MA542 Lecture

Timothy Kohl

Boston University

April 25, 2025

Now if $E/\mathbb{Q}$ is a splitting field of $\Phi_n(x)$ then E must contain ζ a primitive n^{th} root of unity, where without loss of generality, $\zeta = \zeta_n = e^{\frac{2\pi i}{n}}$ and so it's clear that $E = \mathbb{Q}(\zeta)$.

Recall that all the roots of $\Phi_n(x)$ are of the form ζ^k where $k \in U(n)$.

Moreover, observe that if $C = \langle \zeta \rangle$ then C is cyclic of order n, and its generators are precisely these primitive n^{th} roots ζ^k for $k \in U(n)$.

And so, if we consider $Aut(C)$ then $\psi_i \in Aut(C)$ if and only if $\psi_i(\zeta) = \zeta^{k_i}$ for some $k_i \in U(n)$ and that
$\psi_i(\psi_j(\zeta)) = (\zeta^{k_j})^{k_i} = \zeta^{k_j k_i} = \zeta^{k_i k_j} = \psi_j(\psi_i(\zeta))$.

That is $Aut(C) \cong U(n)$ and, moreover, if $\sigma \in Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ then $\sigma(\zeta) = \zeta^k$ for some $k \in U(n)$.

ergo $Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong U(n) \cong Aut(C) = Aut(\langle\zeta\rangle)$.

We note also that, as $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is abelian, it is solvable, so therefore all the roots of unity, principally ζ_n itself is expressible as combinations of radicals of different types.

What is also interesting is that this implies that the values of the trigonometric functions $cos(\frac{2\pi}{n})$ and $sin(\frac{2\pi}{n})$ are algebraic numbers.

Another, somewhat random, but interesting related fact is that for any prime p, one has

$$\mathbb{Q}(\zeta_p) \supseteq \mathbb{Q}(\sqrt{p}) \text{ if } p \equiv 1(\mod 4)$$
$$\mathbb{Q}(\zeta_p) \supseteq \mathbb{Q}(\sqrt{-p}) \text{ if } p \equiv 3(\mod 4)$$

The study of cyclotomic fields also touches on some deeper ideas, in particular those relating to 'what kind of groups arise as Galois groups'?

For cyclotomic fields, we have just established that $Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong U(n)$ is abelian, so let's explore the nature of these groups.

Later on we will consider questions of what types of extensions have abelian Galois groups in general.

As we saw earlier, $U(p) = \mathbb{Z}_p - \{0\}$ is actually a cyclic group of order $\phi(p) = p - 1$, and what's kind of interesting (in and of itself) is the question of what is the so-called 'least primitive root', that is, the least $r \in U(p)$ such that $U(p) = \langle r \rangle$.

We can give a small table which shows an interesting pattern:

p	r
2	1
3	2
5	2
7	3
11	2
13	2
17	3
19	2
23	5
29	2
31	3
37	2

It seems that '2' is frequently the least primitive root, but it is not known if it ever 'stops' being the least primitive root after some point.

Indeed, looking further, there are many primes for which 2 is the least primitive root:

$3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83, 101, 107, 131, 139, 149, 163, 173, 179,$
$181, 197, 211, 227, 269, 293, 317, 347, 349, 373, 379, 389, 419, 421, 443, 461,$
$467, 491, 509, 523, 541, 547, 557, 563, 587, 613, 619, 653, 659, 661, 677, 701, 709$

Does this sequence (A001122 on http://oeis.org) stop? Who knows?

The case of $U(p)$ begs the question of whether $U(n)$ is cyclic in general? i.e. Is $U(n) \cong \mathbb{Z}_{\phi(n)}$?

The answer is no, but we can give some specific facts about the structure of $U(n)$.

FACTS:

- $U(n)$ is cyclic if $n = 1, 2, 4, p^k, 2p^k$ for p an odd prime.
- $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$. (Exercise)
- $\phi(ab) = \phi(a)\phi(b)$ if $gcd(a, b) = 1$
- $U(8) = \{1, 3, 5, 7\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$
- $U(16) = \{1, 3, 5, 7, 9, 11, 13, 15\} \cong \mathbb{Z}_4 \times \mathbb{Z}_2$
- $U(2^k) \cong \mathbb{Z}_{2^{k-2}} \times \mathbb{Z}_2$ for $k \geq 3$

And to joint these facts together we have a fundamental fact:

Proposition

$U(ab) \cong U(a) \times U(b)$ *if* $gcd(a, b) = 1$.

The demonstration of this follows very closely to how one proves that $\mathbb{Z}_{ab} \cong \mathbb{Z}_a \times \mathbb{Z}_b$ if $gcd(a, b) = 1$.

As such, we can compute $U(n)$ for $n = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$ by determining $U(p_i^{e_i})$ using the above facts we enumerated.

For example:

$$U(15) = U(3 \cdot 5) = U(3) \times U(5) \cong \mathbb{Z}_2 \times \mathbb{Z}_4$$
$$U(20) = U(4 \cdot 5) = U(4) \times U(5) \cong \mathbb{Z}_2 \times \mathbb{Z}_4$$
$$U(60) = U(4 \cdot 3 \cdot 5) = U(4) \times U(3) \times U(5) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$$

Which groups can appear as Galois groups?

Our study of cyclotomic extensions is a nice lead in to this question.

We begin by quoting the following fairly deep fact known as the Kronecker-Weber Theorem

Theorem

If $E/\mathbb{Q}$ is a Galois where $Gal(E/\mathbb{Q})$ is abelian, then there exists and $n \geq 1$ such that $E \subseteq \mathbb{Q}(\zeta_n)$.

Now we are not going to attempt to prove this, but we can give a parallel analysis which deals with the determination of field extensions of $\mathbb{Q}$ have a cyclic Galois group.

Theorem

For every n, there exists a field extension $E/\mathbb{Q}$ such that $Gal(E/\mathbb{Q}) \cong \mathbb{Z}_n$.

To begin the proof of this result, we first quote another fairly deep theorem, this one from number theory, about primes in 'arithmetic progression'.

Theorem (Dirichlet)

Given a, d integers which are relatively prime, then the sequence $a, a+d, a+2d, \ldots$ contains infinitely many primes.

And for our purposes, one prime in this sequence is enough, and we see that any such prime is congruent to 'a' mod d.

So given our 'n', certainly $gcd(1, n) = 1$ so consider the sequence $1, 1 + n, 1 + 2n, 1 + 3n, \ldots$ which by Dirichlet's theorem contains a prime p with property that $p \equiv 1(mod\ n)$.

Consider now $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ where $Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = \langle\sigma\rangle \cong \mathbb{Z}_{p-1}$ and let $E = \mathbb{Q}(\zeta_p)_{\langle\sigma^n\rangle}$.

We have that $|\langle\sigma^n\rangle| = \frac{p-1}{n}$ which is an integer since $p \equiv 1(mod\ n)$.

Moreover, by FTGT, $[\mathbb{Q}(\zeta_p) : \mathbb{Q}(\zeta_p)_{\langle\sigma^n\rangle}] = |\langle\sigma^n\rangle| = \frac{p-1}{n}$ and thus $[\mathbb{Q}(\zeta_p)_{\langle\sigma^n\rangle} : \mathbb{Q}] = n$ since

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}(\zeta_p)_{\langle\sigma^n\rangle}][\mathbb{Q}(\zeta_p)_{\langle\sigma^n\rangle} : \mathbb{Q}] = [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$$

and since $\langle\sigma^n\rangle \triangleleft \langle\sigma\rangle$ then $\mathbb{Q}(\zeta_p)_{\langle\sigma^n\rangle}/\mathbb{Q}$ is Galois with group $\langle\sigma\rangle/\langle\sigma^n\rangle \cong \mathbb{Z}_{p-1}/\mathbb{Z}_{\frac{p-1}{n}} \cong \mathbb{Z}_n$. □

For example, say $n = 3$ then $p = 7$ works since $7 \equiv 1 (mod\ 3)$ and for $Gal(\mathbb{Q}(\zeta_7)/\mathbb{Q}) = \langle \sigma \rangle$ we have $\sigma(\zeta_7) = \zeta_7^3$ and so consider now $\langle \sigma^3 \rangle = \{I, \sigma^3\}$, namely $|\sigma^3| = \frac{6}{3} = 2$.

Let $\alpha = I(\zeta_7) + \sigma^3(\zeta_7) = \zeta_7 + \zeta_7^6$ and observe that

$$\begin{aligned} \sigma^3(\alpha) &= \sigma^3(\zeta_7 + \zeta_7^6) \\ &= \sigma^3(\zeta_7) + \sigma^3(\zeta_7^6) \\ &= \zeta_7^6 + \zeta_7^{36} \\ &= \zeta_7^6 + \zeta_7^1 \\ &= \alpha \end{aligned}$$

If we let

$$\beta = \sigma(\alpha) = \zeta_7^3 + \zeta_7^4$$
$$\gamma = \sigma^2(\alpha) = \zeta_7^2 + \zeta_7^5$$

then we note that

$$\begin{aligned}
\sigma^3(\beta) &= \sigma^3(\sigma(\alpha)) \\
&= \sigma(\sigma^3(\alpha)) \\
&= \sigma(\alpha) \\
&= \beta \\
\sigma^3(\gamma) &= \sigma^3(\sigma^2(\alpha)) \\
&= \sigma^2(\sigma^3(\alpha)) \\
&= \sigma^2(\alpha) \\
&= \gamma
\end{aligned}$$

which means $\alpha, \beta, \gamma \in \mathbb{Q}(\zeta_7)_{\langle\sigma^3\rangle}$

Since $\Phi_7(x) = x^6 + x^5 + \cdots + x + 1$ then $\zeta_7^6 + \zeta_7^5 + \cdots + \zeta_7 + 1 = 0$ and so

$$\alpha + \beta + \gamma = 1$$
$$\alpha\beta + \beta\gamma + \gamma\alpha = -2$$
$$\alpha\beta\gamma = 1$$

which implies that $(x - \alpha)(x - \beta)(x - \gamma) = x^3 + x^2 - 2x + 1 \in \mathbb{Q}[x]$ is a polynomial whose splitting field is $E = \mathbb{Q}(\zeta_7)_{\langle\sigma^3\rangle}$ and that $E = \mathbb{Q}(\alpha)$, and that $irr(\alpha, \mathbb{Q}) = x^3 + x^2 - 2x + 1$.

And again we note that $\beta, \gamma \in E$ too.

The point is that not only can we prove that there are Galois extensions of $\mathbb{Q}$ with any arbitrary cyclic group as their Galois group, but we can generally describe the extension in some detail.