# Lecture 15 Basic number theory

**Defn** We say that an algebraic field extn $L/K$ is separable if $\forall \alpha \in L$ its min. poly. $P_{\alpha/K}(X) \in K[X]$

is s.t.

$$P_{\alpha/K}(X) = \prod_{i=1}^{d} (X - \alpha_i)$$

over its splitting field has all $\alpha_1, \ldots, \alpha_d$ distinct.

**Prop:** Given a field extn $L/K$ and $\alpha \in L$ algebraic $/K$, the minimum polynomial $P_{\alpha/K}(X) \in K[X]$, then either

(i) $\chi(K) = p > 0$ and $\exists\ r \in \{0, 1, 2, 3, \dots\}$ s.t.

$$P_{\alpha/K}(X) = g(X^{p^r}) = (g(X))^{p^r},$$

where all the roots of $g(X)$ are distinct, or

(ii) $\chi(K) = 0$ and all the roots of $P_{\alpha/K}(X)$ are simple.

Proof

By a criterion we have shown before,

$$\alpha \text{ is a simple root of } P_{\alpha/k}(X) \iff P'_{\alpha/k}(\alpha) \neq 0.$$

But $\deg P'_{\alpha/k}(X) < \deg P_{\alpha/k}(X)$. So the minimality of $P_{\alpha/k}(X)$ yields the implication

$$P'_{\alpha/k}(\alpha) = 0 \implies P'_{\alpha/k}(X) = 0.$$

More precisely, we may write

$$p_{\alpha/k}(X) = X^d + \sum_{n=0}^{d-1} a_n X^n$$

and therefore

$$p'_{\alpha/k}(X) = d X^{d-1} + \sum_{n=1}^{d-1} n a_n X^{n-1} \qquad \text{(A)}$$

Thus $p'_{\alpha/k}(\alpha) = 0 \Rightarrow \chi(k) = p > 0$ and

(i) $p \mid d$, $\quad (d = p d_1)$

(ii) $\forall\, n \in \{1, \dots, d-1\} : p \nmid n \Rightarrow a_n = 0.$

Therefore $p_{\alpha/k}(X) = \left(X^{d_1}\right)^p + \sum_m a_{pm} X^{pm} = g_1(X^p).$

$g_1(X) := X^{d_1} + \sum a_{1,m} X^m$

This way we may define

$$g_1(X) = g_2(X^p)$$

$$g_2(X) = g_3(X^p)$$

$$\vdots$$

$$g_r(X) = g_{r-1}(X^r)$$

and stop when the polynomial $g(X) := g_r(X)$ has simple roots only. We thus get (i). If $\chi(K) = 0$, then (✡) is never the zero polynomial and (ii) follows □

Defn Notation as above, we write $[K(\alpha):K]_i := p^r$ and call it the degree of inseparability of $K(\alpha)/K$, and $[K(\alpha):K]_s = \deg g(x)$ and call it the degree of separability of $K(\alpha)/K$.

We may extend this definitions to all finite extensions $L/K$ and have the identity

$$[L:K] = [L:K]_s [L:K]_i .$$

$L = K(\alpha)$

**Defn** We say that a finite field ext$^n$ $L/K$ is Galois if

(i) $L/K$ is separable

(ii) $L$ is the splitting field of a polynomial $f(X) \in K[X]$, i.e. if $L/K$ is normal.

If $L/K$ is Galois, we write

$$G(L/K) := \{ \sigma \in \mathrm{Aut}(L) \mid \sigma|_K = id_K \}$$

and call it the Galois group of $L/K$.

**Thm** A finite field ext$^n$ $L/K$ is Galois iff

$$\mathrm{Aut}_K(L) := \{\sigma \in \mathrm{Aut}(L) \mid \sigma|_K = id\}$$

i) s.t.

$$|\mathrm{Aut}_K(L)| = [L:K].$$

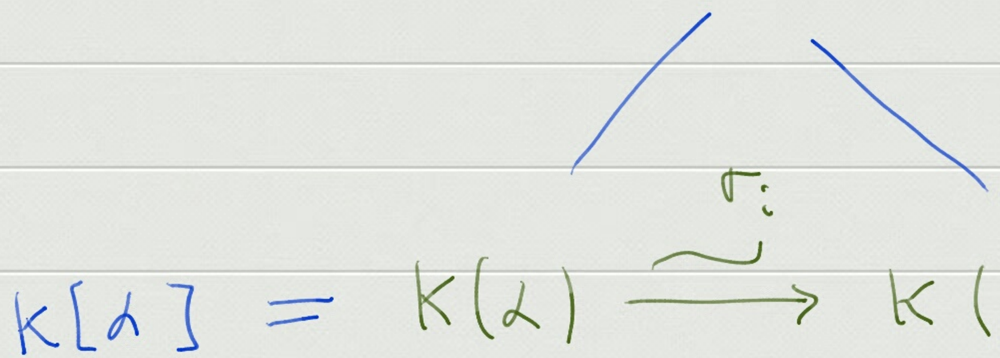
Assume $L = K(\alpha)$

$$L = sf\left(P_{\alpha/K}(x)\right) = K(\alpha_1, \ldots, \alpha_d)$$

Fix an algebraic closure $K^a$ of a given field $K$ and $\alpha \in K^a$. Then

$$P_{\alpha/K}(X) = (X-\alpha_1)\cdot\ldots\cdot(X-\alpha_d), \quad \alpha_i \in K^a,$$

and we have isomorphisms $\qquad (\alpha_1 := \alpha)$



Moreover, for each $\alpha \in K^a$ we have a 1-1 correspondence

$$C_\alpha := \{\alpha_1, \dots, \alpha_d\} \longleftrightarrow \left\{ \sigma_i : K(\alpha) \xrightarrow{\sim} L \;\middle|\; \begin{array}{ccc} & K^a & \\ \nearrow & & \nwarrow \\ K(\alpha) & & \\ & \searrow \quad \swarrow & \\ & K & \end{array} \right\}$$

$$\alpha_i \mapsto \sigma_i(\alpha)$$

$$\alpha$$

We shall now discuss a key example of Galois field ext'n. Let $n \in \{2, 3, 4, \dots\}$, $\zeta_n := e^{2\pi i/n} \in \mathbb{C}$,

$$\mu_n := \zeta_n^{\mathbb{Z}} = \zeta^{\mathbb{Z}/n\mathbb{Z}} = \{1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}\}.$$

We have

$$\begin{array}{ccc} L = \mathbb{Q}(\mu_n) & & \\ | & \overset{\kappa}{\longrightarrow} & \mathrm{Aut}(L/K) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times \\ & & \sigma \longmapsto a_\sigma \\ K = \mathbb{Q} & & \end{array}$$

Here $\forall\ \sigma \in \mathrm{Aut}(L/K)$ then $\sigma(\zeta_n)$ is another generator of $\mu_n$, thus $\sigma(\zeta_n) = \zeta_n^{a_\sigma}$, where $a_\sigma \in (\mathbb{Z}/n\mathbb{Z})^\times$. Clearly $\kappa$ is injective. Moreover

**Thm** We have a group isomorphism

$$\begin{array}{ccc} \mathrm{Gal}(L/\mathbb{Q}) & \xrightarrow{K} & (\mathbb{Z}/n\mathbb{Z})^\times \\ \sigma & \longmapsto & a_\sigma \end{array}$$

*Proof* — after van der Waerden

It suffices to show that the degree of the minimum polynomial $P_{\xi/\mathbb{Q}}(X) \in \mathbb{Q}[X]$ of a primitive $n$-th root of unity $\xi$ is $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$.

We'll need the following.

Lemma (Gauß) Given monic $f(X) \in \mathbb{Z}[X]$ and

$$f = gh$$

where $g(X), h(X) \in \mathbb{Q}[X]$ are monic, then $g(X), h(X) \in \mathbb{Z}[X]$.

Proof of lemma

Let $m \in \mathbb{Z}_{\geq 1}$ be minimal s.t. $m\,g(X) \in \mathbb{Z}[X]$,

$n \in \mathbb{Z}_{\geq 1}$ " " $n \cdot h(X) \in \mathbb{Z}[X]$.

Note that the coefficients of $m\,g(X)$ have no common divisor greatest than 1. The same for $n\,h(X)$.

Suppose that $nm > 1$. Pick any prime $p \mid nm$ and consider that

$$mnf = mg \cdot nh.$$

The canonical map $\mathbb{Z} \longrightarrow \mathbb{F}_p$ yields

$$\tilde{m}\tilde{n}\tilde{f} = \tilde{m}\tilde{g} \cdot \tilde{n}\tilde{h} = \tilde{0}$$

Thus either $\tilde{m}\tilde{g} = \tilde{0}$ or $\tilde{n}\tilde{h} = \tilde{0}$, a contradiction.

Hence $nm = 1$, so $n = 1$ and $m = 1$. $\square$

Claim The polynomial $P_{\zeta/\mathbb{Q}}(X) \in \mathbb{Z}[X]$

Proof of claim

By definition $P_{\zeta/\mathbb{Q}}(X)$ is monic and lies in $\mathbb{Q}[X]$. Moreover, as $\zeta$ is a zero of $F(X) = X^n - 1$, then $P_{\zeta/\mathbb{Q}}(X) \mid F(X)$, so the Gauß lemma implies that $P_{\zeta/\mathbb{Q}}(X) \in \mathbb{Z}[X]$ $\square$

We need to show that $\forall\ a \in \mathbb{Z}$ s.t. $(a,n)=1$,

$$P_{\zeta/\mathbb{Q}}(\zeta^a) = 0$$

Claim We may assume WLOG that $a = p$, prime not dividing $n$.

Proof of claim

[Ex.]

Consider that the factorization over $\mathbb{Q}$ into monic irred's

$$X^n - 1 = f_1(X) \cdot \ldots \cdot f_k(X) \qquad \star$$

must be also over $\mathbb{Z}$ (again by the Gauß lemma),

so the canonical map $\mathbb{Z} \longrightarrow \mathbb{F}_p$ yields

$$X^n - \tilde{1} = \tilde{f}_1(X) \cdot \ldots \cdot \tilde{f}_k(X)$$

over $\mathbb{F}_p$. Let $L$ be the splitting field of $X^n - 1$ over $\mathbb{F}_p$.

As $p \nmid n$, $X^n - 1 = (X - z_1) \cdot \ldots \cdot (X - z_n)$, with

$z_1, \ldots, z_n \in L$ distinct. Thus $i \neq j$ implies that

$$(\tilde{f}_i, \tilde{f}_j) = 1.$$

Choose the numbering in (★) so that $f_1(X) = P_{\xi/\mathbb{Q}}(X)$ and suppose $\xi^p$ is a root of $f_j(X)$. In particular, $\xi$ is a root of $f_j(X^p)$, so $f_1(X) \mid f_j(X^p)$. Then $\tilde{f}_1(X) \mid \tilde{f}_j(X^p)$.

Hence $\forall$ root $z \in L$ of $\tilde{f}_1(X)$ we have $\tilde{f}_j(z^p) = 0$.

But $\tilde{f}_1(z^p) = \left(\tilde{f}_1(z)\right)^p = 0$, so $\tilde{f}_1(X)$ and $\tilde{f}_j(X)$ are not coprime if $j \neq 1$. Therefore $j = 1$, i.e. $k$ is an isomorphism. □