MA542 Lecture

Timothy Kohl

Boston University

April 16, 2025

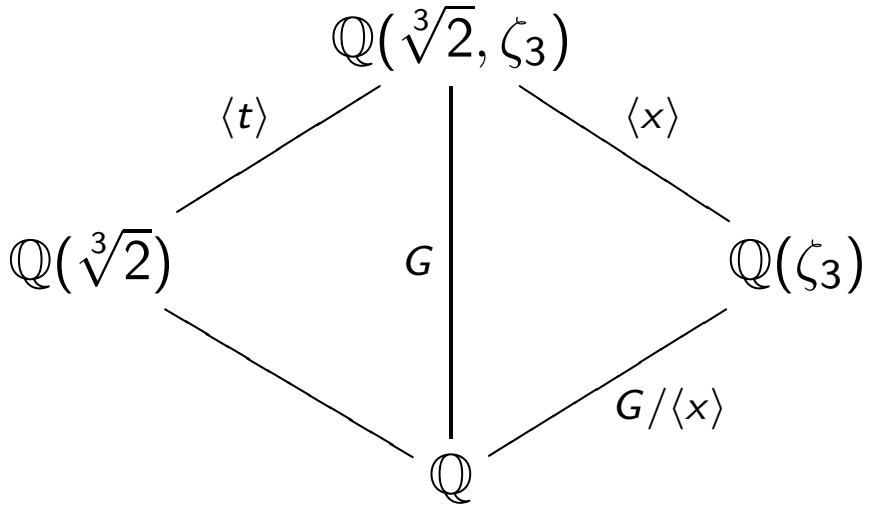
When $G = ND$ for $D \leq G$ and $N \triangleleft G$ we saw that

$$n_1 d_1 n_2 d_2 = n_1 d_1 n_2 d_1^{-1} d_1 d_2 = n_1 (d_1 n_2 d_1^{-1}) d_1 d_2$$

but $dNd^{-1} = N$ (which is a consequence of the normality of N in G) means that D is acting on N by 'inner automorphisms' (i.e. conjugation) which means that there is a homomorphism $f : D \to Aut(N)$ given by $f(d)(n) = dnd^{-1}$.

The upshot of this is that $ND \cong N \rtimes_f D$, namely the internal semi-direct product is isomorphic to the external semi-direct product.

So let's consider two examples we already know, and view them in the framework of Natural Irrationality, and (internal/external) semi-direct products.



where $\mathbb{Q}(\sqrt[3]{2},\zeta_3)$ is the compositum $\mathbb{Q}(\sqrt[3]{2})\mathbb{Q}(\zeta_3)$ and $Gal(\mathbb{Q}(\sqrt[3]{2},\zeta_3)/\mathbb{Q}(\sqrt[3]{2})) \cong Gal(\mathbb{Q}(\zeta_3)/\mathbb{Q})$.
Moreover, $G = \langle x, t \mid x^3 = 1, t^2 = 1, xt = tx^{-1}\rangle = \langle x\rangle\langle t\rangle$ as an internal semi-direct product.

Indeed $xt = tx^{-1}$ is equivalent to the conjugation fact: $txt^{-1} = x^{-1}$, namely how $\langle t\rangle$ acts on $\langle x\rangle$ by automorphisms, where indeed $x \mapsto x^{-1}$ is an automorphism of $\langle x\rangle$.

An identical analysis applies to the splitting field $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ for $x^4 - 2$ where

$$G = \langle x, t \mid x^3 = 1, t^2 = 1, xt = tx^{-1} \rangle = \langle x \rangle \langle t \rangle$$

again, an internal semi-direct product.

Note, both of these are examples where the Galois group is Dihedral, and indeed given the presentation

$$D_n = \langle x, t \mid x^n = 1, t^2 = 1, xt = tx^{-1} \rangle$$

we have that D_n is an internal semi-direct product, $\langle x \rangle \langle t \rangle$.

Moreover, this illustrates that D_n can be represented abstractly as a semi-direct product, namely

$$D_n \cong \mathbb{Z}_n \rtimes_f \mathbb{Z}_2$$

where $f : \mathbb{Z}_2 \to Aut(\mathbb{Z}_n) \cong U(n)$ is give by $f(i) = (-1)^i$, that is $f(i)(a) = (-1)^i a$.

For larger n, there are, of course, similarities in the analysis of the splitting fields and Galois groups of $x^n - a$, where a is not an n^{th} power in $\mathbb{Q}$.

We are not going to go through the *entire* development but we can outline not only the similarities, but also the important differences.

Consider $x^5 - 2 \in \mathbb{Q}[x]$, and realize, first of all, that there's nothing particulary special about '2' in $x^n - 2$ except for the fact that, since 2 is prime, $\sqrt[n]{2}$ is not in $\mathbb{Q}$.

The splitting field of $x^5 - 2$ is $\mathbb{Q}(\sqrt[5]{2}, \zeta_5)$ where ζ_5 is a primitive 5^{th} root of unity.

So in particular $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = \phi(5) = 4$ which is different than the two previous examples in that $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = \phi(3) = 2$ and (since we $\zeta_4 = i$) $[\mathbb{Q}(\zeta_4) : \mathbb{Q}] = \phi(4) = 2$ also.

And we have the basis for $\mathbb{Q}(\zeta_5)/\mathbb{Q}$ given by $\{1, \zeta_5, \zeta_5^2, \zeta_5^3\}$.

Also, the basis for $\mathbb{Q}(\sqrt[5]{2})/\mathbb{Q}$ is $\{1, \sqrt[5]{2}, \sqrt[5]{2}^2, \sqrt[5]{2}^3, \sqrt[5]{2}^4\}$ As such $[\mathbb{Q}(\sqrt[5]{2}, \zeta_5) : \mathbb{Q}] = 5 \cdot 4$ and the basis for $\mathbb{Q}(\sqrt[5]{2}, \zeta_5)/\mathbb{Q}$ is

$$\begin{aligned}
&\{1, \sqrt[5]{2}, \sqrt[5]{2}^2, \sqrt[5]{2}^3, \sqrt[5]{2}^4, \\
&\zeta_5, \zeta_5\sqrt[5]{2}, \zeta_5\sqrt[5]{2}^2, \zeta_5\sqrt[5]{2}^3, \zeta_5\sqrt[5]{2}^4, \\
&\zeta_5^2, \zeta_5^2\sqrt[5]{2}, \zeta_5^2\sqrt[5]{2}^2, \zeta_5^2\sqrt[5]{2}^3, \zeta_5^2\sqrt[5]{2}^4, \\
&\zeta_5^3, \zeta_5^3\sqrt[5]{2}, \zeta_5^3\sqrt[5]{2}^2, \zeta_5^3\sqrt[5]{2}^3, \zeta_5^3\sqrt[5]{2}^4\}
\end{aligned}$$

And so, the Galois group again must map roots to roots and so one must account for how it acts on $\sqrt[5]{2}$ and on ζ_5.

The Galois group of $\mathbb{Q}(\zeta_5)/\mathbb{Q}$ is determined by the fact that ζ_5 satsfies the equation

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1 = 0$$

which has roots $\zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4$ and where $\zeta_5^4 = -\zeta_5^3 - \zeta_5^2 - \zeta_5 - 1$.

It turns out (and we'll explore this in more detail later) that $Gal(\mathbb{Q}(\zeta_5)/\mathbb{Q}) = \langle t \rangle$ where $t(\zeta_5) = \zeta_5^3$, as then $t^2(\zeta_5) = \zeta_5^4$, $t^3(\zeta_5) = \zeta_5^2$ and $t^4 = I$.

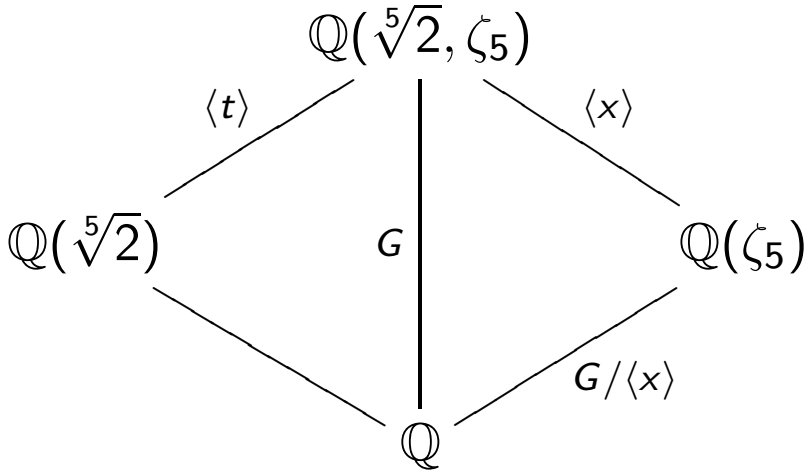
The other generator of the Galois group is x where $x(\sqrt[5]{2}) = \zeta_5\sqrt[5]{2}$ and, as you might expect, $|x| = 5$ and one can show that $txt^{-1} = x^3$, which, in a way, echoes how t acts on ζ_5 where $t(\zeta_5) = \zeta_5^3$.

This is not an accident.

So $G = Gal(\mathbb{Q}(\sqrt[5]{2}, \zeta_5)/\mathbb{Q})$ is given by the presentation

$$\langle x, t \mid x^5 = 1, t^4 = 1, txt^{-1} = x^3 \rangle$$

and indeed, t conjugating x to x^3 is an automorphism of $\langle x \rangle$ since $\langle x \rangle \triangleleft G$, so that G is the internal semi-direct product $\langle x \rangle \langle t \rangle \cong \mathbb{Z}_5 \rtimes_f \mathbb{Z}_4$.



Solvability By Radicals

Recall the quadratic formula for solving $ax^2 + bx + c = 0$.

$$x = \frac{-b \pm \sqrt{b^2 - 4c}}{2a} \in \mathbb{Q}(\sqrt{b^2 - 4ac})$$

and for cubic equations $ax^3 + bx^2 + cx + d = 0$ a bit of 'conditioning' is needed.

For $x^3 + bx^2 + cx + d$, we make the variable substitution $x = t - \frac{b}{3}$ one obtains the 'depressed cubic'

$$t^3 + pt + q$$

where $p = \frac{3c - b^2}{3}$, and $q = \frac{2b^3 - 9bc + 27d}{27}$.

The solutions of this equation are

$$A + B, \ \frac{-(A+B)}{2} + \frac{(A-B)\sqrt{-3}}{2}, \ \frac{-(A+B)}{2} - \frac{(A-B)\sqrt{-3}}{2}$$

where

$$A = \sqrt[3]{\frac{-q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

$$B = \sqrt[3]{\frac{-q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

There is also a 'quartic formula' for solving $ax^4 + bx^3 + cx^2 + dx + c = 0$ in terms of the coefficients $\{a, b, c, d, e, f\}$.

However, we will not give the formula here.

For degree 5 and beyond there are no known 'universal' formulae for the roots of the polynomial, expressed in terms of the coefficients by any combination of field operations (i.e. addition, multiplication etc.) and root extraction.

This doesn't mean that one cannot solve certain quintic polynomials, but there is no 'quintic formula'.

Definition

Let F be a field and let $f(x) \in F[x]$; we say that $f(x)$ is solvable by radicals over F if $f(x)$ splits in some extension $F(a_1, \ldots, a_n)/F$ where for positive integers $k_1, \ldots, k_n$ one has

$$\begin{aligned} a_1^{k_1} &\in F \\ a_2^{k_2} &\in F(a_1) \\ a_3^{k_3} &\in F(a_1, a_2) \\ &\vdots \\ a_n^{k_n} &\in F(a_1, a_2, \ldots, a_{n-1}) \end{aligned}$$

Such extensions are basically formed by repeated adjunction of roots of elements in each field in progressive fashion to form the next 'higher' field above F.

In parallel, we have the following definition for groups.

Definition

A group G is solvable if G has a series of subgroups

$$\{e\} = H_0 \leq H_1 \leq H_2 \leq \cdots \leq H_k = G$$

where for each $0 \leq i < k$, $H_i \triangleleft H_{i+1}$ and H_i/H_{i+1} is abelian.

One obvious class of examples are abelian groups since every subgroup of an abelian group is abelian, and all subgroups are normal, and certainly any quotient is abelian.

We note a few interesting facts about the class of solvable groups.

Proposition

Subgroups of solvable groups are solvable.

PROOF:
If $K \leq G$ where G is solvable then for the series

$$\{e\} = H_0 \leq H_1 \leq H_2 \leq \cdots \leq H_k = G$$

take the intersection of each of these with K to yield

$$\{e\} = H_0 \cap K \leq H_1 \cap K \leq H_2 \cap K \leq \cdots \leq H_k \cap K = G \cap K = K$$

and since $H_i \triangleleft H_{i+1}$ then $K \cap H_i \triangleleft K \cap H_{i+1}$. If $x + (H_i \cap K)$ and $y + (H_i \cap K)$ are in $(H_{i+1} \cap K)/(H_i \cap K)$ then $x + H_i, y + H_i$ are in H_{i+1}/H_i and so $xyx^{-1}y^{-1} = h \in H_i$. But since $x, y \in H_{i+1} \cap K$, (so in particular $x, y \in K$) then so is h and thus $xyx^{-1}y^{-1} \in H_i \cap K$.

Thus $(H_{i+1} \cap K)/(H_i \cap K)$ is abelian. □

Proposition

If G is solvable and $K \triangleleft G$ then G/K is solvable.

PROOF: Take a series $\{e\} = H_0 \leq H_1 \leq H_2 \leq \cdots \leq H_k = G$ for G and 'multiply' each term by K to yield

$$K = H_0K \leq H_1K \leq H_2K \leq \cdots \leq H_kK = GK$$

and since $H_i \triangleleft H_{i+1}$ it's easy to show $H_iK \triangleleft H_{i+1}K$, moreover $K \triangleleft H_iK$ for each H_i and so we can form the quotients H_iK/K, all of which are subgroups of G/K.

PROOF: (continued)

That is, we have a series

$$K/K = H_0K/K \leq H_1K/K \leq H_2K/K \leq \cdots \leq H_kK/K = GK/K = G/K$$

and the last detail is to show that $H_iK/H_{i+1}K$ is abelian, which is a straightforward, but somewhat messy calculation which we shall leave as an exercise.

(The basic point to use is that H_i/H_{i+1} is abelian and see where that leads.) $\square$.

So we've shown that the class of solvable groups is closed under the operation of taking subgroups, and forming quotients.

It's not to difficult to show the following:

Proposition

If G_1 and G_2 are solvable, so is $G_1 \times G_2$.

the proof of which is a nice exercise.

The other rather nice property, which touches on the results we just showed about how solvability is 'inherited' by subgroups and quotients, is this:

Theorem

For a group G with normal subgroup K, if any two of G, K, or G/K are solvable, so is the other.

We won't go through the proof here, but it is not excessively difficult.