MATH 594. NORM AND TRACE

An interesting application of Galois theory is to help us understand properties of two special constructions associated to field extensions, the *norm* and *trace*. If L/k is a finite extension, we define the norm and trace maps

$$\mathrm{N}_{L/k} : L \to k, \quad \mathrm{Tr}_{L/k} : L \to k$$

as follows: $\mathrm{N}_{L/k}(a) = \det(m_a)$, $\mathrm{Tr}_{L/k}(a) = \mathrm{trace}(m_a)$ where $m_a : L \to L$ is the k-linear map of multiplication by a. Since $m_a \circ m_{a'} = m_{aa'}$, $m_a + m_{a'} = m_{a+a'}$, and (for $c \in k$) $m_{ca} = c \cdot m_a$, the multiplicativity of determinants and the k-linearity of traces immediately implies that $\mathrm{N}_{L/k}$ is multiplicative and $\mathrm{Tr}_{L/k}$ is k-linear.

1. THE TRACE

For $a \in L$, if we build a k-basis of L by first picking a basis of $k(a)$ and then picking a basis of L over $k(a)$, we get a 'block' matrix for m_a in terms of which we deduce

$$\mathrm{Tr}_{L/k}(a) = [L : k(a)]\mathrm{Tr}_{k(a)/k}(a).$$

This shows that $\mathrm{Tr}_{L/k}(a)$ essentially only depends on $k(a)/k$ (which is intrinsic to a, or the minimal polynomial of a), up to the factor of $[L : k(a)]$. Hence, we deduce that this trace does *not* depend on how a is embedded into L. Actually, we can push this basic formula a bit further:

Lemma 1.1. *If L/k is not separable, then* $\mathrm{Tr}_{L/k} = 0$.

Proof. If L/k is not separable, then $p = \mathrm{char}(k) > 0$ and either $L/k(a)$ is not separable or else $k(a)/k$ is not separable. In the first case, $[L : k(a)]$ is divisible by $[L : k(a)]_i > 1$ in $\mathbf{Z}$ and so is divisible by p, whence $[L : k(a)] = 0$ in k. In the second case, the minimal polynomial for a over $k(a)$ has degree p^m for some $m \geq 1$ and the coefficient of T^{p^m-1} is 0, in which case $\mathrm{Tr}_{k(a)/k}(a) = 0$. In either case, we conclude from the formula preceding the lemma that $\mathrm{Tr}_{L/k}(a) = 0$. ■

Because of this lemma, the trace is interesting primarily in the separable case. Here Galois theory is helpful:

Theorem 1.2. *If L/k is separable and F/L is an extension which is normal over k, then for any $a \in L$ we have*

$$\mathrm{Tr}_{L/k}(a) = \sum \sigma(a),$$

where the sum in F is taken over all k-embeddings $\sigma : L \hookrightarrow F$.

Proof. Without loss of generality, we can replace F by the normal closure of L in F (relative to k) and so may assume that F is finite Galois over k. Clearly $\mathrm{Tr}_{k(a)/k}(a)$ is the sum of all distinct images of a under k-embeddings of $k(a)$ into F (hint: use that the characteritic polynomial for m_a on $k(a)$ is the minimal polynomial of a over k!!). Let $a' \in F$ be a k-conjugate of a. Make $k(a')$ an intermediate extension of L/k via the unique k-embedding sending a' to a. Note that $L/k(a')$ is separable. The number of k-embeddings of L into F which send a to a' is equal to $[L : k(a')]_s = [L : k(a')] = [L : k]/[k(a') : k]$, which is exactly $[L : k(a)]$ (since $[k(a') : k] = [k(a) : k]$). Now use the formula above Lemma 1.1 to get the proposed trace formula. ■

Combining our results in the separable and inseparable cases yields a basic transitivity property that holds without separability restrictions:

Corollary 1.3. *If $L'/L/k$ is a tower of finite extensions, then* $\mathrm{Tr}_{L'/k} = \mathrm{Tr}_{L/k} \circ \mathrm{Tr}_{L'/L}$.

Proof. If L'/k is not separable, then L'/L is not separable or L/k is not separable. In this case, both sides of the 'transitivity formula' are 0. Now suppose L'/k is separable, so L'/L and L/k are separable. Choose F/L' finite and Galois over k. Let $G = \mathrm{Gal}(F/k)$, $H' = \mathrm{Gal}(F/L')$, and $H = \mathrm{Gal}(F/L)$. By the theorem,

$$\mathrm{Tr}_{L'/k}(a) = \sum_{g \in G/H'} g(a),$$

where G/H' is the left coset space of H' in G and g is really running through a set of representatives for these cosets. Meanwhile,

$$\mathrm{Tr}_{L'/L}(a) = \sum_{g \in H/H'} g(a),$$

so

$$\mathrm{Tr}_{L/k}(\mathrm{Tr}_{L'/L}(a)) = \sum_{\gamma \in G/H} \gamma \left(\sum_{g \in H/H'} \gamma(g(a)) \right) = \sum_{\gamma \in G/H} \sum_{g \in H/H'} \gamma(g(a)).$$

As g runs through a set of left coset representatives for H/H' and γ runs through a set of left coset representatives for G/H, clearly γg runs through a set of left coset representatives for G/H'. This yields the formula. ∎

We now aim to show that when L/k is separable, then $\mathrm{Tr}_{L/k} : L \to k$ is *not* zero. There is a trivial case: if $[L : k]$ is non-zero in k, then since $\mathrm{Tr}_{L/k}(1) = \dim_k L = [L : k]$ is nonzero in k, this case is settled. Note that this takes care of characteristic 0. But of course what is more interesting is that even in positive characteristic, the trace is non-vanishing for separable extensions. Proving this (even uniformly across all characteristics at once) requires a better technique.

The key is to introduce a concept called *discriminant*. If $E = \{e_1, \dots, e_n\}$ is a k-basis of L, we get a natural symmetric k-valued k-bilinear form on L via $(x, y) \mapsto \mathrm{Tr}_{L/k}(xy)$. This bilinear form can be described by a matrix $M_E = (\mathrm{Tr}_{L/k}(e_i e_j))$ depending on the basis E, and recall that when we change E to some other ordered basis E' then $M_{E'} = T M_E T^t$ where T is the change of basis matrix from E to E'. Hence, $\det(M_{E'}) = \det(T)^2 \det(M_E)$. Although $\det(M_E)$ is not independent of E, we see that *up to* $(k^\times)^2$*-multiple* it is well-defined. In particular, whether or not $\det(M_E)$ vanishes is independent of E, and when such non-vanishing happens we get an element $d_{L/k} \in k^\times/(k^\times)^2$ which *is* intrinsic to L/k. This resulting element is called the *discriminant* of L over k (and in the other cases when $\det(M_E) = 0$ for all E, we say "the discriminant vanishes").

Now we can prove the desired result:

Theorem 1.4. *If L/k is separable, then $\mathrm{Tr}_{L/k}$ is nonzero.*

Proof. By transitivity, we can pass to a separable extension on L and hence may assume L/k is Galois. By the primitive element theorem, $L = k(\alpha)$ for some α. Let $f_\alpha \in k[T]$ be the minimal polynomial of α. Consider the basis $E = \{1, \alpha, \dots\}$ given by powers of α. It suffices to prove $\det(M_E) \neq 0$, since the vanishing of trace would force $M_E = 0$.

Using the trace formula in terms of Galois theory, as proven above, the matrix M_E has ij entry given by

$$\mathrm{Tr}_{L/k}(\alpha^i \alpha^j) = \sum_g g(\alpha)^{i+j},$$

where g runs over all k-embeddings of L into L, which is to say g runs over $\mathrm{Gal}(L/k)$. But as we saw in class, the determinant of this matrix is equal to the discriminant of the polynomial f_α. That is, it is equal to $\prod(g(\alpha) - h(\alpha))$ and g, h run over (unordered) pairs of distinct elements of $\mathrm{Gal}(L/k)$. This product is visibly nonzero, since α is a primitive element for the Galois extension L/k! ∎

2. The norm

Having developed the additive side of the theory, we now turn to the multplicative side, the norm. Since $\mathrm{N}_{L/k}(1) = 1$, we get a group homomorphism $\mathrm{N}_{L/k} : L^\times \to k^\times$. One has the formula $\mathrm{N}_{L/k}(a) = \mathrm{N}_{k(a)/k}(a)^{[L:k(a)]}$ for any $a \in L$, a multiplicative version of the formula for traces preceding Lemma 1.1, and the proof goes in the exact same way. Likewise, one gets a formula in the separable case in terms of forming *products*: $\mathrm{N}_{L/k}(a) = \prod \sigma(a)$ inside of a normal extension F/k containing L, where σ runs over k-embeddings of L into F.

The hard part of the theory of the norm is transitivity. The reason is that in the case of the trace, the inseparable theory was silly (the zero map), so everything came down to the separable case where we had a nice clean formula in terms of Galois conjugates and group theory! But for the norm we really have to do some work: the norm is *not* identically 1 on $L^\times$ even in the purely inseparable case.

Example 2.1. Assume k is non-perfect of characteristic $p > 0$, and $a \in k$ is not a pth power (e.g., $k = \mathbf{F}_p(t)$ and $a = t$). Let $L = k(a^{1/p})$. What is $\mathrm{N}_{L/k}(a^{1/p})$? I claim this is equal to a. To check such an equality, it suffices to check after raising both sides to the pth power (due to *uniqueness* of pth roots in characteristic p). But $\mathrm{N}_{L/k}$ is multiplicative, so we're reduced to showing $\mathrm{N}_{L/k}(a) = a^p$. But this is clear: $m_a : L \to L$ is just $a \cdot \mathrm{id}_L$, whose determinant is $a^{[L:k]} = a^p$.

With the explanation of the difficulty given, we now prove the transitivity:

Theorem 2.2. *Let $L'/L/k$ be a tower of finite extensions. Then $\mathrm{N}_{L'/k} = \mathrm{N}_{L/k} \circ \mathrm{N}_{L'/L}$.*

Proof. We have to give an alternative formula for the norm. The formula is:

$$\mathrm{N}_{L/k}(a) = \left(\prod g(a)\right)^{[L:k]_i},$$

where g runs over the distinct k-embeddings of L into a normal extension F of L (the addititive version would say $\mathrm{Tr}_{L/k}(a) = [L : k]_i \cdot \sum g(a)$, and this is *easy* to prove from what we have shown above: in the separable case it is our old Galois-theoretic trace formula, and in the inseparable case it is zero). To prove this norm formula, note that in the separable case it is just the product formula we have recorded earlier. Thus, we may assume $[L : k]_i > 1$, so in particular we are in characteristic $p > 0$. In this case, it suffices to check our formula after raising both sides to an arbitrary p-power. But both sides are multiplicative in a, so if we raise to the power $[k(a) : k]_i$ and recall that from HW 11, Exercise 7 (or direct arguments) that $a^{[k(a):k]_i}$ is separable over k, we get to the case in which a is separable over k. Thus, $k(a)$ lies inside of the maximal subextension $K \subseteq L$ which is separable over k.

Clearly the k-embeddings of L into a fixed normal extension F/k which admits *some* k-embedding of L are in bijection with the k-embeddings of K (since L/K is purely inseparable, so once K is k-embedded into F the extension of this to a k-embedding of L can be done in exactly one way). Thus, the right side of our putative norm formula is just

$$\left(\prod_{\gamma \in \mathrm{Gal}(K/k)} g(a)\right)^{[L:K]},$$

since $[L : k]_i = [L : K]$ by definition of "inseparable degree". On the other hand, if we compute the determinant of the multiplication map by a on L by first building a basis of K over k and then picking a basis of L over K, we get a block matrix with $[L : K]$ blocks down the diagonal which are all just the matrix for multiplication by a on K. Thus, since the determinant of such a block form is the $[L : K]$th power of the determinant of the common block, we get $\mathrm{N}_{L/k}(a) = \mathrm{N}_{K/k}(a)^{[L:K]}$. Hence, we are reduced to the formula $\mathrm{N}_{K/k}(a) = \prod_g g(a)$ with g running over $\mathrm{Gal}(K/k)$, and this is already known.

Now that we have a new formula for the norm, we can use it. The advantage of this formula is that the inseparability aspect is entirely hidden in the exponent $[L : k]_i$, and we know that inseparable degrees are multiplicative in towers. This will enable us to circumvent the difficulty one encounters by trying to directly attack the transitivity problem by expressing field extensions as "inseparable on top of a separable" (an approach which quickly hits the snag that in a tower we cannot necessarily put the separable piece of the second stage of the tower "below" the inseparable piece on top of the first stage of the tower).

For a given tower $L'/L/k$ for which we want to prove transitivity, choose an extension F/L' which is normal over k. Thus, by multiplicativity of $\mathrm{N}_{L/k}$ and our "new" norm formula applied to L'/L, we get

$$\mathrm{N}_{L/k}(\mathrm{N}_{L'/L}(a)) = \mathrm{N}_{L/k}\left(\prod_g g(a)\right)^{[L':L]_i}$$

for $a \in L'$, where g runs over all L-embeddings of L' into F (recall that we are giving ourselves at the outset a preferred embedding j' of L' into F, and this is what we use to single out a preferred embedding j_0 of L

into F over k so as to compute $\mathrm{N}_{L'/L}$ inside of F; that is, all g's are over j_0). Now using multiplicativity some more, we get

$$\mathrm{N}_{L/k}(\mathrm{N}_{L'/L}(a)) = \prod_{j:L\hookrightarrow F} jj_0^{-1}\left(\prod_g g(a))\right)^{[L':L]_i[L:k]_i} = \prod_{\sigma\in\mathrm{Aut}(j_0(L)/k)} \sigma\left(\prod_{g:L'\hookrightarrow F} g(a)\right)^{[L':k]_i}.$$

The k-automorphisms of $j_0(L)$ have the form $j_0 \circ \tau \circ j_0^{-1}$ as τ runs over the k-automorphisms of L (where $j_0 : L \to j_0(L)$ is an isomorphism). Using this, it becomes a pleasant exercise with properties of normal extensions to check that the iterated product is equal to $\prod_{h:L'\hookrightarrow F} h(a)$, so we recover $\mathrm{N}_{L/k}(a)$, as desired. ∎