Galois Theory 2018
Transitivity of Trace and Norm (non-examinable handout)

pmhw@dpmms.cam.ac.uk

Theorem (3.12)**.** *Let $M/L/K$ be finite extensions and $x \in M$. Then*

$$\mathrm{N}_{M/K}(x) = \mathrm{N}_{L/K}(\mathrm{N}_{M/L}(x)), \quad \mathrm{Tr}_{M/K}(x) = \mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(x))$$

For trace (which is easy) this was proved in the lectures.

In fact it is easier (as often happens!) to prove a more general statement. Suppose that V is a finite-dimensional vector space over L, and $u \colon V \to V$ is an L-endomorphism of V. Then u is also K-linear. Write $\det_L(u)$, $\mathrm{tr}_L(u)$ for the determinant/trace of u regarded as an endomorphism of the L-vector space V, and $\det_K(u)$, $\mathrm{tr}_K(u)$ for them when we view V as a K-vector space. Theorem 3.12 is the special case $V = M$, $u = \theta_x$ of:

Theorem. $\det_K(u) = \mathrm{N}_{L/K}\det_L(u)$ *and* $\mathrm{tr}_K(u) = \mathrm{Tr}_{L/K}\mathrm{tr}_L(u)$.

Proof. We first make an additional assumption: that u is *cyclic*, meaning that the $L[u]$-module V is cyclic. Recall (from IB GRM) that this means that there exists $e_0 \in V$ such that the elements

$$e_0,\ e_1 = u(e_1),\ \ldots,\ e_{n-1} = u^{n-1}(e_1) \quad (n = \dim_L V)$$

form a basis of V over L. Then we have

$$u^n(e_0) = -\sum_{i=0}^{n-1} a_i e_i, \quad a_i \in L$$

and $X^n + \sum_{i=0}^{n-1} a_i X^i \in L[X]$ is both the minimal and the characteristic polynomial of u. The matrix of u in terms of the basis (e_i) is

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

and so $\det_L(u) = (-1)^n a_0$, $\mathrm{tr}_L(u) = -a_{n-1}$. (Compare proof of 3.9.)

Now choose a basis $f_1, \ldots, f_m$ for L/K, and let $A_i \in M_n(K)$ be the matrix of T_{a_i}, the K-endomorphism $x \mapsto a_i x$ of L. Then the mn elements of V

$$e_0 f_1, \ldots, e_0 f_m, e_1 f_1, \ldots, e_{n-1} f_m$$

form a K-basis for V, and the matrix of u, as a K-endomorphism of V, with respect to this basis is

$$\begin{pmatrix} 0 & 0 & \dots & 0 & -A_0 \\ I_m & 0 & \dots & 0 & -A_1 \\ 0 & I_m & \dots & 0 & -A_2 \\ \vdots & & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & I_m & -A_{n-1} \end{pmatrix}$$

which has trace $-\mathrm{tr}(A_{n-1}) = -\mathrm{Tr}_{L/K}(a_{n-1}) = \mathrm{Tr}_{L/K}\mathrm{tr}_L(u)$ by the above.

Applying a cyclic permutation of the columns to the right m times, we see that its determinant is

$$(-1)^{m(mn-1)} \begin{vmatrix} -A_0 & 0 & \dots & 0 \\ -A_1 & I_m & \dots & 0 \\ \vdots & & \ddots & \vdots \\ -A_{n-1} & 0 & \dots & I_m \end{vmatrix} = (-1)^{mn}\det(A_0) = \mathrm{N}_{L/K}((-1)^m a_0).$$

This proves the theorem for a cyclic endomorphism.

In general, we know by module theory that V is a direct sum $\bigoplus V_i$ of cyclic $L[u]$-modules. Let u_i be the cyclic endomorphism of V_i thus obtained. Now, determinant is multiplicative for direct sums, and trace is additive. Since $\mathrm{N}_{L/K}$ is multiplicative and $\mathrm{Tr}_{L/K}$ is additive, we have

$$\det{}_K(u) = \prod_i \det{}_K(u_i) = \prod_i \mathrm{N}_{L/K}\det{}_L(u_i) = \mathrm{N}_{L/K}(\prod_i \det{}_L(u_i)) = \mathrm{N}_{L/K}\det{}_L(u)$$

and similarly for trace. $\square$

Characteristic polynomials. Replacing $M/L/K$ with $M(T)/L(T)/K(T)$, we can deduce that if $x \in M$, then

$$f_{x,M/K}(T) = N_{L(T)/K(T)} f_{x,M/L}(T)$$

where $f_{x,M/L} \in L[T]$ is the characteristic polynomial of the L-endomorphism θ_x of M.