Lecture # 6 (16/10/2025)

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 nth 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).

(Morandi 7.2)

I mean: $\operatorname{char} K \nmid n$

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

iso to a subgroup of

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 $\sigma \in \mathrm{Gal}(L/K)$, there exists $j \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that

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

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 $(n, \mathrm{char}\ K) = 1$. Let $K_n := K(\mu_n)$ and $L := K_n(\alpha^{1/n})$. Then $\mathrm{Gal}(L/K)$ is solvable.

$\exists\ a \in L$ such that $\alpha^{1/n} = a$, $a^n = \alpha \in K_n$

proof Since we have a s.e.s.

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

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

First, note that we have

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

Second, by Proposition 1,

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

∎

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.

(For a proof that L/K_n is cyclic see Morandi 9.6)

Proof

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

(recall: $K_n = K(\mu_n)$ and $\operatorname{char} K \nmid n$)

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

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

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

(Note that $\sigma(\beta^n) = \beta^n \Rightarrow \beta^n \in K_n$, $\beta^n = \alpha$)

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

↑ Dedekind's Lemma (page 7)

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

(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:

$$\mathrm{Gal}\left(F/K_n(\beta)\right) = \{\varphi \in G ;\ \varphi(\beta) = \beta\}$$

$$= \{1\}$$

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

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

Let $P(X) := \min_{K_n} \sigma$. Since $P(\sigma) = 0$ and $\sigma^n - \mathrm{id}_L = 0_L$, $\deg(P) = n$ and $P(X) = X^n - 1$.

$\blacksquare$

Lemma 2 (Lec #5)
//

Proposition 4 Any cyclic extension of a field K of $\operatorname{char} K = 0$ 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,

$$G = \mathrm{Gal}(LK_n/K_n) \simeq \mathrm{Gal}(L/L \cap K_n)$$

$$\cap$$

$$\mathrm{Gal}(L/K)$$

So, G is cyclic of order $d \mid n$.

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. $\chi : G \longrightarrow K^\times$.

Dedekind's Lemma Any set $\{\chi_1, \dots, \chi_n\}$ of distinct characters $\chi_i : G \longrightarrow K^\times$ is linearly independent in $K[G]$ (as vector space / K)

group ring

proof Take $\chi := \sum_{i=1}^{n} a_i \chi_i$ with $a_i \in K$ such that $\chi(g) = 0 \ \forall \ g \in G$. We want to show that $a_i = 0 \ \forall \ i$.

We can use induction on n:

$n = 1$ ✓ : 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

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

$$\underbrace{\qquad\qquad}_{=0} \qquad\qquad \underbrace{\qquad\qquad}_{=0}$$

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

where $b_i := a_i \left(\chi_i(h) - \chi_n(h) \right)$

By the inductive step, each b_i is zero,

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

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

∎

Corollary If L and K are fields and $\sigma_1, \ldots, \sigma_n \in \mathrm{Hom}(L, K)$ are distinct, then the σ_is are l.i. over K.

We apply the Lemma to the restriction to the group of units

• Cyclic extensions of degree p in char $= p$

Given a field F of char $= p$, consider

$$\varphi_p : \begin{array}{ccc} F & \longrightarrow & F \\ a & \longmapsto & a^p - a \end{array} \qquad \left(\Rightarrow \operatorname{Ker} \varphi_p = \mathbb{F}_p \right)$$

Note also that if $a \in \mathbb{F}_p$, then

$$\varphi_p^{-1}(a) = \{ a + i \; ; \; i \in \mathbb{F}_p \}$$

Morandi 9.8

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

Then $L = K(\alpha)$, where $\alpha = \varphi_p^{-1}(a)$ for some $a \in K$.

In other words, $a \in K$ is s.t. $\alpha^p - \alpha - a = 0$

proof Let $G = \operatorname{Gal}(L/K) = \langle \sigma \rangle$ and $T = \sigma - id_L$ $\left(T : L \to L \text{ linear} \right)$.

Then • $\operatorname{Ker}(T) = K$

• $T^p = (\sigma - id_L)^p = \sigma^p - id_L = 0_L$

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

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

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

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

$T(\alpha) = T^{p-1}(\beta) = 1_K \iff \sigma(\alpha) - \alpha = 1_K$

$\Updownarrow$

$\sigma(\alpha) = \alpha + 1$

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

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

(∄ int. fields)

Lastly, we need to check that

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

$$\Updownarrow$$

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

Indeed,

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

$\square$

Conversely,

no root of f lies in K $\Rightarrow$ a is not a root of f

Morandi 9.9

Proposition Let $\text{char}(K) = p$ and $a \in K \setminus \varphi_p^{-1}(K)$. 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

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

$[L:K] > 1$ $\Rightarrow$

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

Now, suppose that f is not irreducible.

Then we can write $f = g_1 \cdot \ldots \cdot g_n$ $n > 1$ w/ each g_i irred.

Now, for each i, if β is a root of g_i, β is a root of f, hence $L = K(\beta)$ (as above)

This implies $[L:K] = \deg g_i \ \forall i$

But if all g_i have the same degree, then

$p = \deg f = n \cdot \deg g_1$ and p prime + $\deg g_i > 1$ $\Rightarrow n = 1$

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

$\Rightarrow [L/K] = \deg f = p$ ∎

Note that f is separable as it is irreducible and it's formal derivative is not 0 in $K[X]$

The normal basis theorem

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

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

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

Then

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

$K[x]$ is a PID + DedeKind $\Rightarrow Ann_{K[x]}(L) = (x^n - 1)$

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

$$ev_\ell : K[x] \longrightarrow L$$
$$f(x) \longmapsto f(\sigma)(\ell)$$

has Kernel $x^n - 1$.

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

and under this iso,

$$\{1, X, \ldots, X^{n-1}\} \longmapsto \{\ell, \sigma(\ell), \ldots, \sigma^{n-1}(\ell)\}$$

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).