MA542 Lecture

Timothy Kohl

Boston University

April 28, 2025

Non-cyclic abelian groups?

For non-cyclic abelian groups, it's a bit more subtle a problem.

For example, suppose we want to find a Galois extension with group G that is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_3$?

Consider $\mathbb{Q}(\zeta_{49})$ and $\mathbb{Q}(\zeta_9)$ where

$$Gal(\mathbb{Q}(\zeta_{49})/\mathbb{Q}) \cong \mathbb{Z}_{\phi(49)} = \mathbb{Z}_{42} \cong \mathbb{Z}_7 \times \mathbb{Z}_6 \cong \mathbb{Z}_7 \times \mathbb{Z}_3 \times \mathbb{Z}_2$$
$$Gal(\mathbb{Q}(\zeta_9)/\mathbb{Q}) \cong \mathbb{Z}_{\phi(9)} = \mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$$

so, for $9 \cdot 49 = 441$ we have

$$Gal(\mathbb{Q}(\zeta_{441})/\mathbb{Q}) \cong \mathbb{Z}_{\phi(441)} \cong \mathbb{Z}_7 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$$

So $Gal(\mathbb{Q}(\zeta_{441})/\mathbb{Q}) \cong (\mathbb{Z}_7 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \times (\mathbb{Z}_3 \times \mathbb{Z}_3)$ which means we can find a subgroup $H \cong \mathbb{Z}_7 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, which yields a factor group

$$\begin{aligned} G/H &\cong (\mathbb{Z}_7 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \times (\mathbb{Z}_3 \times \mathbb{Z}_3)/(\mathbb{Z}_7 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \\ &\cong \mathbb{Z}_3 \times \mathbb{Z}_3 \end{aligned}$$

and this quotient is the Galois group of $\mathbb{Q}(\zeta_{441})_H/\mathbb{Q}$.

So indeed, we can (with some work) find Galois extensions of $\mathbb{Q}$ with abelian Galois groups of any type we wish, all given as subfields of cyclotomic extensions.

non-abelian Galois Groups

For non-abelian Galois groups, we look at a slightly different setup.

Theorem

For every n there exists a field extension L/K such that $Gal(L/K) \cong S_n$.

And as a consequence we have:

Corollary

For any finite group G, there exists a field extension E/K such that $Gal(L/E) \cong G$.

Before looking at the proof of the theorem, let's examine why the corollary is true.

It has to do with a very general result about groups and their permutations.

Definition

For a finite set X, let $Perm(X)$ be the set of all permutations of X, also sometimes denoted $Sym(X)$ or S_X.

The most familiar example of this is for $X = \{1, 2, \ldots, n\}$ where $Perm(X) = S_n$, the n^{th} symmetric group.

For a given group G, we can view the underlying set of elements of G as a set which can be permuted like any other set.

This gives rise to the following important idea.

Definition

For G a finite group, the left regular representation is the function $\lambda : G \to Perm(G)$ defined by $\lambda(g)(h) = gh$ for each $h \in G$.

The reason $\lambda : G \to Perm(G)$ makes sense is that for each $g \in G$ and elements $h_1, h_2 \in G$ we have that $gh_1 = gh_2$ if and only if $h_1 = h_2$.

This means that if $G = \{h_1, h_2, \ldots, h_n\}$ then for $g \in G$ we get a re-arrangement, i.e. permutation in that $gh \in G$ for each $h \in G$ so $G = \{gh_1, gh_2, \ldots, gh_n\}$ where, by the above observation, $gh_i = gh_j$ implies $h_i = h_j$.

To give an example of how this works, suppose we have $G = \mathbb{Z}_3 = \{0, 1, 2\}$ where now, since G is 'additive', we have $\lambda(g)(h) = g + h$.

So now, consider $\lambda(1)$ where $\lambda(1)(0) = 1 + 0 = 1$, $\lambda(1)(1) = 1 + 1 = 2$ and $\lambda(1)(2) = 1 + 2 = 0$ which means we can write $\lambda(1)$ in cycle notation as

$$\lambda(1) = (0, 1, 2)$$

and similarly $\lambda(2) = (0, 2, 1)$ and $\lambda(0) = ()$

Recall that the trivial permutation is written in cycle notation as '()'.

A different example is for
$G = D_3 = \langle x, t \mid x^3 = 1, t^2 = 1, xt = tx^{-1} \rangle = \{1, x, x^2, t, tx, tx^2\}$ and here we can compute $\lambda(x)$ where now

$$\begin{aligned}
\lambda(x)(1) &= x \cdot 1 = x \\
\lambda(x)(x) &= x \cdot x = x^2 \\
\lambda(x)(x^2) &= x \cdot x^2 = 1 \\
\lambda(x)(t) &= x \cdot t = tx^2 \\
\lambda(x)(tx) &= x \cdot tx = t \\
\lambda(x)(tx^2) &= x \cdot tx^2 = tx
\end{aligned}$$

which can be represented in cycle notation as $(1, x, x^2)(t, tx^2, tx)$.

There are two key observations about $\lambda : G \rightarrow Perm(G)$.

First, λ is a group homomorphism since
$\lambda(g_1 g_2)(h) = g_1 g_2 h = g_1(g_2 h) = \lambda(g_1)(\lambda(g_2)(h)) = (\lambda(g_1) \circ \lambda(g_2))(h)$.

Second, λ is one-to-one. If we compute $ker(\lambda)$ we find that $\lambda(g)(h) = h$ for all $h \in G$ implies that $gh = h$ which implies that $g = e$, that is $\lambda(g)$ is the identity permutation, only if $g = e$, so $ker(\lambda) = \{e\}$.

We also observe that if $|G| = n$ then, clearly
$Perm(G) \cong Perm(\{1, 2, \ldots, n\}) = S_n$.

This observation, together with the fact that λ is 1-1 yields the following theorem.

Theorem (Cayley)

If $|G| = n$ then there exists a subgroup of S_n isomorphic to G.

As $\lambda : G \to Perm(G) \cong S_n$ is one-to-one then $\lambda(G)$ is a subgroup of $Perm(G)$ that is isomorphic to G.

So what this implies is that S_n in some sense contains 'every group of order n' in that a group with n elements can be embedded in its group of permutations, and this group of permutations (of a set with n elements) is isomorphic to S_n.

We shall see subsequently how to apply this to infer that every finite group G is a Galois group, but a bit more foundation is needed.

non-abelian Galois Groups

We aim to cover the following two facts.

Theorem

For every n there exists a field extension L/K such that $Gal(L/K) \cong S_n$.

Corollary

For any finite group G, there exists a field extension E/K such that $Gal(L/E) \cong G$.

The one caveat is that K is not $\mathbb{Q}$, and indeed the fields we will be dealing with are *not* number fields, like $\mathbb{Q}$ etc., that we've been examining up till now.

Definition

For $n \geq 1$ let $\mathbb{Q}(x_1, \ldots, x_n) = Frac(\mathbb{Q}[x_1, \ldots, x_n])$ which is the field of rational functions in n variables with coefficients in $\mathbb{Q}$.

Consider now the <u>elementary symmetric functions</u> $\{f_1, \ldots, f_n\}$

$$f_1 = \sum_{i=1}^{n} x_i = x_1 + x_2 + \cdots + x_n$$

$$f_2 = \sum_{1 \leq i < j \leq n} x_i x_j = x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n$$

$$f_3 = \sum_{1 \leq i < j < k \leq n} x_i x_j x_k = x_1x_2x_3 + \cdots + \cdots + x_{n-2}x_{n-1}x_n$$

$$\vdots$$

$$f_n = x_1 x_2 \cdots x_n$$

For example, with $n = 4$ we have

$$\begin{aligned}
f_1 &= x_1 + x_2 + x_3 + x_4 \\
f_2 &= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 \\
f_3 &= x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 \\
f_4 &= x_1x_2x_3x_4
\end{aligned}$$

and to give a sense of the number of terms, for any n and any $r \leq n$ the symmetric function f_r has $\binom{n}{r}$ terms since one is adding up all possible expressions in r of the n variables.

Symmetric 'expressions' arise quite naturally when looking at the factorization of 'ordinary' polynomials as products of linear terms.

For example, if $g(x) = (x - \alpha)(x - \beta)$ then $g(x) = x^2 - (\alpha + \beta)x + \alpha\beta$, namely $g(x) = x^2 - f_1(\alpha, \beta)x + f_2(\alpha, \beta)$.

If $g(x) = (x - \alpha)(x - \beta)(x - \gamma)$ then

$$\begin{aligned} g(x) &= x^3 - (\alpha + \beta + \gamma)x^2 + (\alpha\beta + \alpha\gamma + \beta\gamma)x - (\alpha\beta\gamma) \\ &= x^3 - f_1(\alpha, \beta, \gamma)x^2 + f_2(\alpha, \beta, \gamma)x - f_3(\alpha, \beta, \gamma) \end{aligned}$$

and this pattern holds in general.

Namely, if we define $f_0(x_1, \ldots, x_n) = 1$ then for monic $g(x)$ with roots $\alpha_1, \alpha_2, \ldots, \alpha_n$ we have

$$g(x) = \sum_{k=0}^{n} (-1)^k f_k(\alpha_1, \ldots, \alpha_n) x^{n-k}$$

and indeed, the 'symmetry' of these functions (in general) corresponds to the 'symmetry' that arises when these roots are permuted by the action of a Galois group. (More on this later.)

The reason the f_r are called symmetric is that, if $f(x_1, x_2, \ldots, x_n) \in \mathbb{Q}(x_1, \ldots, x_n)$ then $\sigma \in S_n$ acts on this function by shuffling variables, namely $\sigma(f(x_1, \ldots, x_n)) = f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$.

For example, if $f(x_1, x_2, x_3) = x_1 + x_2x_3^2 + x_2^2$ and $\sigma = (1, 2, 3)$ then $\sigma(f(x_1, x_2, x_3)) = x_2 + x_3x_1^2 + x_3^2$.

So what we have is that $\sigma \in S_n$ induces an automorphism of $\mathbb{Q}(x_1, \ldots, x_n)$ since one can verify that $\sigma(f + g) = \sigma(f) + \sigma(g)$ and $\sigma(fg) = \sigma(f)\sigma(g)$, and clearly σ acts in a 1-1 fashion and every element of $\mathbb{Q}(x_1, \ldots, x_n)$ is $\sigma(f)$ for some other $f \in \mathbb{Q}(x_1, \ldots, x_n)$. (Exercise!)

So what makes the f_r we defined earlier 'symmetric'?

So we have that each $\sigma \in S_n$ acts as an automorphism of $\mathbb{Q}(x_1, \ldots, x_n)$ which begs the question as to what is $\mathbb{Q}(x_1, \ldots, x_n)_{S_n}$?

Proposition

For a given $n \geq 1$ with associated elementary symmetric functions $f_1, \ldots, f_n$ we have $\mathbb{Q}(x_1, \ldots, x_n)_{S_n} = \mathbb{Q}(f_1, \ldots, f_n)$, namely the field generated adjoining $\{f_1, \ldots, f_n\}$ to $\mathbb{Q}$ (which includes all sums, differences, products, and quotients of the f_i).

For a basic example, consider $\sigma = (1, 2, 3) \in S_3$ and $f_1 = x_1 + x_2 + x_3$ then $\sigma(f_1) = x_{\sigma(1)} + x_{\sigma(2)} + x_{\sigma(3)} = x_2 + x_3 + x_1 = x_1 + x_2 + x_3 = f_1$.

Similarly, f_1, f_2, f_3 are all unchanged if acted on by any $\sigma \in S_3$ since a rearrangement of the variables gives an expression which is a re-arrangement of the original function, but which equals the original function.

So if $K = \mathbb{Q}(f_1, \ldots, f_n)$ and $L = \mathbb{Q}(x_1, \ldots, x_n)$ then L/K is Galois with $Gal(L/K) = S_n$.

The reason L is Galois over K is that K is exactly the fixed field of S_n and that $[L : K] = n! = |S_n|$.

Example: $n = 2$, $f_1 = x_1 + x_2$ and $f_2 = x_1 x_2$ and observe that $\mathbb{Q}(f_1, f_2)$ does not contain 'x_1' and 'x_2' as independent elements.

However, if we adjoin x_1 to $\mathbb{Q}(f_1, f_2)$ then we note that $f_2 \cdot 1 + (-1) \cdot x_1 = x_2$ so that $\mathbb{Q}(f_1, f_2)(x_1)$ contains x_2 so it equals $\mathbb{Q}(x_1, x_2)$ which means $\mathbb{Q}(x_1, x_2)$ is a $\mathbb{Q}(f_1, f_2)$ vector space with basis $\{1, x_1\}$, so it has dimension $2 = 2!$, i.e. $[\mathbb{Q}(x_1, x_2) : \mathbb{Q}(f_1, f_2)] = 2! = |S_2|$.

In general, we can exhibit a basis of $\mathbb{Q}(x_1,\ldots,x_n)$ over $\mathbb{Q}(f_1,\ldots,f_n)$, specifically

$$\mathcal{B} = \{x_1^{e_1}x_2^{e_2}\cdots x_n^{e_n} \mid 0 \leq e_t < t\}$$

which means $e_1 = 0$, $e_2 = 0,1$, $e_3 = 0,1,2$ etc. yielding the fact that $|\mathcal{B}| = n!$.

Example:

$n = 2 \rightarrow \mathcal{B} = \{x_1^0x_2^0, x_1^0x_2^1\} = \{1, x_2\}$

$n = 3 \rightarrow \mathcal{B} = \{1, x_2, x_2x_3, x_2x_3^2, x_3, x_3^2\}$.

So now that we've established the existence of a Galois extension E/F with $Gal(E/F) \cong S_n$ we can use Cayley's theorem.

Specifically, if G is a group of order n, then G embeds as a subgroup of S_n, which means that, there exists a subgroup $H \leq Gal(E/F) \cong S_n$ such that $H \cong G$.

This means that $Gal(E/E_H) = H \cong G$ and we're done.

So what about finding a Galois extension E/F where say $F \supseteq \mathbb{Q}$ with $Gal(E/F) \cong G$?

There are various results which imply, for example that there *do* exist Galois extensions $E/\mathbb{Q}$ where the Galois group $Gal(E/\mathbb{Q}) \cong S_n$ for every $n \geq 2$.

What this implies therefore is that for any group G, there is an intermediate field $\mathbb{Q} \subseteq K \subseteq E$ such that $Gal(E/K) \cong G$, but whether there exists a Galois extension of $\mathbb{Q}$ with an arbitrary Galois group G is still an open question.

The strongest result that is known is that every solvable group is 'realizable' over $\mathbb{Q}$ as a Galois group.

It's known also that many simple groups (those with no normal subgroups) are realizable as Galois groups over $\mathbb{Q}$, for example A_n for $n \geq 5$ as well as others.