September 26:

Math 432 Class Lecture Notes

- Traces and Norms
- Discriminants

0.1 Traces and Norms

If E/F is a finite extension of fields, then for every element $x \in E$ we get a "multiplication by x" mapping from E to E that is an endomorphism of an F-vector space of dimension $n := [E : F]$. The trace and norm of this element were defined to be the trace and determinant of this linear transformation, respectively.

From these definitions it follow immediately that the trace and norm are elements of F. It also follows that the trace is a homomorphism for addition, and the norm is a homomorphism for multiplication.

Theorem 1. For all x, y in E,

$$Tr_{E/F}(x+y) = Tr_{E/F}(x) + Tr_{E/F}(y), \qquad N_{E/F}(xy) = NE/F(x)NE/F(y).$$

Now we express the trace and norm of an element of E in terms of the minimal polynomial of the element.

Theorem 2. Let β be any element of E, and assume that its minimal polynomial over F is

$$\mathrm{m}_\beta(x) = x^k - a_1 x^{k-1} + \cdots + (-1)^k a_k.$$

Then n is divisible by k and

$$Tr_{E/F}(\beta) = \frac{n}{k} a_1, \qquad N_{E/F}(\beta) = a_k^{n/k}.$$

Proof. It is fairly easy to verify this directly, but more amusing to do it by using linear algebra.

First note that $F(\beta)$ has degree k over F, so that $n = [E : F]$ is divisible by k.

It is known (under the rubric "Rational Canonical Form") that every square matrix A over a field is similar to a matrix that is a direct sum of companion matrices

$$A = C_1 + C_2 + \cdots + C_m$$

where C_i is the companion matrix of a polynomial f_i and f_i divides f_{i+1} for $1 \leq i < m$.

Remark 3.

$$\begin{bmatrix} 0 & 0 & 0 & -d \\ 1 & 0 & 0 & -c \\ 0 & 1 & 0 & -b \\ 0 & 0 & 1 & -a \end{bmatrix}$$

This generalizes in an obvious way to arbitrary monic polynomials, and the key property is that the characteristic polynomial of the companion matrix of f is f itself.

Remark 4. The f_i in the rational canonical form are called invariant factors of A. Moreover, they are unique: two matrices have the same rational canonical form if and only if they are similar.

Remark 5. In the rational canonical form, the characteristic polynomial of A is the product of the f_i. The minimal polynomial, i.e., the monic polynomial of smallest degree that vanishes when A is substituted, is the last invariant factor f_m.

Let mul_β denote the "multiplication by β" linear transformation on E, as an F vector space. Since the minimal polynomial of mul_β is irreducible, the invariant factors are of the form $1, 1, \cdots, \mathrm{m}_\beta, \mathrm{m}_\beta, \cdots, \mathrm{m}_\beta$. Thus the characteristic polynomial of mul_β is a power of m_β, say

$$f_\beta = \mathrm{m}_\beta^r.$$

By comparing degrees, we see that $n = kr$.

The trace of mul_β is the negative of the coefficient of x^{n-1} in the characteristic polynomial, so

$$Tr_{E/F}(\beta) = ra_1.$$

The determinant of mul_β is $(-1)^n$ times the constant coefficient, so

$$(-1)^n N_{E/F}(\beta) = \Big((-1)^k a_k\Big)^r.$$

The relationships in the theorem now follow from the fact that $n = kr$. □

Now we express the trace and norm in terms of the embeddings of E into a splitting field. Using the Primitive Element Theorem, there is an α such that $E = F(\alpha)$. If K is the splitting field of m_α then by the Embedding Theorem there are n embeddings of E into K; label them $\sigma_1, \sigma_2, \cdots, \sigma_n$ where we let σ_1 be the identity. To simplify notation slightly we write

$$\beta^{(i)} := \sigma_i(\beta)$$

where β is any element of F.

Theorem 6.

$$Tr_{E/F}(\beta) = \sum_i \beta^{(i)}, \qquad N_{E/F}(\beta) = \prod_i \beta^{(i)}.$$

Corollary 7. If $\beta \in F$ then

$$Tr_{E/F} = n\beta, \qquad N_{E/F}(\beta) = \beta^n.$$

Proof. (of the theorem) Let $[F(\beta) : F] = k$, and $[E : F(\beta)] = r$, so that $kr = n$. There are k embeddings of $F(\beta)$ into K and, by the generalized form of the Emedding Theorem, each of those embeddings has r extensions to an embedding of E into K. We find that

$$Tr_{E/F}(\beta) = ra_1 = r\sum_\tau \tau(\beta)$$

since coefficient a_1 of m_β is the sum of the distinct roots of m_β. It follows that

$$Tr_{E/F}(\beta) = \sum_\tau \tau(\beta) = \sum_{\sigma_i \text{ extends } \tau} \sum_\tau \tau(\beta) = \sum_i \sigma_i(\beta) = \sum_i \beta^{(i)}$$

as desired. The formula for the norm follows from a very similar calculation. □

This result reduces the calculation of norms and traces to exercises in elementary symmetric functions.

Corollary 8. If $\beta = g(\alpha)$ for some polynomial $g(x) \in F[x]$ then

$$Tr_{E/F}(\beta) = \sum_i g(\alpha^{(i)}), \qquad N_{E/F}(\beta) = \prod_i g(\alpha^{(i)}).$$

The sum and product of g evaluated at the conjugates of α are symmetric functions in the $\alpha^{(i)}$ and, by the basic theorem on elementary symmetric functions, are polynomials in the coefficients of m_α.

Example 9. If $m_\alpha(x) = x^n - a_1 x^{n-1} + a_2 x^{n-2} - \cdots$ then

$$Tr(\alpha^2) = \sum_i \left(\alpha^{(i)}\right)^2 = \left(\sum_i \alpha^{(i)}\right)^2 - 2\sum_{i<j} \alpha^{(i)}\alpha^{(j)} = a_1^2 - 2a_2.$$

Example 10. If u is an element of F then

$$N(\alpha - u) = \prod_i (\alpha^{(i)} - u) = (-1)^n \prod_i (u - \alpha^{(i)} = (-1)^n \mathrm{m}_\alpha(u).$$

0.2 The discriminants of a basis

Let F be a number field of degree n over $\mathbf{Q}$.

Definition 11. If $\alpha_1, \alpha_2, \cdots, \alpha_n$ is a basis of F over $\mathbf{Q}$ then the **discriminant** of the basis is defined to be the square of the determinant

$$\mathrm{disc}(\alpha_1, \alpha_2, \cdots, \alpha_n) := \det[\alpha_i^{(j)}]^2$$

of the matrix whose entry in the i-th row and j-th column is the image of α_i under the j-th embedding.

Remark 12. Although the numbering of the basis elements is fixed, the numbering of the embeddings is arbitrary. However, if the embeddings are permuted the determinant only changes at most by a sign, so the square of the determinant is independent of the choice of numbering.

Theorem 13. **(a)** The discriminant of a basis $\{\alpha_i\}$ is an element of $\mathbf{Q}$.

(b) The discriminant is given by

$$\operatorname{disc}(\alpha_1, \alpha_2, \cdots, \alpha_n) = \det[Tr_{F/\mathbf{Q}}(\alpha_i \alpha_j)].$$

Proof. The product of matrices $M = [a_{ij}]$ and $N = [b_{ij}]$ is

$$MN = \left[\sum_k a_{ik} b_{kj}\right]$$

where in each case the index i refers to the row and the index j refers to the column. Applying this to the matrix $M = [\alpha_i^{(j)}]$ in the definition of the discriminant, and its transpose, we find that

$$\begin{aligned} \operatorname{disc}(\alpha_i) &= \det(M)^2 = \det(M)\det(M^t) = \det(MM^t) \quad (1) \\ &= \det([\sum_k \alpha_i^{(k)} \alpha_j^{(k)}]) = \det[Tr_{F/\mathbf{Q}}(\alpha_i \alpha_j]. \quad (2) \end{aligned}$$

This proves the second claim in the theorem, and the first claim follows immediately since each trace, and therefore the determinant of the matrix of traces, is a rational number. □

There is a special case where the discriminant is especially easy to compute, namely when the basis is a "power basis" consisting of the powers of an element α:

$$1, \alpha, \alpha^2, \cdots, \alpha^{n-1}.$$

In this case the matrix M in the definition of the discriminant is

$$M = \left[\left(\alpha^{(j)}\right)^i\right]_{0 \le i < n, 1 \le j \le n}.$$

This is the famous Vanderonde matrix, whose determinant is

$$\det(M) = \prod_{i<j} (\alpha^{(j)} - \alpha^{(i)}).$$

Therefore

$$\operatorname{disc}(1, \alpha, \alpha^2, \cdots, \alpha^{n-1}) = \prod_{i<j} \left(\alpha^{(j)} - \alpha^{(i)}\right)^2$$

which is called the **discriminant** of the (monic) polynomial m_α. In the near future we will learn techniques for calculating this discriminant efficiently.

Remark 14. The word “discriminant” will be used in several different ways, though there isn’t much real chance of ambiguity, since we will always be taking the discriminant of something specific. So far, we know the discriminant of a basis, and of a polynomial. Later, we will learn that the ring of integers has a basis, and will define the discriminant of a number field to the the discriminant of such a basis.