MATH8510
Lecture 22 Notes

Charlie Conneen

October 14, 2022

Lifting absolute values to finite extensions

First, we recall the notion of *degree* of a field extension.

Definition. Let L/K be a field extension. The **degree** of this extension is given by

$$[L:K] \coloneqq \dim_K(L).$$

Corollary (of the Theorem from last lecture)**.** *If $[L:K] < \infty$ and K is complete with respect to an absolute value $|\cdot|_K$, then there exists at most one absolute value $|\cdot|_L$ such that $|\alpha|_L = |\alpha|_K$ for all $\alpha \in K$. Furthermore, if such an absolute value exists, then $(L, |\cdot|_L)$ is complete.*

Proof. Suppose $|\cdot|_L, |\cdot|_L'$ are two absolute values on L which restrict to $|\cdot|_K$ on K. Then properties (i)-(iii) of absolute values imply $|\cdot|_L$ and $|\cdot|_L'$ are not just absolute values, but norms, treating L as a K-vector space. So the previous theorem yields some $C > 0$ such that $|x|_L \leq C \cdot |x|_L'$ for all $x \in L$.

Now take any $y \in L$. Then for all $n \in \mathbb{N}$,

$$|y|_L = (|y^n|_L)^{1/n} \leq \left(C|y^n|'\right)^{1/n} = C^{1/n} \cdot |y|_L'$$

Take $n \to \infty$ to observe that $|y|_L \leq |y|_L'$. By symmetry of this argument, $|y|_L = |y|_L'$.

Completeness follows from the previous theorem, since we have obtained a norm on a finite dimensional vector space over a field which is complete. ■

Recall that $\dim_{\mathbb{R}} \mathbb{C} = 2$. How do we obtain *the* absolute value on $\mathbb{C}$ which extends $|\cdot|_\infty$? We will use the fact that $\mathbb{C} = \langle 1, i\rangle$, and use this basis to talk about multiplication by $\alpha = a + bi \in \mathbb{C}$ as

$$(a+bi)(x+yi) = (ax-by) + (bx+ay)i = \begin{pmatrix} ax-by \\ bx+ay \end{pmatrix} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{C}.$$

In other words, $(-)\cdot\alpha \colon \mathbb{C} \to \mathbb{C}$ is an $\mathbb{R}$-linear map represented by a matrix with

$$\begin{vmatrix} a & -b \\ b & a \end{vmatrix} = a^2 + b^2 \in \mathbb{R}$$

and this determinant is independent of our choice of basis $\{1, i\}$. So this matrix representation of the multiplication map allows us to *define*

$$|\alpha|_{\mathbb{C}} := \left|\det\left(\mathbb{C} \xrightarrow{(-)\cdot\alpha} \mathbb{C}\right)\right|_{\infty}$$

Definition. Suppose L/K is a finite field extension. For each $\alpha \in L$, the **field norm from L to K**, $N_{L/K}\colon L \to K$, is defined by

$$N_{L/K}(\alpha) := \det\left(L \xrightarrow{(-)\cdot\alpha} L\right)$$

as a K-linear map.

A few comments:

1. This is well-defined precisely because $(-) \cdot \alpha$ is K-linear, by the distributive property in L, combined with the fact that determinants are basis-invariant.

2. Since the determinant is multiplicative, $N_{L/K}(\alpha\beta) = N_{L/K}(\alpha) \cdot N_{L/K}(\beta)$.

3. If $\alpha \in L$ happens to be in K, then

$$N_{L/K}(\alpha) = \det\begin{pmatrix} \alpha & & 0 \\ & \ddots & \\ 0 & & \alpha \end{pmatrix} = \alpha^{[L:K]}$$

Recall. Given a field K and an element $\alpha \in \overline{K}$ (where $\overline{K}$ denotes the algebraic closure of K), there exists a unique monic irreducible polynomial

$$\mu_{\alpha,K}(X) \in K[X]$$

called the **minimal polynomial** of α over K, which satisfies $\mu_{\alpha,K}(\alpha) = 0 \in \overline{K}$. The **conjugates** of α over K are the roots of $\mu_{\alpha,K}$ in $\overline{K}$ (possibly repeated). If the roots of $\mu_{\alpha,K}$ are all distinct, then $\mu_{\alpha,K}$ is called **separable**. The field $L = K(\alpha)$, the smallest subfield of $\overline{K}$ containing K and α, satisfies $[L : K] = \deg(\mu_{\alpha,K})$.

Proposition. *If $\mu_{\alpha,K}$ is separable, and $\{\alpha_1, \ldots, \alpha_n\} \subseteq L = K(\alpha)$ are the roots of $\mu_{\alpha,K}$, then $\mathrm{Gal}(L/K) = \mathrm{Aut}(L/K)$ can be written as $\{\sigma_1, \ldots, \sigma_n\}$ where each σ_i satisfies $\sigma_i(\alpha) = \alpha_i$.* ■

Lemma. *Let K be a field, $\alpha \in \overline{K}$. The following are true:*

(a) $N_{K(\alpha)/K}(\alpha) = (-1)^n a_0 = \prod_{i=1}^n \alpha_i$, *where $n = [L : K]$, a_0 is the constant term of $\mu_{\alpha,K}$, and $\{\alpha_1, \ldots, \alpha_n\}$ are the conjugates of α.*

(b) If L/K is any finite extension with $\alpha \in L$, then

$$N_{L/K}(\alpha) = \left(N_{K(\alpha)/K}(\alpha)\right)^{[L:K(\alpha)]}$$

Note that part (b) is a special case of what is known as the "transitivity of norm maps": if $K \hookrightarrow F \hookrightarrow L$ is a tower of field extensions, and $[L : K] < \infty$, then $N_{L/K} = N_{F/K} \circ N_{L/F}$.

Proof. To show (a), note that $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a basis for $K(\alpha)/K$ as a K-vector space. So multiplication by α shifts all of the associated column vectors:

$$\begin{pmatrix}1\\0\\0\\\vdots\\0\end{pmatrix} \xmapsto{(-)\cdot\alpha} \begin{pmatrix}0\\1\\0\\\vdots\\0\end{pmatrix} \xmapsto{(-)\cdot\alpha} \begin{pmatrix}0\\0\\1\\0\\\vdots\\0\end{pmatrix} \xmapsto{(-)\cdot\alpha} \cdots \xmapsto{(-)\cdot\alpha} \begin{pmatrix}0\\\vdots\\0\\1\end{pmatrix} \xmapsto{(-)\cdot\alpha} \begin{pmatrix}-a_0\\-a_1\\\vdots\\-a_{n-1}\end{pmatrix}$$

where $\{a_0, \ldots, a_{n-1}\}$ are the coefficients of $\mu_{\alpha,K}$. In this basis, the associated matrix of the K-linear map $(-)\cdot\alpha$ is given by

$$\begin{pmatrix}0 & 0 & \cdots & 0 & -a_0\\ 1 & 0 & \cdots & 0 & -a_1\\ 0 & 1 & \cdots & 0 & -a_2\\ 0 & 0 & \ddots & 0 & \vdots\\ 0 & 0 & \cdots & 1 & -a_{n-1}\end{pmatrix}$$

and the determinant of this map is $(-1)^n a_0$. ∎