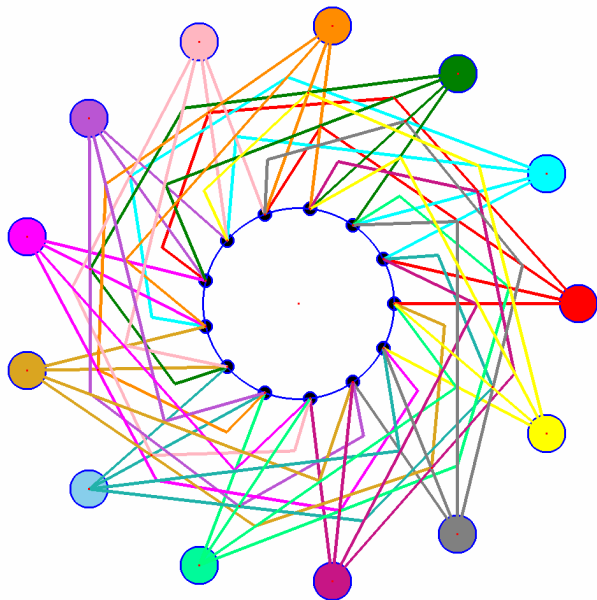
As a gift, the Galois group



Chase the natural, it comes galloping back :
Affine Geometry, the return (of the Jedi).

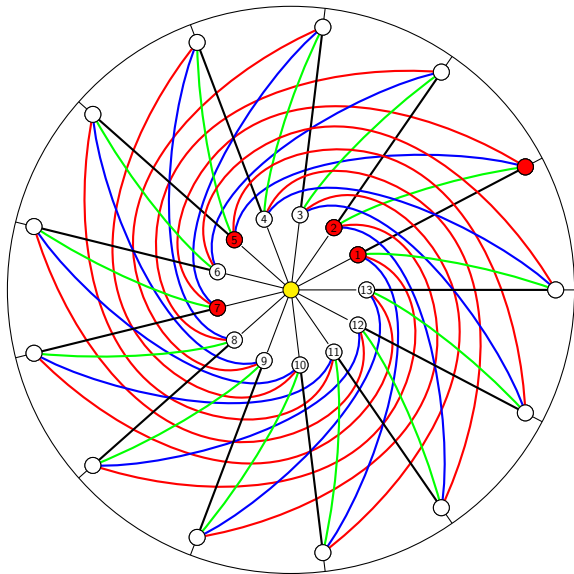
In the previous Lattice, there is hidden a very nice affine space.
And, more unbelievably, this lattice hides also the picture of the
Projective Plane over $\mathbb{F}_3$.

Spiders' Nest.— The Kellerian 13-star

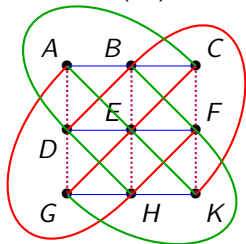
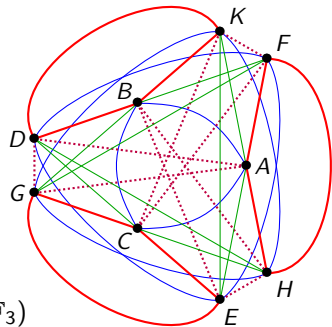
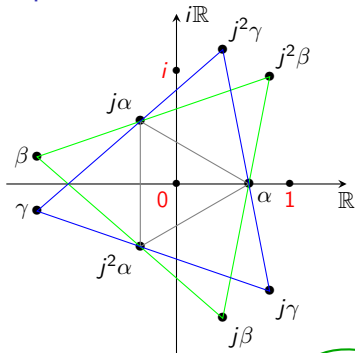


The Field $\mathbb{F}_{3^3} \simeq \mathbb{F}_3[X]/(X^3 - X + 1)$. The Cyclic group $C_{26} \simeq \mathbb{F}_{27}^* = \langle \overline{X} \rangle$.

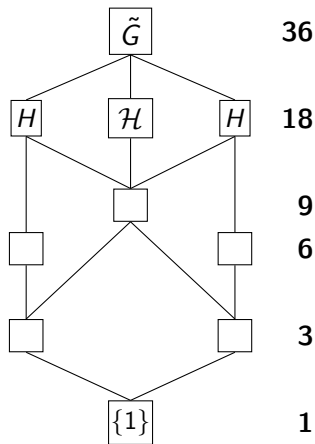
Subgroups of $C_3 \times C_3 \times C_3$.— Smooth, but as much venomous!



The set of the nine roots of $X^9 + 3X^6 + 3X^3 - 1$ as an affine space



The Lattice of normal subgroups of $\tilde{G} := \mathfrak{S}_3 \times \mathfrak{S}_3$



The Invariant Lattice of $\tilde{G} = \mathfrak{S}_3 \times \mathfrak{S}_3$

Character Table of our **much well know** group of order 18,

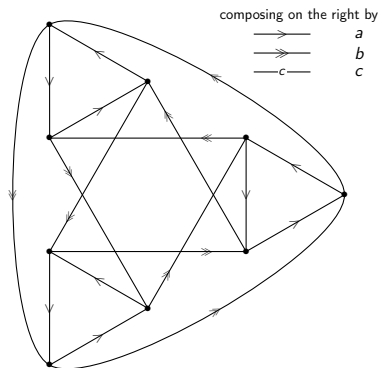
# ordre représ.	1 1 $(0, 0), 0$	9 2 $(0, 0), \varepsilon$	2 3 $(1, 0), 0$	2 3 $(1, 1), 0$	2 3 $(1, 2), 0$	2 3 $(0, 1), 0$
χ_1	1	1	1	1	1	1
χ_2	1	-1	1	1	1	1
χ_3	2	0	2	-1	-1	-1
χ_4	2	0	-1	2	-1	-1
χ_5	2	0	-1	-1	2	-1
χ_6	2	0	-1	-1	-1	2

Cayley Graphs

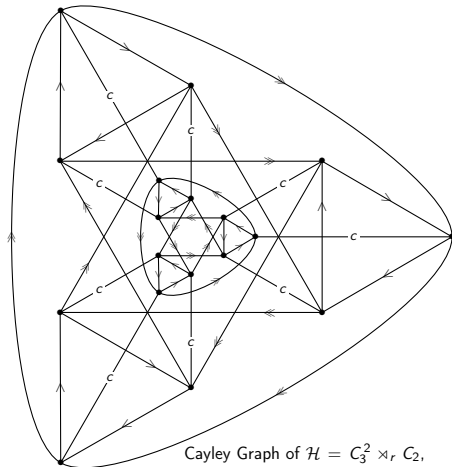
It admits as a presentation

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

Its lattice shows that it can not be generated by only two of its elements!

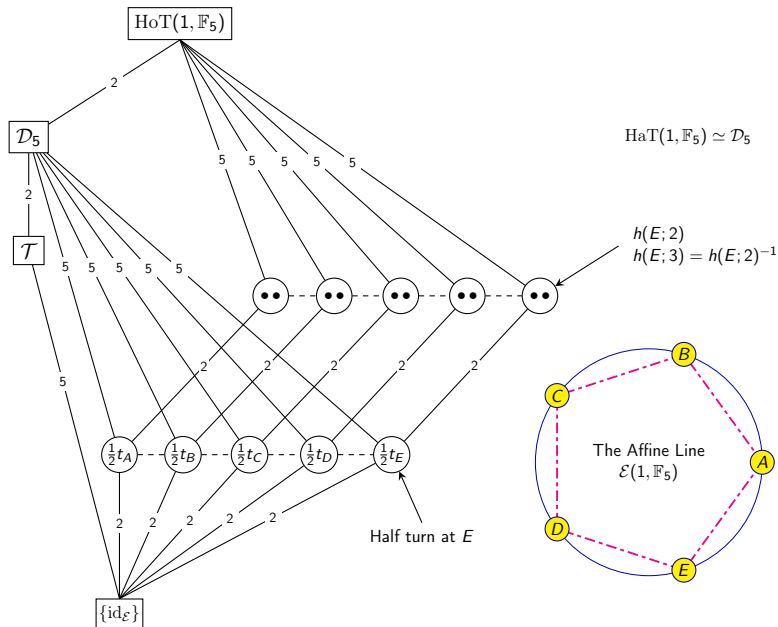


Graphe de Cayley de $C_3 \times C_3$



Cayley Graph of $\mathcal{H} = C_3^2 \rtimes_r C_2$,
associated to the re-
presentation (1), above

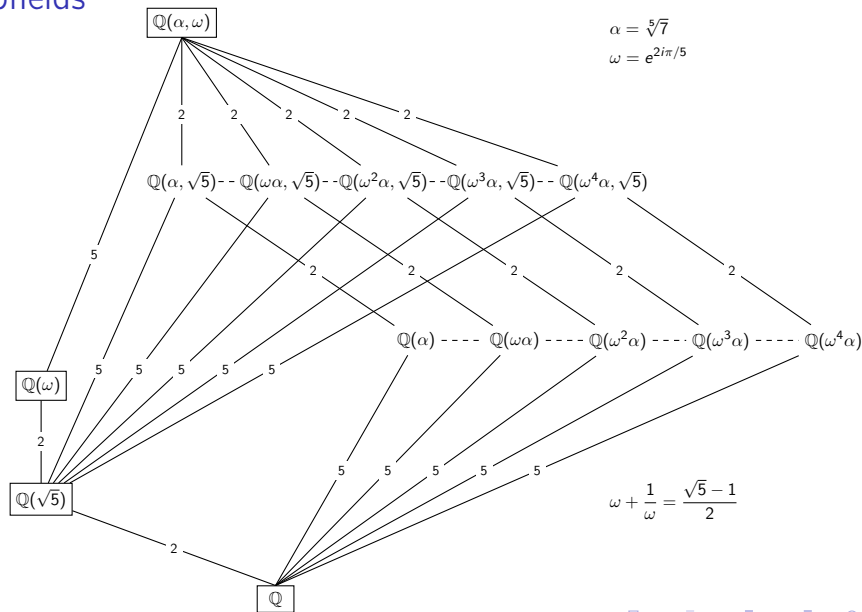
A Cherry on the Cake.– The Affine Line Group $\text{HoT}(1, \mathbb{F}_5)$



The Last Dessert.— The splitting field of $X^5 - 7$ and its subfields

$$\alpha = \sqrt[5]{7}$$

$$\omega = e^{2i\pi/5}$$



Bibliography.–

[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).

[Mn]– Conférence IREM (Oct. 2015) Rached Mneimné. *Un groupe d'ordre 18 peu connu*, bientôt sur le WEB.

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