MATH 5020

GALOIS REPRESENTATIONS

$G_{\mathbb{Q}} \circlearrowleft$

LECTURE 4

SPRING 2022

INSTRUCTOR: ÁLVARO LOZANO-ROBLEDO
MONT 233
ALOZANO.CLAS.UCONN.EDU/MATH5020S22
ALVARO.LOZANO-ROBLEDO@UCONN.EDU

§. Cyclotomic Extensions

Def Let $\mu_n \subseteq \mathbb{C}$ be the grp of n-th roots of unity in $\mathbb{C}$.
Then n-th cyclotomic polynomial

$$\Phi_n(x) = \prod_{\substack{\zeta \in \mu_n \\ \text{primitive}}} (x - \zeta) = \prod_{\substack{1 \le a \le n \\ (a,n)=1}} (x - \zeta_n^a)$$

where ζ_n is a fixed n-th prim root of unity (e.g. $\zeta_n = e^{\frac{2\pi i}{n}}$)

Prop.

1) $\phi_n(x) \mid x^n - 1$
2) $\phi_n(x)$ is defined over $\mathbb{Q}$
3) $\phi_n(x)$ is irreducible, monic, in $\mathbb{Z}[x]$
4) $\deg \phi_n(x) = \varphi(n)$, where φ is the Euler φ-function.
5) $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

ex $\phi_1(x) = x - 1, \quad \phi_2(x) = x + 1, \quad \phi_3 = x^2 + x + 1$

p prime $\quad \Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$

$\phi_4(x) = x^2 + 1$

$\Phi_6(x) = x^6 + x^3 + 1$

$\vdots$

Thm $\quad \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$

$$\sigma_a : \zeta_n \mapsto \zeta_n^a \longleftarrow\!\shortmid \; a \bmod n$$

Cor Suppose $n = p_1^{e_1} \cdots p_k^{e_k}$, then

$$\begin{array}{ccccccc}
\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) & \cong & \mathrm{Gal}(\mathbb{Q}(\zeta_{p_1^{e_1}})/\mathbb{Q}) & \times & \cdots & \times & \mathrm{Gal}(\mathbb{Q}(\zeta_{p_k^{e_k}})/\mathbb{Q}) \\
\wr\| & & \wr\| & & & & \wr\| \\
\left(\mathbb{Z}/n\mathbb{Z}\right)^\times & \cong & \left(\mathbb{Z}/p_1^{e_1}\mathbb{Z}\right)^\times & \times & \cdots & \times & \left(\mathbb{Z}/p_k^{e_k}\mathbb{Z}\right)^\times
\end{array}$$

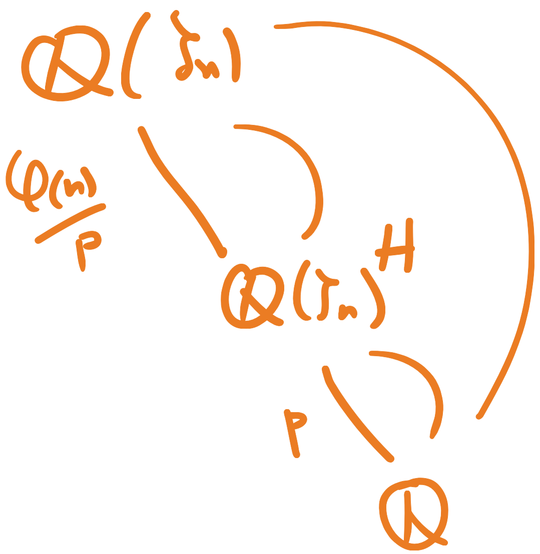
Def Let L/K be an ext'n. We say L/K is an abelian extension if (1) it is Galois and (2) $\mathrm{Gal}(L/K)$ is an abelian gp.

Cor Every ~~s~~ subfield of a cycl. ext'n is an abelian extension of $\mathbb{Q}$.

ex (extensions of $\mathbb{Q}$ of degree p)
(abelian)

Let $n>0$, $\mathbb{Q}(\zeta_n)$, then $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$

so $|G| = \varphi(n)$, abelian, $\Rightarrow$ If $p \mid \varphi(n)$ then G has a subgp H of order $\varphi(n)/p$ of index p.



and $\mathbb{Q}(\zeta_n)^H/\mathbb{Q}$ is of degree p, $H \lhd G$,
with $\mathrm{Gal}(\mathbb{Q}(\zeta_n)^H/\mathbb{Q}) \cong \mathbb{Z}/p\mathbb{Z}$

ex $p=3$, $n=7$

$\varphi(7)=6$

$$\mathbb{Q}(\zeta_n) \supseteq \underbrace{K \supseteq \mathbb{Q}}_{3}$$

Recall: $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$

$= \#\{1 \le a \le n : \gcd(a,n)=1\}$

- $\varphi(1)=1$
- $\varphi(p)=p-1$
- $\varphi(p^n)=p^{n-1}(p-1)$
- $\varphi(ab)=\varphi(a)\varphi(b)$, $\gcd(a,b)=1$

$$\begin{tikzcd}
& \mathbb{Q}(\zeta_7) \arrow[dl, dash, "2"'] \arrow[dr, dash, "3"] & \\
\mathbb{Q}(\cos\frac{2\pi}{7}) =: K \arrow[dr, dash, "3"'] & & F = \mathbb{Q}(\sqrt{-7}) \arrow[dl, dash, "2"] \\
& \mathbb{Q} &
\end{tikzcd}$$

$\{\pm1\} \subseteq (\mathbb{Z}/7\mathbb{Z})^\times$

$\{1,2,4\} \subseteq (\mathbb{Z}/7\mathbb{Z})^\times$

Why $\cos\frac{2\pi}{7}$?? $\zeta_7 + \zeta_7^{-1}$ is fixed by $\{\pm1\} = \{\sigma_1, \sigma_{-1}\}$

- $\sigma_1(\zeta_7+\zeta_7^{-1}) = \zeta_7 + \zeta_7^{-1}$
- $\sigma_{-1}(\zeta_7+\zeta_7^{-1}) = \zeta_7^{-1} + (\zeta_7^{-1})^{-1} = \zeta_7^{-1} + \zeta_7 = \zeta_7 + \zeta_7$ ✓

$\Rightarrow \zeta_7 + \zeta_7^{-1} \subseteq \mathbb{Q}(\zeta_7)^{\{\pm1\}}$

$$\zeta_7 + \zeta_7^{-1} = e^{\frac{2\pi i}{7}} + e^{-\frac{2\pi i}{7}}$$

$$= \cos\frac{2\pi}{7} + i\sin\frac{2\pi}{7} + \cos\left(-\frac{2\pi}{7}\right) + i\sin\left(-\frac{2\pi}{7}\right)$$

$$= 2\cos\frac{2\pi}{7} + i\sin\frac{2\pi}{7} - i\sin\frac{2\pi}{7}$$

$$= 2\cos\frac{2\pi}{7}$$

$\Rightarrow$ $\cos\frac{2\pi}{7}$ is fixed by $\{\pm 1\}$ $\Rightarrow$ $\cos\frac{2\pi}{7} \in \underbrace{\mathbb{Q}(\zeta_7)^{\{\pm 1\}}}_{\deg 3}$

$$\Rightarrow \mathbb{Q}(\zeta_7)^{\{\pm 1\}} = \mathbb{Q}\left(\cos\frac{2\pi}{7}\right).$$

$\mathbb{Q}\left(\cos\frac{2\pi}{7}\right)/\mathbb{Q}$ is a cyclic abelian ext'n of deg 3.

ex $p=3$, $n=13$, $\varphi(13)=12$,

H is cyclic of order 4, $H=\{1,5,8,12\}$

$$\mathbb{Q}(\zeta_{13})^H = \mathbb{Q}\left(\zeta_{13}+\zeta_{13}^5+\zeta_{13}^8+\zeta_{13}^{12}\right)$$

$$\begin{tikzcd}
\mathbb{Q}(\zeta_{13}) \arrow[dr, dash, "4"'] & \\
& \mathbb{Q}(\zeta_{13})^H \arrow[dr, dash, "3"'] & \\
& & \mathbb{Q}
\end{tikzcd}$$

ex $p=5$, $n=11$

$$\begin{tikzcd}
\mathbb{Q}(\zeta_{11}) \arrow[dr, dash, "2"'] & \\
& \mathbb{Q}(\zeta_{11})^{\pm 1} = \mathbb{Q}(\zeta_{11}+\zeta_{11}^{-1}) \arrow[dr, dash] & \\
& & \mathbb{Q}
\end{tikzcd}$$

ex $q \equiv 1 \bmod p$

Dirichlet's thm on arithm. prog.

∞'ly many such q.

$$\begin{tikzcd}
\mathbb{Q}(\zeta_q) \arrow[dr, dash, "\frac{q-1}{p}"'] \arrow[ddrr, dash, bend left, "{q-1,\ p \mid q-1}"] & & \\
& K \arrow[dr, dash, "p"] & \\
& & \mathbb{Q}
\end{tikzcd}$$

ex $p=3$, $n=9$, $\varphi(n)=\varphi(9)=3\cdot(3-1)=6$

$$\begin{tikzcd}
 & \mathbb{Q}(\zeta_9) \arrow[dl, dash, "3"', "\{1 \bmod 3\}"] \arrow[dd, dash, "6", "(\mathbb{Z}/9\mathbb{Z})^\times"'] \arrow[dr, dash, "H"] & \\
\mathbb{Q}(\zeta_3) \arrow[dr, dash, "2"'] & & K_1 \arrow[dl, dash, "3"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

$|H|=2$, $H=\{\pm 1 \bmod 9\}$

$H \cong (\mathbb{Z}/3\mathbb{Z})^\times$

$$\begin{tikzcd}
 & \mathbb{Q}(\zeta_{25}) \arrow[dl, dash, "5"', "\{1 \bmod 5\}"] \arrow[dr, dash, "H=\langle 7\rangle=\{1,7,18,24\}"] & \\
\mathbb{Q}(\zeta_5) \arrow[dr, dash, "4"'] & & K_1 \arrow[dl, dash, "5"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

ex $p=5$, $n=25$, $\varphi(25)=4\cdot 5$

Cor If G is <u>any</u> finite ab gp, then there is $n>0$ s.t. $\mathbb{Q}(\zeta_n)$ contains a subfield K w/ $\mathrm{Gal}(K/\mathbb{Q}) \cong G$.

ex $G = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, Q: What is K?

$\cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$

$$F = \mathbb{Q}(\zeta_7, \zeta_9, \zeta_{11}) = \overbrace{\mathbb{Q}(\zeta_7)\,\mathbb{Q}(\zeta_9)\,\mathbb{Q}(\zeta_{11})}^{\text{disjoint!}} = \mathbb{Q}(\zeta_{7\cdot 9\cdot 11})$$

$$\mathrm{Gal}(F/\mathbb{Q}) \cong (\mathbb{Z}/7\mathbb{Z})^\times \times (\mathbb{Z}/9\mathbb{Z})^\times \times (\mathbb{Z}/11\mathbb{Z})^\times$$

take $H \cong \{\pm 1\} \times \{\pm 1\} \times \{\pm 1\}$

so that $\mathrm{Gal}(F/\mathbb{Q})/H \cong \mathbb{Z}/3 \times \mathbb{Z}/3 \times \mathbb{Z}/5$

$\Rightarrow F^H = K$ has Gal gp $\cong \mathbb{Z}/3 \times \mathbb{Z}/15$. Here $n = 7\cdot 9\cdot 11$.

Fact If $\gcd(m,n)=1$, then $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$.

1) $\gcd(m,n)=1 \Rightarrow \underbrace{\mathbb{Q}(\zeta_m)}_{\deg=\varphi(m)} \underbrace{\mathbb{Q}(\zeta_n)}_{\deg=\varphi(n)} = \underbrace{\mathbb{Q}(\zeta_{mn})}_{\deg=\varphi(mn)}$

then $\Rightarrow$ $\varphi(mn) = \dfrac{\varphi(m)\cdot\varphi(n)}{\deg \text{ of } \mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n)}$ $\Rightarrow \deg$ of $\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n) = 1$.

$\varphi(mn) = \varphi(m)\cdot\varphi(n)$

Euler φ!

2) Ramification: $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is ramified at primes $|n$

$\mathbb{Q}(\zeta_m)/\mathbb{Q}$ is ramified at primes $|m$

$\Rightarrow \mathbb{Q}(\zeta_n)\cap\mathbb{Q}(\zeta_m)$ ramified at primes that divide $\gcd(m,n)=1$

$\Rightarrow$ unramified!

$\Rightarrow$ it's $\mathbb{Q}$.

Thm (Kronecker-Weber Theorem)

Let $K/\mathbb{Q}$ be an abelian ext'n of $\mathbb{Q}$. Then, there is a cyclotomic ext'n $\mathbb{Q}(\zeta_n)$ s.t. $K \subseteq \mathbb{Q}(\zeta_n)$.

ex $K = \mathbb{Q}(\sqrt{2+\sqrt{2}})$ has $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$.

$\rightarrow$ it must be cyclotomic.

In fact: $\mathbb{Q}(\underbrace{\sqrt{2+\sqrt{2+\cdots+\sqrt{2}}}}_{n \text{ times}}) \subseteq \mathbb{Q}(\zeta_{2^{n+2}})$

(ex: DF. ch 14.5. #8)

ex $\mathbb{Q}(\sqrt[3]{2})$ cannot be a subfield of a cyclo. ext'n.

$$\mathbb{Q}(\sqrt[3]{2}) \subseteq \underbrace{\mathbb{Q}(\sqrt[3]{2}, \zeta_3)}_{\text{Gal closure}} \subseteq \underbrace{\mathbb{Q}(\zeta_n)}_{\text{Galois}/\mathbb{Q}}$$

$\mathrm{Gal}(\ /\mathbb{Q}) \cong S_3$ not abelian $\Rightarrow$ $\times$ subfields of cyclo. ext'ns are Galois + abelian.

ex $\underbrace{\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt[4]{3})}_{\text{ab. ext'n of deg 2}}$ however $\mathbb{Q}(\sqrt[4]{3}) \not\subseteq \underbrace{\mathbb{Q}(\sqrt{3}, \zeta_n)}_{\text{Gal is abelian.}}$

Gal closure is non-ab.

WARNING! If K is NOT $\mathbb{Q}$ then there are ab. ext'n's of K that are NOT cyclotomic.

ex (DF: Ch 14.7. #19)

Let $D \in \mathbb{Z}$, sq. free, $K = \mathbb{Q}(\sqrt{D})$

FACT There exists $\mathbb{Q} \subseteq K \subseteq L$ w/ $Gal(L/K) \cong \mathbb{Z}/2\mathbb{Z}$

iff $D = s^2 + t^2$ is a sum of two (rational) squares.

ex $D = 2 = 1 + 1$, $L = \mathbb{Q}(\sqrt{2+\sqrt{2}})$

$D \neq s^2 + t^2$, let $\alpha \in K$, $\alpha \notin \mathbb{Q}$, let $F = K(\sqrt{\alpha})$

then $F/\mathbb{Q}$ cannot be $\mathbb{Z}/4$, cannot be $\mathbb{Z}/2 \times \mathbb{Z}/2$

$\Rightarrow$ not Gal over $\mathbb{Q}$ $\rightarrow$ not cyclotomic over K.

The End.