Math 250A Lecture 24 Notes

Daniel Raban

November 21, 2017

1 Norm and Trace

1.1 Norm and trace of finitely generated extensions

Let L/K be a field extension. The norm and the trace satisfy

$$N(ab) = N(a)N(b)$$

$$\operatorname{tr}(a+b) = \operatorname{tr}(a) + \operatorname{tr}(b),$$

so we can think of the norm and trace as homomorphisms $L^* \to K^*$ under $\times$ and $L \to K$ under $+$, respectively.

Suppose a generates L/K ($L = K(a)$). a satisfies an irreducible polynomial $x^n + b_{n-1}x^{n-1} + \cdots + b_0 = 0$. What are the trace and norm of a? Choose a basis for L over K, say $\{1, a, a^2, \ldots, a^{n-1}\}$. Then multiplying by a makes $1 \mapsto a$, $a \mapsto a^2$, ... So a is given by the matrix

$$\begin{bmatrix} 0 & 0 & \cdots & 0 & -b_0 \\ 1 & 0 & \cdots & 0 & -b_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -b_{n-2} \\ 0 & \cdots & 0 & 1 & -b_{n-1} \end{bmatrix}.$$

The trace is $-b_{n-1}$,and the norm is $\pm b_0$.

Suppose the polynomial has roots $a = a_1, a_2, \ldots, a_n$ in an algebraic closure of L. Then $b_{n-1} =_1 + \cdots + a_n$, and $b_0 = \pm a_1, \ldots a_n$. So the trace is the sum of the roots of the polynomial, and the norm is the product of the roots.

Example 1.1. In $\mathbb{C}/\mathbb{R}$, we have

$$\operatorname{tr}(z) = z + \bar{z}$$

$$N(z) = z\bar{z}.$$

Suppose we have $K \subseteq K(a) \subseteq L$. Then $N(a)$ in L is $(N(a)(\text{in } K(a)))^{[L:K(a)]}$ and $\text{tr}(a)$ in L is $(\text{tr}(a)(\text{in } K(a))) \cdot [L : K(a)]$ (exercise).

Suppose $L : K$ is Galois with group G, then other roots are given by $\sigma_i(a)$ for $\sigma \in G$, so

$$N(a) = \prod_{\sigma \in G} \sigma(a),$$

$$\text{tr}(a) = \sum_{\sigma \in G} \sigma(a).$$

1.2 The integers of a quadratic field

Recall that $\mathbb{Q}[\sqrt{-3}]$ contains the ring $\mathbb{Z}[\sqrt{-3}]$, which is not a UFD since $4 = 2 \times 2 = (1 + \sqrt{-3})(1 - \sqrt{3})$. It is also contained in $\mathbb{Z}[\frac{\sqrt{-3}+1}{2}]$, the Eisenstein integers, which is a UFD.

Given a field L containing $\mathbb{Q}$, what is a "nice" ring in it? The answer is that this is the ring of algebraic integers in K.

Definition 1.1. The ring of *algebraic integers* in K is the ring of elements in a field $K/\mathbb{Q}$ that are roots of polynomials in $\mathbb{Z}[x]$ with leading coefficient 1.

Proposition 1.1. *Let $L/\mathbb{Q}$ be a finite extension. Then for $\alpha \in L$, the following are equivalent:*

1. *α is algebraically independent (root of $x^n + \cdots = 0$).*
2. *We can find a finitely generated $\mathbb{Z}$-module A in L spanning L so that $\alpha A \subseteq A$.*

Proof. (1) $\implies$ (2): Take A to be spanned by $1, \alpha, \alpha^2, \ldots, a^{n-1}$. Then $\alpha\alpha^{n-1}$ is a linear combination of $1, \alpha, \alpha^2, \ldots, a^{n-1}$.

(2) $\implies$ (1): α is a linear transformation of a free $\mathbb{Z}$-module A. α is a root of its characteristic polynomial, which has leading coefficient 1 and other roots in $\mathbb{Z}$. □

Suppose $L = \mathbb{Q}(\sqrt{N})$, where N is a squarefree integer. We want to find the algebraic integers in L. The easiest examples are $m + n\sqrt{N}$, for $m, n \in \mathbb{Z}$. Sometimes, there are others, such as $\frac{\sqrt{3}+1}{2}$. The key point is that if α is an algebraic integer, so are $\text{tr}(\alpha)$ and $N(\alpha)$. So $\text{tr}(\alpha), N(\alpha) \in \mathbb{Z}$.

What are the norm and trace of $m + n\sqrt{N}$? Choose the basis $\left\{1, \sqrt{N}\right\}$ for $L/\mathbb{Q}$. Multiplying by m makes $1 \mapsto m$ and $\sqrt{N} \mapsto m\sqrt{N}$, and multiplying by $n\sqrt{N}$ makes $1 \mapsto n\sqrt{N}$ and $\sqrt{N} \mapsto nN$. So we get the matrix

$$\begin{bmatrix} m & nN \\ n & m \end{bmatrix}.$$

These must be in $\mathbb{Z}$. $2m \in \mathbb{Z}$ makes $m \in \mathbb{Z}$, so $m^2 - n^2 \in \mathbb{Z}$. So $n \in \mathbb{Z}$, as n is squarefree. The other case is that $m \in \mathbb{Z} + 1/2$, so $m^2 = k + 1/4$. We need $m^2 - n^N \in \mathbb{Z}$, which is $1/4 - 4n^2 \in \mathbb{Z}$. So $1 \equiv (2n)^2 N \pmod 4$. If $N \equiv 2, 3 \pmod 4$, we have no solutions. So we must have $N \equiv 1 \pmod 4$. The integerrs of $\mathbb{Q}(\sqrt{N})$ are given by $\mathbb{Z}[\sqrt{N}]$ if $n \equiv 2, 3 \pmod 4$, and $\mathbb{Z}[\frac{1+\sqrt{N}}{2}]$ if $n \equiv 1 \pmod 4$.

The trace gives us a bilinear form on L/K with $(a, b) = \mathrm{tr}(ab)$. This is either 0 or nondegenerate.

Example 1.2. Here is an example when $(\cdot, \cdot)$ is zero. Let $K - F_p(t^p)$ and $L = F_p(t)$. $K \subseteq L$ and this is an inseparable extension. Any element of L is the root of an equation of the form $x^p - a$ for $a \in K$, where the coefficient of $x^{p-1} = 0$. This coefficient in the trace, so the trace is always 0.

For separable extensions L/K, the trace is not identically 0. This is trivial in characteristic 0 because $\mathrm{tr}(1) = [L : k] \neq 0$.

Definition 1.2. A *character* of a group G is a homomorphism from $G \to K^*$ (a "1-dimensional representation" of G).

Lemma 1.1 (Artin)**.** *Suppose G is a group (or monoid) and K is a field. If $\chi_1, \chi_2, \ldots, \chi_n$ are distinct characters, they are linearly independent; i.e. if*

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

for all $g \in G$, then $a_1 = a_2 = \cdots = a_n = 0$.

Proof. Suppose $a_1\chi_1(g) + a_2\chi_2(g) + \cdots + a_n\chi_n(g) = 0$ for all g. Pick all a_i to be not all zero and n to be as small as possible. Since $\chi_1 \neq \chi_2$, pick $h \in G$ with $\chi_1(h) \neq \chi_2(h)$. Then

$$a_1\chi_1(gh) + a_2\chi_2(gh) + \cdots + a_n\chi_n(gh) = 0$$

for all g, which means that

$$a_1\chi_1(g)\chi_1(h) + a_2\chi_2(g)\chi_2(h) + \cdots + a_n\chi_n(g)\chi_n(h) = 0.$$

If we multiply the original relation by $\chi_1(h)$, we get

$$a_1\chi_1(g)\chi_1(h) + a_2\chi_2(g)\chi_1(h) + \cdots + a_n\chi_n(g)\chi_1(h) = 0$$

If we subtract these two equations, we get

$$a_2(\chi_1(h) - \chi_2(h))\chi_2(g) + a_3(\chi_1(h) - \chi_3(h))\chi_3(g) + \cdots + a_n(\chi_1(h) - \chi_n(h))\chi_n(g) = 0.$$

Note that $\chi_1(h) - \chi_2(h) \neq 0$. So we have a smaller nonzero linear relation between $\chi_1, \ldots, \chi_n$, which is a contradiction since we chose n to be as small as possible. $\square$

Proposition 1.2. *For a Galois extension L/K, the trace is not identically zero.*

Proof. We have that the trace is $\mathrm{tr}(a) = \sigma_1(a) + \sigma_2(a) + \cdots + \sigma_n(a)$ with $\sigma_i \in G$. If $\mathrm{tr}(a) = 0$ for all a, we have a linear relation between $\sigma_1, \ldots, \sigma_n$. This is not possible by Artin's lemma. So $\mathrm{tr}(a) \neq 0$ for some a. Separable extensions are similar and we leave that case as an exercise. □

1.3 Discriminant of a field extension L/K

Definition 1.3. The *discriminant* of L/K is the discriminant of the bilinear form $(a, b) = \mathrm{tr}(ab)$ on the vector space L.

Choose a basis $\{a_1, \ldots, a_n\}$ for L over K. The discriminant is $\det(B)$, where $B_{i,j} = (a_i, a_j)$. This depends on the choice of basis. If $\{b_1, \ldots, b_n\}$ is another basis, then some matrix times A gives a change of basis from $a_1, \ldots, a_n$ to $b_1, \ldots, b_n$. The discriminant for the bases is the discriminant for $b_1, \ldots, b_n$ times the determinant of A. So the discriminant is well-defined up to multiplication by squares of K. So $\mathrm{disc}(L/K) \in K^*/(K^*)^2$.

Example 1.3. Suppose $L = K(a)$. What is the discriminant of L/K? The element a is a root of some irreducible polynomial $p(a)$. Choose the basis $1, a, a^2, \ldots, a^{n-1}$ of L/K. The discriminant is equal to the determinant of

$$\begin{bmatrix} \mathrm{tr}(1) & \mathrm{tr}(a) & \mathrm{tr}(a^2) & \cdots & \mathrm{tr}(a^{n-1}) \\ \mathrm{tr}(a) & \mathrm{tr}(a^2) & \ddots & & \\ \vdots & \vdots & & & \end{bmatrix}$$

Assume L/K is Galois for simplicity. Then $\mathrm{tr}(a^k) = \sum_{\sigma \in G} \sigma(a^k)$, so we get

$$\begin{bmatrix} \sum \sigma(1 \cdot 1) & \sum \sigma(1 \cdot a) & \sum \sigma(1 \cdot a^2) & \cdots & \mathrm{tr}(a^{n-1}) \\ \sum \sigma(1 \cdot a) & \sum \sigma(1 \cdot a^2) & \ddots & & \\ \vdots & \vdots & & & \end{bmatrix}$$

This is the product of the matrices

$$\begin{bmatrix} \sigma_1(1) & \sigma_2(1) & \sigma_3(1) & \cdots & \sigma_n(1) \\ \sigma_1(a) & \sigma_2(a) & \ddots & & \\ \vdots & \vdots & & & \end{bmatrix} \begin{bmatrix} \sigma_1(1) & \sigma_1(a) & \sigma_1(a^2) & \cdots & \sigma_1(a^{n-1}) \\ \sigma_2(1) & \sigma_2(a) & \ddots & & \\ \vdots & \vdots & & & \end{bmatrix}$$

which are transposes of each other.

Recall the Vandemonde determinant

$$\det \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ a & b & c & \cdots & \\ a^2 & b^2 & c^2 & \cdots & \\ \vdots & \vdots & \vdots & \ddots & \\ a^{n-1} & b^{n-1} & c^{n-1} & \cdots & \end{bmatrix} = \pm(a-b)(a-c)(a-d)(a-e)\cdots(b-c)(b-a)\cdots,$$

which is the product of the differences of different variables (where each difference is only counted once). These are equal because the degrees are the same, and the left side is divisible by $a-b$ (and other terms) as if $a=b$, the the first two columns are the same. So they differ up to a constant, which is 1.

So the discriminant is the square of the determinant $\Delta = \pm\prod_{i<j}(\sigma_i(a)-\sigma_j(a))$. So Δ^2 is the discriminant of the polynomial $p(x)$. This means that the discriminant of the field extension is jist the discriminant of the irreudicible polynomial of a.

1.4 Applications of the discriminant of a field extension

Example 1.4. Look at the fields $\mathbb{Q}[x]/(x^2+x+1)$, $\mathbb{Q}[x]/(x_x^3-1)$, and $\mathbb{Q}[x]/(x^3-x+1)$. Which are isomorphic? The discriminants are -31, -31, and -23; remember to think of these as elements of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$. The third differs from the first two; $-23/-31$ is not a square in $\mathbb{Q}^*$. The first two fields are isomorphic; change x to $-x$.

Example 1.5. Let's find algebraic integers in $L=\mathbb{Q}(\alpha)$, where $\alpha^2+\alpha+1=0$. Look at the discriminant of the basis $\{1,\alpha,\alpha^2\}$. The discriminant os -31. Let A be the $\mathbb{Z}$-linear span of $1,\alpha,\alpha^2$. Suppose B is the set of all algebraic integers. So $A\subseteq B$. $\operatorname{disc}(B) = \operatorname{disc}(A)\times\det(x)^2$, where x is the matrix taking the basis of A to the basis of B. The determinant is the order of the group B/A. Now note that -31 is squarefree. Then $\det(x)=1$, so $B=A$.

Example 1.6. Take $\mathbb{Q}(\sqrt{-3})$, so $\alpha=\sqrt{-3}$ and $\alpha^3+3=0$. This has discriminant -12, which is not squarefree. We have $\mathbb{Z}[\alpha]\subsetneq\mathbb{Z}[\frac{\sqrt{-3}+1}{2}]$, so you have to do more work.

Recall that the norm is a homomorphism $L^*\to K^*$. What are the kernel and the image of this map? These can be quite complicated.

Example 1.7. Look at $N:\mathbb{C}^*\to\mathbb{R}^*$ given by $N(z)=|z|^2=z\bar{z}$. The image is the positive reals.

Example 1.8. Look at $N:\mathbb{Q}(i)^*\to\mathbb{Q}^*$ given by $a+bi\mapsto a^2+b^2$. THe image of the norm is the rational number that are sums of 2 squares. As you can see, this gets complicated, even in simple cases.

Theorem 1.1. *If L,K are finite fields, then $N:L^*\to K^*$ is onto.*

Proof. Recall[1] that the Galois group of L/K is cyclic, generated by the Frobenius element $x \mapsto x^q$, where $q = |K|$. The Galois group is $\{\} 1, F, F^2, \ldots, F^{n-1}$, where $n = [L : K]$.

$$\begin{aligned} N(a) &= aF(a)F^2(a)\cdots F^{n-1}(a) \\ &= aa^q a^{q^2}\cdots a^{q^{n-1}} \\ &= a^{q^{n-1}/(q-1)}. \end{aligned}$$

So there are at most $q^{n-1}/(q-1)$ elements of norm 1. The image has at most $q-1$ elements. The order of kernel times the order of the image is the order of L^* $(q^n - 1)$, so the kernel and image indeed have order $q^{n-1}/(q-1)$ and $q-1$, respectively. □

What is the kernel of $N : L \to K$? Hilbert showed that If L/K is a cyclic extension generated by σ, then $N(a) = 1$ iff $a - \sigma(b)/b$ for some $b \in L^*$.

[1] Maybe we should put "recall" instead. Professor Borcherds is unsure whether he actually remembered to introduce this when we went over finite fields.