

## Lecture 8 The discriminant

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

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

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

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

Proof

Suppose there is a nontrivial relation

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

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



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

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

Thus

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

$$+ \left\{ \begin{array}{l} \cancel{a_1 \chi_1(x)} + a_2 \cdot \frac{\chi_2(x) \chi_2(g)}{\chi_1(g)} + \dots + a_n \cdot \frac{\chi_n(x) \chi_n(g)}{\chi_1(g)} = 0 \\ \cancel{-a_1 \chi_1(x)} - a_2 \chi_2(x) - \dots \dots - a_n \chi_n(x) = 0 \end{array} \right.$$

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

But (\*) implies that

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

So the linear relation (☆) 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.

$$\text{Tr}_{E/K} : E \longrightarrow K$$

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

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

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

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

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

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

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

$$E \times E \longrightarrow E$$

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

Prop'n The above bilinear form induces an isomorphism of  $K$ -vector spaces

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

$$x \longmapsto \left( \begin{array}{c} E \longrightarrow E \\ y \longmapsto B(x, y) \end{array} \right)$$

Proof

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

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

$$\begin{aligned}\varphi_x: E &\longrightarrow E \\ x &\longmapsto B(x, y)\end{aligned}$$

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

which means that for all  $z \in E$

$$\text{Tr}_{E/K}(z) = 0,$$

contradicting Artin's theorem. Thus  $x = 0$   $\square$

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  $B = \{1, \alpha, \dots, \alpha^{n-1}\}$  is a basis for  $E/K$  we have the following formula

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

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  $\mathbb{Z}[X_1, \dots, X_n]$ .