MA542 Lecture

Timothy Kohl

Boston University

April 14, 2025

For $x^3 - 2$ and $x^4 - 2$ in $\mathbb{Q}[x]$ we got that the Galois groups were

$$\langle x, t \mid x^3 = 1, t^2 = 1, xt = tx^{-1} \rangle \cong D_3$$
$$\langle x, t \mid x^4 = 1, t^2 = 1, xt = tx^{-1} \rangle \cong D_4$$

but what about $x^n - 2$ for *larger* n, say $n = 5$?

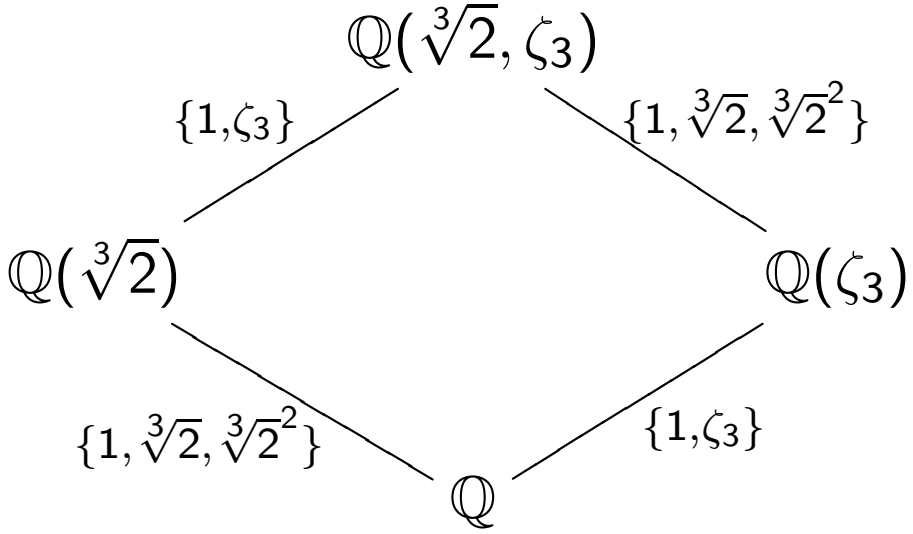
Before we look at the splitting field for $x^5 - 2$ we should take a closer look at something we have been using without really justifying it.

For example, with $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ we have have used the fact that the basis of $\mathbb{Q}(\zeta_3)/\mathbb{Q}$ is $\{1, \zeta_3\}$ and that the basis of $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is $\{1, \sqrt[3]{2}, \sqrt[3]{2}^2\}$, to infer that the basis of $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$ is the 'product' of these two bases

$$\{1, \zeta_3\} \cdot \{1, \sqrt[3]{2}, \sqrt[3]{2}^2\} = \{1, \sqrt[3]{2}, \sqrt[3]{2}^2, \zeta_3, \zeta_3\sqrt[3]{2}, \zeta_3\sqrt[3]{2}^2\}$$

The reason we can do this has to do, primarily, with the fact that $\mathbb{Q}(\zeta_3) \cap \mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}$.

This implies that $\{1, \sqrt[3]{2}, \sqrt[3]{2}^2\}$ is a basis of $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}(\zeta_3)$, and symmetrically $\{1, \zeta_3\}$ is a basis of $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}(\sqrt[3]{2})$ which we can diagram:



And even more interestingly, this kind of 'parallelism' has a bearing on the relationships between the different Galois groups, which we shall explore soon.

Another view we can take of $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ is as what we call the 'compositum' namely $\mathbb{Q}(\sqrt[3]{2})\mathbb{Q}(\zeta_3)$ which is the subfield of $\mathbb{C}$ consisting of all products of elements from both fields.

Note, one must **not** confuse this with the direct product of the two fields, which would **not** be a field.

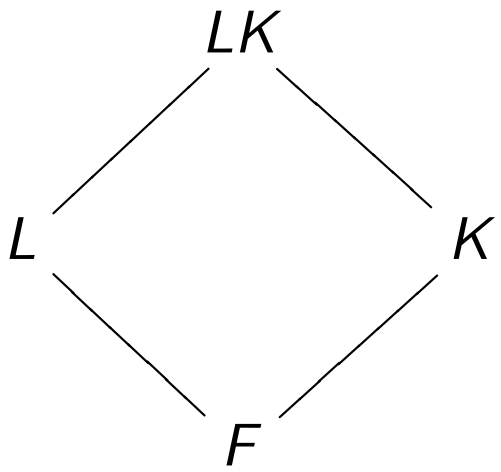
In fact, product is not necessarily the best way to think of this, rather we should view $\mathbb{Q}(\sqrt[3]{2})\mathbb{Q}(\zeta_3)$ as the smallest subfield of $\mathbb{C}$ that contains *both* $\mathbb{Q}(\sqrt[3]{2})$ and $\mathbb{Q}(\zeta_3)$.

In general, if K and L are fields (both of which are containd in some larger field, e.g. $\mathbb{C}$) then the compositum LK is the smallest subfield of this larger field which contains both L and K.

If we let $F = L \cap K$ and if K and L are finite extensions of F, then a basis of L/F and one of K/F can be multiplied to yield a basis of the compositum LK over F.

In a way, this derives from how we proved that $[E : K][K : F] = [E : F]$ for fields $F \subseteq K \subseteq E$.

The importance of the intersection $F = L \cap K$ is that for such a situation:



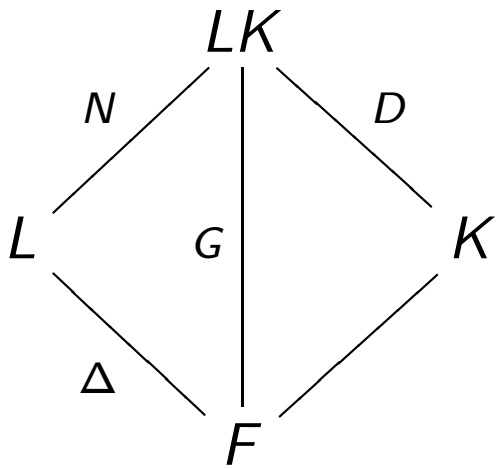
we have that $[LK : F] = [L : F][K : F] = [LK : K][K : F]$ since $F = L \cap K$.

This is what we term 'linear disjointness' in that no basis element of L/F can be written in terms of the basis of K/F and vice versa.

Linear disjointness has some implications when one considers the Galois group of a compositum of two fields.

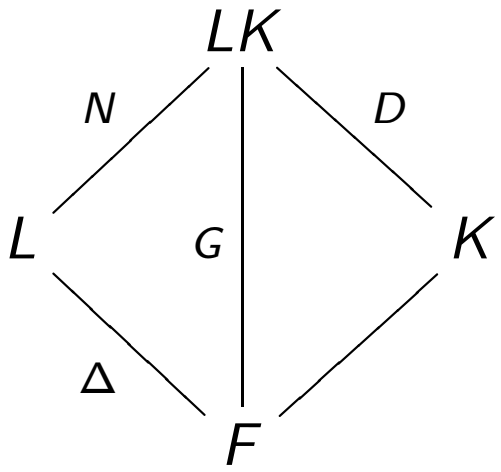
So suppose L/F and K/F are algebraic extensions of F where $L \cap K = F$, and suppose that say LK/F and L/F are Galois, (and LK/K is Galois automatically) but K/F was not.

Suppose also that $G = Gal(LK/F)$, $N = Gal(LK/L)$, $D = Gal(LK/K)$, $\Delta = Gal(L/F)$.



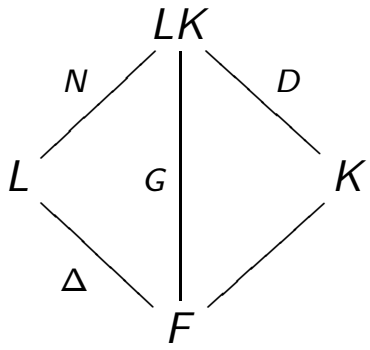
and as L/F is Galois, then this implies that $N \triangleleft G$.

With this setup



we have that $D \cong \Delta$ which is what is called Natural Irrationality which is a result due to LaGrange.

The argument one makes to show this is that the action of D on LK fixes K so that if one restricts D to the elements of L inside LK then one gets an action of D on L by automorphisms, and this action is identical with that of Δ.



Another way to think of the action of D on LK/K as being 'equivalent' to the action of Δ on L/F is as follows.

If we have a basis $\{\beta_1, \beta_2, \ldots, \beta_m\}$ for L, viewed as an F-vector space, then every element of L is a linear combination $a_1\beta_1 + \cdots + a_m\beta_m$ for $a_1, \ldots, a_m \in F$.

However, if we take all K-linear combinations (i.e. the K-span of $\{\beta_1, \ldots, \beta_m\}$) then this is then going to give us a field extension of K and this field extension has degree m, but it is a field extension contained in LK but since $[LK : K] = m$ then this must actually *equal* LK, which means LK is the span of the basis $\{\beta_1, \ldots, \beta_m\}$.

What this also means is that, again, since the elements of D act on LK and fix K then they must be acting on the basis elements $\{\beta_i\}$ but this action agrees with the action of Δ on the $\{\beta_i\}$.

Or, one could start with Δ acting on L and fixing F and extend this action to LK which we assume acts trivially on K, i.e. giving us the elements of D.

We note that N and D are subgroups of G, whereas Δ is isomorphic to the quotient and is therefore not necessarily a subgroup of G itself.

Also, since $L \cap K = F$ then $N \cap D = \{1\}$.

Furthermore, as $N \triangleleft G$ and $D \leq G$ then $ND = \{nd \,|n \in N, d \in D\}$ is a subgroup of G. Why?

If $N \triangleleft G$ and $D \leq G$ then ND is a group since, first of all $1 \in ND$ since $1 \in N$ and $1 \in D$ so $1 = 1 \cdot 1 \in ND$

Next, if $n_1 d_1, n_2 d_2 \in ND$ then is $n_1 d_1 n_2 d_2 \in ND$?

Well, note that $d_1 n_2 \in d_1 N$ (the left coset) and by normality $d_1 N = N d_1$ so therefore $d_1 n_2 = n_3 d_1$ for some $n_3 \in N$, so

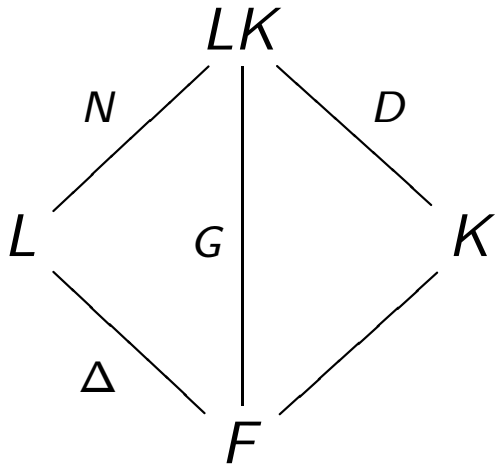
$$n_1 d_1 n_2 d_2 = n_1 (d_1 n_2) d_2 = n_1 n_3 d_1 d_2 \in ND$$

so we have closure.

Moreover $(nd)^{-1} = d^{-1} n^{-1} \in d^{-1} N$ and since $d^{-1} N = N d^{-1}$ then $d^{-1} n^{-1} = n'^{-1} d_1^{-1} \in ND$ so ND is closed under inverses and therefore a group.

We call this the 'internal semi-direct product' of N and D.

So now, with



with $L \cap K = F$ then, as we mentioned above, $N \cap D = \{1\}$ and so

$$|ND| = \frac{|N| \cdot |D|}{|N \cap D|} = |N| \cdot |D|$$

where now, $[LK : K] = |D|$, $[LK : L] = |N|$ and $|G| = [LK : F] = [L : F][K : F] = [LK : K][LK : L] = |N| \cdot |D|$ which means

$$G = ND$$

namely G is the internal semi-direct product of N and D.

However, we should emphatically point out that it's not necessarily the case that $ND \cong N \times D$.

Since $G = ND$, where $N \triangleleft G$ then this means that $gNg^{-1} = N$ for all $g \in G$.

As such when multiplying $(n_1 d_1)(n_2 d_2)$ we can write

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

where now, since $N \triangleleft G$ then $d_1 n_2 d_1^{-1} \in N$ so the product is in ND again.

The product in ND being induced by the 'action' of D on N is an example of a group automorphism.

Definition

For a group G, a bijective homomorphism $\alpha : G \to G$ is called an automorphism of G.

And, like a Galois group, the composition of group automorphisms is a group automorphism so we have:

Definition

For a group G, the set of all automorphisms of G is itself a group, and is denoted $Aut(G)$.

For example, if $G = \mathbb{Z}_n$ then $Aut(G) = U(n)$ since if $\psi : \mathbb{Z}_n \to \mathbb{Z}_n$ is an automorphism then it must be one-to-one, and since 1 generates $\mathbb{Z}_n$ then ψ is determined by $\psi(1)$, since then $\psi(k) = \psi(k \cdot 1) = k\psi(1)$.

If now $\psi(1) = r$ then we must have $|r| = |1| = n$ which means $r \in U(n)$, i.e. $gcd(r, n) = 1$.

If we denote by ψ_r the automorphism for which $\psi_r(1) = r$ then $\psi_{r_1}(\psi_{r_2}(1)) = \psi_{r_1}(r_2) = r_1 \cdot r_2$, thus $Aut(\mathbb{Z}_n) \cong U(n)$ where

$$U(n) \ni r \mapsto \psi_r \in Aut(\mathbb{Z}_n)$$

.

Automorphisms can be used to define a way of combining groups to get new groups.

Definition

If N and D are groups, and $f : D \to Aut(N)$ is a homomorphism, then the (external) semi-direct product $N \rtimes_f D$ is a group, where the elements consist of ordered pairs (n, d) (i.e. $N \times D$) but where the multiplication is defined as follows:

$$(n_1, d_1) * (n_2, d_2) = (n_1 f(d_1)(n_2), d_1 d_2)$$

where the identity is (e_N, e_D) and $(n, d)^{-1} = (f(d^{-1})(n^{-1}), d^{-1})$

One can check (Exercise!) that $N \rtimes_f D$ is associative.

And we note that although $N \rtimes_f D$ is, as a set, the direct product, the group structure is more complicated.

However, if $f : D \to Aut(N)$ is trivial, namely $f(d) = I_N$ for all $d \in D$ then

$$(n_1, d_1) * (n_2, d_2) = (n_1 f(d_1)(n_2), d_1 d_2) = (n_1 n_2, d_1 d_2)$$

so that the group structure *is* that of the direct product, so the direct product is just a special case of semi-direct product.

So what does this have to do with Galois groups, and our example where $G = ND$?