

Lecture # 6 (16/10/2024)

Today: An overview on cyclotomic and cyclic extensions.

Definition Let K be a field. If $\omega \in K$ is a root of $x^n - 1$ then ω is called an n th root of unity. If, moreover, the order of ω in $K^\times$ is n , then ω is called a primitive n -th root of unity.

Definition A cyclotomic extension is an extension of the form $K(\omega)/K$ where ω an n -th root of unity (for some n).

Proposition 1 Suppose that $(\text{char } K, n) = 1$ and let $L = \text{SF}_K(x^n - 1)$. Then L/K is Galois and L is generated by any primitive n -th root of unity. Moreover, $\text{Gal}(L/K) \leq (\mathbb{Z}/n\mathbb{Z})^\times$.

Thus, every cyclotomic extension $K(\mu_n)/K$ is Abelian and its degree divides $\phi(n)$.

↑ Euler totient function

In fact, one can show that for each $\sigma \in \text{Gal}(L/K)$, there exists $j \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that

$$\sigma \omega = \omega^j \quad \forall \omega \text{ s.t. } \omega^n = 1$$

This defines an injective homomorphism $\sigma \mapsto [j]$

Proposition 2 Let K be a field and let $n \in \mathbb{Z}_{>0}$ be such that $(n, \text{char } K) = 1$. Let $K_n := K(\mu_n)$ and $L := K_n(\alpha^{1/n})$. Then $\text{Gal}(L/K)$ is solvable.

proof Since we have a s.e.s.

$$1 \rightarrow \text{Gal}(L/K_n) \rightarrow \text{Gal}(L/K) \xrightarrow{\text{res}} \text{Gal}(K_n/K) \rightarrow 1$$

it suffices to show that $\text{Gal}(L/K_n)$ and $\text{Gal}(K_n/K)$ are solvable.

First, note that we have

$$\begin{aligned} \text{Gal}(L/K_n) &\hookrightarrow \mu_n \simeq \mathbb{Z}/n\mathbb{Z} \\ \sigma &\mapsto \frac{\sigma(\alpha^{1/n})}{\alpha^{1/n}} \end{aligned}$$

Second, by Proposition 1,

$$\text{Gal}(K_n/K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$$



Note: Galois criterion $\Rightarrow L/K$, L/K_n and K_n/K are solvable.

(K & n as before...)

Proposition 3 Any cyclic Galois extension of K_n of order dividing n is of the form L/K_n .

proof

Let F/K_n be a cyclic Galois extension
whose degree divides n .

(recall: $K_n = K(\mu_n)$ and $(\text{char } K, n) = 1$)

Write $G = \text{Gal}(F/K_n) = \langle \sigma \rangle$ and let
 ζ be a primitive n -th root of unity.

We will show that there exists $\beta \in F^\times$ s.t.

$$\frac{\sigma(\beta)}{\beta} = \zeta \in \mu_n \quad (\text{cf. Prop. 2})$$

(Note that $\sigma(\beta^n) = \beta^n \Rightarrow \beta^n \underset{\text{def}}{=} \in K_n$)

Since $\{1, \sigma, \dots, \sigma^{n-1}\}$ is l.i. / K_n , $\exists f \in F$ s.t.

$\uparrow$
Dedekind's Lemma

$$\beta := f + \zeta \sigma(f) + \zeta^2 \sigma^2(f) + \dots + \zeta^{n-1} \sigma^{n-1}(f) \neq 0 \quad *$$

(given any $p(x) \in K_n[x] \setminus \{0\}$ of $\deg \leq n-1$, $p(\sigma) \neq 0$)

Then using $\star$ we deduce that :

$$\begin{aligned}\text{Gal}(F/K_n(\beta)) &= \{ \varphi \in G ; \varphi(\beta) = \beta \} \\ &= \{ 1 \}\end{aligned}$$

$$\Rightarrow K_n(\beta) = F.$$

Alternatively, note that showing that β exists is equivalent to showing that $\sigma: L \rightarrow L$ is diagonalizable with eigenvalues the roots of $X^n - 1$.

Let $P(X) := \min_{K_n} \sigma$. Since $P(\sigma) = 0$

and $\sigma^n - \text{id}_L = 0_L$, $\deg(P) = n$

and $P(X) = X^n - 1$.



Lemma 2 (Lec #5)

Proposition 4 Any cyclic extension of a field K of char $K=0$ is solvable.

Lemma Given L/K , $M/K \subset \bar{K}/K$ finite, if M/K and LM/M are solvable then L/K is solvable.

proof

We apply the lemma to $M = K_n = K(\mu_n)$ where $n = [L:K]$.

Then M/K is clearly solvable.

Now,

$$G = \text{Gal}(LK_n / K_n) \simeq \text{Gal}\left(L / L \cap K_n\right) \\ \simeq \prod \text{Gal}(L/K)$$

So, G is cyclic of order $d|n$.

Proposition 3 $\Rightarrow LK_n = K_n(\alpha^{1/n})$

Independence of characters

Definition A character of a grp. G in a field K , is a grp.hom. $\chi: G \rightarrow K^\times$.

Dedekind's Lemma Any set $\{\chi_1, \dots, \chi_n\}$ of distinct characters $\chi_i: G \rightarrow K^\times$ is linearly independent in $\text{Hom}(G, K^\times)$.

proof Take $\chi := \sum_{i=1}^n a_i \chi_i$ with

$\chi(g) = 0 \ \forall g \in G$. We want to show $a_i = 0 \ \forall i$.

We can use induction on n .

$n=1 \checkmark$: if $a_1 \chi_1(g) = 0 \ \forall g \in G$, then $a_1 = 0$ since $\chi_1(g) \in K^\times$

Now, for any $g, h \in G$ we have that

$$0 = \underbrace{\sum_{i=1}^n a_i \chi_i(hg)}_{=0} - \chi_n(h) \underbrace{\left(\sum_{i=1}^n a_i \chi_i(g) \right)}_{=0}$$

$$= \sum_{i=1}^{n-1} b_i \chi_i(g)$$

$$\text{where } b_i := a_i (\chi_i(h) - \chi_n(h))$$

By the inductive step, each b_i is zero,

hence $a_1, \dots, a_{n-1} = 0$

and repeating step 1 we deduce that $a_n = 0$.



Corollary If L and K are fields and $\sigma_1, \dots, \sigma_n \in \text{Hom}(L, K)$ are distinct, then the σ_i s are l.i. over K .

- Cyclic extensions of degree p in $\text{char} = p$

Given a field F of $\text{char} = p$, consider

$$\begin{aligned} \Psi_p: F &\longrightarrow F \\ a &\longmapsto a^p - a \end{aligned} \quad \left(\Rightarrow \text{Ker } \Psi_p = \mathbb{F}_p \right)$$

Proposition Let $\text{char}(K) = p$, and let L/K be a cyclic Galois extension of $\deg = p$.

Then $L = K(\alpha)$, where $\alpha = \Psi_p^{-1}(a)$

for some $a \in K$.

proof Let $G = \text{Gal}(L/K) = \langle \sigma \rangle$ and $T = \sigma - \text{id}_L$ ($T: L \rightarrow L$ linear).

Then • $\text{Ker}(T) = K$

$$\bullet \quad T^p = (\sigma - \text{id}_L)^p = \sigma^p - \text{id}_L = 0_L$$

$$\Rightarrow \text{im}(T^{p-1}) \subset \text{Ker}(T)$$

$$\Rightarrow \text{im}(T^{p-1}) = \text{Ker}(T) = K$$

Thus, $\exists \beta \in K$ s.t. $T^{P-1}(\beta) = 1_K$

and we can take $\alpha := T^{P-2}(\beta)$.

$$\left(T(\alpha) = T^{P-1}(\beta) = 1_K \Leftrightarrow \sigma(\alpha) - \alpha = 1_K \right)$$

Then α is not fixed by σ ($\Leftrightarrow \alpha \notin K$)

and since $[L:K] = p$, $L = K(\alpha)$.
(~~X~~ int. fields)

Lastly, we need to check that

$$\sigma(\alpha^P - \alpha) = \alpha^P - \alpha$$

$$\Updownarrow$$

$$\alpha = \varphi_p^{-1}(\alpha) \text{ for some } \alpha \in K.$$

Indeed,

$$\begin{aligned} \sigma(\alpha^P - \alpha) &= \sigma(\alpha)^P - \sigma(\alpha) \\ &= (1 + \alpha)^P - (1 + \alpha) \\ &= \alpha^P - \alpha \end{aligned}$$



Conversely,

Proposition Let $\text{char}(K) = p$ and $a \in K \setminus \Phi_p^{-1}(a)$. Then $f(x) = x^p - x - a$ is irreducible over K and $SF_K(f)/K$ is cyclic Galois of $\deg = p$.

proof Let α be a root of f , then the p roots of f can be written as

$$\alpha, \alpha+1, \dots, \alpha+p-1$$

So, $L = SF_K(f) = K(\alpha)$ w/ $\alpha \notin K$.

Now, if $f = g_1 \cdot \dots \cdot g_n$ w/ each g_i irred.,

then $L = K(\beta)$ where β is a root of some g_i . Thus, $[L:K] = \deg g_i \quad \forall i$

and $\deg f = n \deg g_1 \Rightarrow n=1$ and f is irred.

Finally, since f is irred. and separable
 L/K is cyclic Galois of $\deg = \deg f = p$

□

The normal basis theorem

Definition Let L/K be a Galois extension
with $\text{Gal}(L/K) = \{\sigma_1, \dots, \sigma_n\}$. A normal
basis for L/K is a basis consisting of
 K -conjugate elements $\{\sigma_1(\alpha), \dots, \sigma_n(\alpha)\}$

Examples

- ① $\mathbb{C}/\mathbb{R}$ and $\{1+i, 1-i\}$
- ② $\mathbb{Q}(\mu_p)/\mathbb{Q}$ and $\{\zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1}\}$
- ③ Check that $\mathbb{Q}$ -conjugates of $\sqrt{2} + \sqrt{3}$
do not form a normal basis for $\mathbb{Q}(\sqrt{2} + \sqrt{3})/\mathbb{Q}$.

Thm. Every finite cyclic extension L/K has a normal basis.

proof Write $\text{Gal}(L/K) = \{1, \sigma, \dots, \sigma^{n-1}\} = \langle \sigma \rangle$.

View L as a $K[x]$ -module where x acts on L as σ .

Then

$$x^n - 1 \in \text{Ann}_{K[x]}(L) = \{f \in K[x]; f(\sigma) \equiv 0 \text{ on } L\}$$

$$K[x] \text{ is a PID + Dedekind} \Rightarrow \text{Ann}_{K[x]}(L) = (x^n - 1)$$

Then $\exists l \in L$ s.t. $f(\sigma)(l) = 0 \Leftrightarrow x^n - 1$ divides f

$$\text{ev}_l: K[x] \rightarrow L$$

$$f(x) \mapsto f(\sigma)(l)$$

has kernel $x^n - 1$.

Thus, $K[x]/(x^n - 1) \simeq L$ (they have the same dim)

and under this iso,

$$\{1, X, \dots, X^{n-1}\} \mapsto \{e, \sigma(e), \dots, \sigma^{n-1}(e)\}$$

This gives a normal basis.



Digression on f.g. modules / a PID ...

In the proof, it suffices to show that L is a cyclic $K[x]$ -module, which follows from the fact that the characteristic and the minimal polynomials of σ are the same (+ structure thm for f.g. modules over a PID).