Lecture 24 The discriminant

Let M be a monoid and F a field. A homomorphism $\chi : M \longrightarrow F^{\times}$ is known as a *character*. Any ring homomorphism $\sigma : E \to F$, where E and F are fields, yields a character $\sigma^{\times} : E^{\times} \to F^{\times}$, a fact we shall use soon.

Thm (Artin) Notation as above, if $\chi_1, \ldots, \chi_n$ are distinct characters, then for all $(a_1, \ldots, a_n) \in K^n$,

$$a_1\chi_1 + \cdots + a_n\chi_n = 0$$

implies $(a_1, \ldots, a_n) = (0, \ldots, 0)$.

Proof

Suppose there is a nontrivial retation

$$a_1 \chi_1 + \cdots + a_n \chi_n = 0$$

We may assume WLOG that n is minimal, so $n \geq 2$ and $a_i \neq 0$, for each $i \in \{1, \ldots, n\}$. As $\chi_1 \neq \chi_2$, $\exists\, g \in G$ s.t. $\underbrace{\chi_1(g) \neq \chi_2(g)}_{*}$ and consider that $\forall\, x \in G$

$$a_1 \chi_1(xg) + \cdots + a_n \chi_n(xg) = 0$$

$$a_1 \chi_1(x)\chi_1(g) + \cdots + a_n \chi_n(x)\,\chi_n(g) = 0$$

Thus

$$a_1 \chi_1(x)\chi_1(g) + a_2 \chi_2(x)\chi_2(g) + \cdots + a_n \chi_n(x)\chi_n(g) = 0$$

$$+ \Big\{ \cancel{a_1 \chi_1(x)} + a_2 \cdot \frac{\chi_2(x)\chi_2(g)}{\chi_1(g)} + \cdots + a_n \cdot \frac{\chi_n(x)\chi_n(g)}{\chi_1(g)} = 0$$

$$\Big\lfloor \cancel{-a_1 \chi_1(x)} - a_2 \chi_2(x) - \cdots \qquad \cdots - a_n \chi_n(x) = 0$$

$$\star \left(a_2 \cdot \frac{\chi_2(g)}{\chi_1(g)} - a_2 \right) \chi_2(x) + \cdots \qquad = 0$$

But $(*)$ implies that

$$\left(a_2 \cdot \frac{\chi_2(g)}{\chi_1(g)} - a_2 \right) \neq 0$$

So the linear relation $(\star)$ is nontrivial, and has length $< n$, contradicting the minimality assumption. $\square$

As before, let E/K be a finite field ext'n and assume that it is separable.

$$Tr_{E/K} : E \longrightarrow K$$

Then the trace map is a nonzero element of the dual space $E^* := L_K(E, K)$.

Indeed, recall that for each $\alpha \in E$

$$\mathrm{Tr}_{E/K}(\alpha) = \sum_{\sigma \in \mathrm{Hom}_K(E, \bar{K})} \sigma(\alpha)$$

But Artin's thm on the linear independence of characters implies that

$$\sum_{\sigma \in \mathrm{Hom}_K(E, \bar{K})} \sigma^{\times} \neq 0$$

Hence $\mathrm{Tr}_{E/K}$ is not the zero linear functional.

As above, let E/K be a separable finite field ext'n. Consider the symmetric K-bilinear form

$$E \times E \longrightarrow E$$

$$(x,y) \longmapsto T_{E/K}(xy) =: B(x,y)$$

Propn The above bilinear form induces an isomorphism of K-vector spaces

$$E \xrightarrow{\varphi} L_K(E,K) = E^*$$

$$x \longmapsto \left(E \longrightarrow E,\ y \longmapsto B(x,y) \right)$$

Proof

As E/K is finite dimensional it suffices to prove injectivity, i.e. that $\ker(\varphi) = 0$.

Let $x \in \ker(\varphi)$, then

$$\varphi_x : E \longrightarrow E$$
$$y \longmapsto B(x,y)$$

is the zero map. If $x \neq 0$ then $y \longmapsto xy$ is a permutation of E,

which means that for all $z \in E$

$$Tr_{E/K}(z) = 0,$$

contradicting Artin's theorem. Thus $x = 0$ □

If E/K is as above, and $\mathcal{B} := \{\beta_1, \dots, \beta_n\}$ is a basis for E/K, then we have the *discriminant*

$$d(\beta_1, \dots, \beta_n) := \det \begin{pmatrix} B(\beta_1, \beta_1) & \cdots & B(\beta_1, \beta_n) \\ \vdots & & \vdots \\ B(\beta_n, \beta_1) & \cdots & B(\beta_n, \beta_n) \end{pmatrix}$$

By the above proposition it is non zero. Moreover, it defines a unique class

$$d_{E/K} \in K^\times / (K^\times)^2$$

known as the *discriminant* of E/K. Our separability assumption implies that

E/K is simple, i.e. $E = K(\alpha)$, for some $\alpha \in E$, so $\mathcal{B} = \{1, \alpha, \dots, \alpha^{n-1}\}$ is a basis for E/K we have the following formula

$$d_{E/K} = \prod_{i<j} (\alpha_i - \alpha_j)^2 \mod (K^\times)^2$$

where

$$p_{\alpha/K}(X) = (X - \alpha_1) \cdots (X - \alpha_n)$$

is the factorisation of the minimum polynomial $p_{\alpha/K}(X) \in K[X]$ into linear factors $/\bar{K}$.

Indeed, just apply the Vandermonde polynomial identity

$$\det \begin{pmatrix} 1 & X_1 & \cdots & X_1^{n-1} \\ \vdots & & & \vdots \\ 1 & X_n & \cdots & X_n^{n-1} \end{pmatrix} = \prod_{i<j} (X_i - X_j)$$

regarded as an equality in $\mathbb{Z}[X_1, \ldots, X_n]$.