Math 248A. 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 imply that $\mathrm{N}_{L/k}$ is multiplicative and $\mathrm{Tr}_{L/k}$ is k-linear.

1. Examples

To get a feel for the norm and trace, let's work it out in the simplest case of a separable quadratic extension of fields L/k. We will see that (roughly speaking, and ignoring signs which depend on the field degree) the norm is the constant term of a minimal polynomial and the trace is the second-highest coefficient of a minimal polynomial. This concrete viewpoint is how norms and traces arise very often, but the general concept as defined above is a bit more subtle than this and provide a theory with much better properties than such a naive viewpoint would suggest.

One important point is that for a higher-degree field extension it is generally a pain (and not very informative) to work out explicit formulas for the norm and trace "by hand". Already for cubic fields it can be a pain. But the quadratic case is very useful in practice, as well as algebraically not too complicated, as we shall now see.

Since L/k is separable (or because its degree is so small) there is a primitive element α, which is to say $L = k(\alpha)$, so since $[L : k] = 2$ we see that $\{1, \alpha\}$ is an ordered k-basis of L. Let $f(T) = T^2 + aT + b \in k[T]$ denote the minimal polynomial of α, so the multiplication law of L is governed by the condition $\alpha^2 = -b \cdot 1 - a \cdot \alpha$. In other words, if $\beta = x + y\alpha \in L$ is an arbitrary element (with $x, y \in k$) then we compute that relative to the ordered k-basis $\{1, \alpha\}$ the multiplication map $m_\beta : L \to L$ has matrix

$$\begin{pmatrix} x & -by \\ y & x - ay \end{pmatrix}$$

since $\beta \cdot 1 = x + y\alpha$ and $\beta \cdot \alpha = x\alpha + y\alpha^2 = -by + (x - ay)\alpha$. Thus, for $\beta = x + y\alpha$ with $x, y \in k$ we have

$$\mathrm{Tr}_{L/k}(\beta) = 2x - ay, \quad \mathrm{N}_{L/k}(\beta) = x^2 - axy + by^2.$$

This may look like a mess, but note that if $\sigma \in \mathrm{Gal}(L/k)$ denotes the nontrivial element (so $\alpha + \sigma(\alpha) = -a$ and $\alpha \cdot \sigma(\alpha) = b$, since $T^2 + aT + b = (T - \alpha)(T - \sigma(\alpha))$ is the minimal polynomial of α over k) then

$$\beta + \sigma(\beta) = (x + y\alpha) + (x + y\sigma(\alpha)) = (x + y\alpha) + (x + y(-a - \alpha)) = 2x - ay = \mathrm{Tr}_{L/k}(\beta),$$

$$\beta \cdot \sigma(\beta) = (x + y\alpha)(x + y\sigma(\alpha)) = x^2 + xy(\alpha + \sigma(\alpha)) + y^2\alpha \cdot \sigma(\alpha) = x^2 - axy + by^2 = \mathrm{N}_{L/k}(\beta),$$

so in other words

$$(T - \beta)(T - \sigma(\beta)) = T^2 - (\mathrm{Tr}_{L/k}(\beta))T + \mathrm{N}_{L/k}(\beta) \in k[T].$$

This is a monic quadratic polynomial over k which visibly has β as a root, and so as long as $\beta \notin k$ (i.e., $y \neq 0$) it is the minimal polynomial for β over k. In other words, if $\beta \notin k$ (or equivalently, in terms that generalize to the higher-degree case, if $K = k(\beta)$) then in fact $\mathrm{Tr}_{L/k}(\beta)$ and $\mathrm{N}_{L/k}(\beta)$ are (up to sign) the second-highest coefficient and constant term of its minimal polynomial over k. On the other hand if $\beta \in k$ (i.e., $\beta = x$ and $y = 0$) then $\mathrm{Tr}_{L/k}(\beta) = 2x = 2\beta$ and $\mathrm{N}_{L/k}(\beta) = x^2 = \beta^2$.

These connections of the trace and norm to coefficients of minimal polynomials as well as to sums and products of Galois conjugates over k are the ones which we shall show hold rather generally. When trying to work with Galois conjugates (when L/k is separable) we will need to exercise some care in case L/k is not itself Galois.

2. 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 consisting of $[L : k(a)]$ copies of the smaller square matrix for $m_a : k(a) \to k(a)$ along the main diagonal, so

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

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 over k. Actually, we can push this basic formula a bit further. First, we work out a special case:

Lemma 2.1. *If $f(T) = T^n + c_{n-1}T^{n-1} + \cdots + c_0 \in k[T]$ is the minimal polynomial of a over k then $\mathrm{Tr}_{k(a)/k} = -c_{n-1}$. In other words, this trace is the negative of the second-highest coefficient of the minimal polynomial of a over k.*

Beware that this lemma rests on the fact that the top field for the trace is $k(a)$ and not a larger field.

Proof. The case $n = 1$ is trivial, so we may assume $n \geq 2$. Consider the ordered k-basis $\{1, a, \ldots, a^{n-1}\}$ of $k(a)$. The matrix for the multiplication map $m_a : k(a) \to k(a)$ relative to this basis is as follows: 1's immediately below the main diagonal (since $m_a(a^i) = a^{i+1}$ for $0 \leq i \leq n-2$) and 0's everywhere else except for the final column, which consists of the $-c_j$'s for increasing $0 \leq j \leq n-1$ since

$$m_a(a^{n-1}) = a^n = -c_0 \cdot 1 - c_1 a - \cdots - c_{n-1}a^{n-1}.$$

In particular, the bottom right entry of the matrix is $-c_{n-1}$, and all other diagonal entries vanish. Hence, the trace of the matrix is as desired. ∎

Lemma 2.2. *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 the inseparability degree $[L : k(a)]_i > 1$ in $\mathbf{Z}$ and so is divisible by p, whence $[L : k(a)] = 0$ in k. In the second case, the minimal polynomial f for a over k is a polynomial in T^p, so no monomials of consecutive positive degrees appear in f. Hence, by Lemma 2.1 we get $\mathrm{Tr}_{k(a)/k}(a) = 0$. 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 2.3. *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. We will first focus on $\mathrm{Tr}_{k(a)/k}(a)$ and then use this to get our hands on $\mathrm{Tr}_{L/k}(a)$ (since $k(a)$ may be a proper subfield of L).

By Lemma 2.1, $\mathrm{Tr}_{k(a)/k}(a)$ is the negative of the second-highest coefficient of the minimal polynomial of a over k. But by factoring this polynomial over the Galois extension F/k (where it splits completely) we can identify this second-highest coefficient with the negative of the sum of the roots of the polynomial in F, which is to say the negative of the sum of the k-conjugates of a. To summarize (after canceling the sign), $\mathrm{Tr}_{k(a)/k}(a) \in k$ is the sum of the k-conjugates of a in F, which is to say the sum of the images of a under k-embeddings of $k(a)$ into F.

Consider the various k-embeddings of L into F. Such an embedding can be built up in two stages: first we figure out what to do on $k(a)$, and then the chosen k-embedding $j : k(a) \to F$ is lifted to an embedding $L \to F$. The choices for j are easy to describe: we simply send a to one of its k-conjugates (i.e., roots in F of its minimal polynomial over k, which splits completely in F), and we can use whatever such k-conjugate we

wish. Since there is an embedding of L into F over k, once we have fixed a choice of j, say with $j(a) = a'$, the number of liftings of this to embeddings $L \to F$ is $[L : k(a)]$. Hence, in the proposed summation formula each $\sigma(a) = a'$ really appears $[L : k(a)]$ times, and so the proposed formula is just $[L : k(a)] \sum_{j:k(a)\to k} j(a)$, which is $[L : k(a)]\mathrm{Tr}_{k(a)/k}(a) = \mathrm{Tr}_{L/k}(a)$. ■

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

Corollary 2.4. *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, such as for finite fields, 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 $E = \{e_1, \ldots, e_n\}$ 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 $M_{E'} = TM_E T^t$ 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 2.5. *If L/k is separable, then $\mathrm{Tr}_{L/k}$ is nonzero.*

Proof. Let L'/L be a Galois closure of L/k. Since $\mathrm{Tr}_{L'/k} = \mathrm{Tr}_{L/k} \circ \mathrm{Tr}_{L'/L}$, if $\mathrm{Tr}_{L/k}$ were to be identically zero then $\mathrm{Tr}_{L'/k}$ would vanish as well. Hence, to prove the desired non-vanishing result it suffices to treat L'/k instead of L/k. In other words, we 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 $E = \{1, \alpha, \ldots \alpha^{n-1}\}$ given by powers of α (with $n = [L : k]$). It suffices to prove $\det(M_E) \neq 0$, since the vanishing of trace would force $M_E = 0$ (by definition of M_E) and so would yield a contradiction.

We shall label the rows and columns of M_E by integers from 0 to $n-1$. 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 quite generally, if $\{x_0, \ldots, x_{n-1}\}$ is a finite ordered set of elements in a field (such as the $g(\alpha)$'s in L for a choice of ordering of the g's) the matrix M with ij-entry $\sum_r x_r^{i+j}$ has the form $M = TT^t$ with T the matrix whose ij-entry is $t_{ij} = x_j^i$; indeed,

$$(TT^t)_{ij} = \sum T_{ir}(T^t)_{rj} = \sum t_{ir}t_{jr} = \sum_r x_r^{i+j} = M_{ij}.$$

Hence, $\det M = (\det T)^2$ and $\det T$ is computed by vanderMonde's formula $\prod_{r<s}(x_s - x_r)$, so

$$\det M = \prod_{r<s}(x_s - x_r)^2 = (-1)^{n(n-1)/2}\prod_{\{r,s\}}(x_s - x_r)$$

with the final product taken over *unordered* pairs of distinct integers $0 \leq r, s \leq n-1$.

We conclude that $\det M_E = (-1)^{n(n-1)/2}\prod(g(\alpha) - h(\alpha))$ and g, h run over (unordered) pairs of distinct elements of $\mathrm{Gal}(L/k)$. This expression, called the *discriminant* of f_α, is visibly nonzero since α is a primitive element for the Galois extension L/k (so if $g \neq h$ then necessarily $g(\alpha) \neq h(\alpha)$)! ■

3. 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 2.1, 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 $L^\times$ in the purely inseparable case.

Example 3.1. 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 $a \cdot \mathrm{id}_L$ (i.e., a diagonal matrix whose diagonal entries are all equal to a), whose determinant is $a^{[L:k]} = a^p$.

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

Theorem 3.2. *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 and $[L:k]_i$ denotes the inseparable degree of L/k (equal to 1 in the separable case). This is analogous to the additive claim that $\mathrm{Tr}_{L/k}(a) = [L:k]_i \cdot \sum g(a)$, 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 alternative 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 observe 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

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

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

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

where g ranges over all embeddings $L' \to F$ over $j_0 : L \to F$ (so $(\prod g(a))^{[L':L]_i} \in j_0(L)$ inside of F) and j ranges through all k-embeddings of L into F.

As we vary j, the maps $j j_0^{-1} : j_0(L) \to F$ vary (without repetition) through all k-embeddings of $j_0(L)$ into F; for example, with $j = j_0$ we recover the subfield inclusion of $j_0(L)$ into F. Since F is normal over k and $j_0(L)$ is a subfield of F containing k, every k-embedding of $j_0(L)$ into F is induced by a k-automorphism τ of F. Moreover, two k-automorphisms τ and τ' of F have the same restriction to $j_0(L)$ if and only if τ and τ' lie in the same coset of $\mathrm{Aut}_k(F)/\mathrm{Aut}_{j_0(L)}(F)$. Thus, if $\{\tau_r\}$ is a set of coset representatives for this coset space then for each $a \in L'$ we have

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

We wish to show that the right side is $(\prod_h h(a))^{[L':k]_i}$, with h ranging through all k-embeddings of L' into F, as this final expression is our "new" formula for $\mathrm{N}_{L'/k}(a)$. Since $[L':L]_i[L:k]_i = [L':k]_i$, we are reduced to proving that $\prod_r \prod_g \tau_r(g(a)) = \prod_h h(a)$, with $\{\tau_r\}$ a set of coset representatives for $\mathrm{Aut}_k(F)/\mathrm{Aut}_{j_0(L)}(F)$, g ranging through all embeddings of L' into F over $j_0 : L \to F$, and h ranging through all k-embeddings of L' into F. Thus, it suffices to show that the composite k-embeddings $\tau_r \circ g : L' \to F$ range without repetition through the set of all k-embeddings h of L' into F as we independently vary τ_r and g. First we check that

there are no repetitions in this list. Since each g is the identity map on $j_0(L)$, each map $\tau_r \circ g : L' \to F$ has the same restriction to $j_0(L)$ as does τ_r and so each such composite map determines the coset of τ_r in $\mathrm{Aut}_k(F)/\mathrm{Aut}_{j_0(L)}(F)$. But the τ_r's are a set of representatives for this coset space, so we conclude that if $\tau_r \circ g = \tau_{r'} \circ g'$ as k-embeddings of L' into F then $r = r'$ and hence (since τ_r is an automorphism of F) $g = g'$. The number of τ_r's is

$$\#\mathrm{Aut}_k(F)/\#\mathrm{Aut}_{j_0(L)}(F) = [F : k]_s/[F : j_0(L)]_s = [j_0(L) : k]_s = [L : k]_s$$

and the number of g's is $[L' : L]_s$, so the collection of distinct k-embeddings $\tau_r \circ g : L' \to F$ consists of $[L' : L]_s[L : k]_s$ maps. But $[L' : L]_s[L : k]_s = [L' : k]_s$ is exactly the number of k-embeddings $h : L' \to F$ since F is a normal extension of k into which L' admits *some* k-embedding, so we have exhausted all such maps h without repetition, as desired. ■