September 28:

Math 431 Class Lecture Notes

- Discriminants, continued
- Examples

0.1 Discriminants redux

Let F be a number field of degree n over $\mathbf{Q}$. If $\alpha_1, \cdots, \alpha_n$ is a basis of F over $\mathbf{Q}$ then its discriminant is defined by

$$\mathrm{disc}(\alpha_1, \alpha_2, \cdots, \alpha_n) = \det[\alpha_i^{(j)}]^2 = \det[Tr_{F/\mathbf{Q}}(\alpha_i\alpha_j)].$$

If $\beta_1, \cdots, \beta_n$ is a new basis, it can be described in terms of the basis of α_i by a "change of basis matrix" $A = [a_{ij}]$ whose entries are determined by expressing each of the new basis vectors in terms of the old:

$$\beta_i = \sum_{j=1}^{n} a_{ij}\alpha_j, \quad 1 \leq i \leq n.$$

The entries a_{ij} are in the ground field $\mathbf{Q}$, and the matrix A is nonsingular since the change of basis matrix B from the new basis to the old satisfies $AB = BA = I_n$, i.e., B is the inverse of the matrix A. Indeed, from the linear independence of the α's and the formula

$$\alpha_i = \sum_{j=1}^{n} b_{ij} \sum_{k=1}^{n} a_{jk}\alpha_k$$

we see that the ij entry of BA is the same as the ij entry of the n by n identity matrix I_n.

If $M = [\alpha_i^{(j)}]$ is the matrix in the definition of the discriminant of the original basis, then it is easy to work out that the "discriminant matrix" for the new basis of β's is AM. It follows that

$$\mathrm{disc}(\beta_1, \cdots, \beta_n) = \det(AM)^n = \det(A)^2 \det(M)^2 = \det(A)^2 \mathrm{disc}(\alpha_1, \cdots, \alpha_n).$$

Thus when bases are changed the discriminant changes by the square of the determinant of the change of basis matrix.

Theorem 1. The discriminant of any basis is nonzero. Its sign depends only on the field, and not on the choice of basis.

Proof. Let $F = \mathbf{Q}(\alpha)$. Then the powers of α, from $\alpha^0 = 1$ up to α^{n-1} form a basis, and the discriminant is the discriminant of the minimal polynomial of α. The discriminant of any polynomial with distinct roots is nonzero, and the first statement in the theorem follows immediately. The second follows from the fact that the sign of the discriminant is unchanged by multiplying by a square. □

Remark 2. Later we will see that the sign of the discriminant is $(-1)^{r_2}$ where r_2 is the number of pairs of complex conjugate roots of the minimal polynomial of some (or any) generator α.

0.2 Examples

Example 3. Let $F = \mathbf{Q}(\alpha)$ be a quadratic extension, where

$$m_\alpha(x) = x^2 + ax + b = (x - \alpha)(x - \alpha').$$

Then

$$\mathrm{disc}(1, \alpha) = \det \begin{bmatrix} Tr(1) & Tr(\alpha) \\ Tr(\alpha) & Tr(\alpha^2) \end{bmatrix} = \det \begin{bmatrix} 2 & -a \\ -a & a^2 - 2b \end{bmatrix} = a^2 - 4b.$$

In calculating the traces we can find $Tr(\alpha^2)$ by doing symmetric function calculations (the trace of a power is a power sum, and we know the elementary symmetric functions), or by using linearity of the trace, starting with $\alpha^2 = -a\alpha - b$ so that

$$Tr(\alpha^2) = Tr(-a\alpha - b) = -aTr(\alpha) - bTr(1) = a^2 - 2b.$$

Note that the final form of the discriminant is what is classically called the discriminant of the quadratic polynomial $x^2 + ax + b$.

Example 4. We calculate the discriminant of a special form of a basis of a cubic field. Next time we will how to do these calculations with less effort.

Suppose that $F = \mathbf{Q}(\alpha)$ is a cubic extension, with the minimal polynomial of α having the form

$$\alpha^3 + a\alpha + b = 0.$$

If the three roots of the cubic are $\alpha_1 = \alpha, \alpha_2, \alpha_3$ then the discriminant of the basis $1, \alpha, \alpha^2$ is

$$\prod_{i<j} (\alpha_i - \alpha_j)^2$$

as we saw earlier by considering a Vandermonde matrix.

To find this explicitly in terms of a and b, it is convenient to compute some traces, since

$$\operatorname{disc}(1, \alpha, \alpha^2) = \det \begin{bmatrix} Tr(1) & Tr(\alpha) & Tr(\alpha^2) \\ Tr(\alpha) & Tr(\alpha^2) & Tr(\alpha^3) \\ Tr(\alpha^2) & Tr(\alpha^3) & Tr(\alpha^4) \end{bmatrix}.$$

We find the first three traces by simple symmetric function exercises:

$$Tr(1) = 3, \quad Tr(\alpha) = e_1 = 0, \quad Tr(\alpha^2) = p_2 = e_1^2 - 2e_2 = 0 - 2a = -2a.$$

The remaining traces can be computed by the convenient device of using linearity (which, in effect, gives a recursion on the traces of powers of α). Specifically, from $\alpha^3 = -a\alpha - b$ we get

$$Tr(\alpha^3) = -aTr(\alpha) - bTr(1) = -3b$$

and from $\alpha^4 = -a\alpha^2 - b\alpha$ we get

$$Tr(\alpha^4) = -aTr(\alpha^2) - bTr(\alpha) = 2a^2.$$

Finally, taking the indicated determinant gives the desired discriminant

$$\operatorname{disc}(1, \alpha, \alpha^2) = -4a^3 - 27b^2.$$

This is called the discriminant of the cubic polynomial. With more work one can calculate the discriminant of the general cubic polynomial (i.e., one not missing the quadratic term); this discriminant has 5 terms that are monomials in the three variables.

Remark 5. For a non-monic polynomial $f(x) = a\prod_{i=1}^{n}(x-\alpha_i)$ it turns out to be best (for non-obvious reasons that might be touched on next time) to define the discriminant to be

$$\operatorname{disc}(f) = a^{2n-2}\prod_{i<<j}(\alpha_i-\alpha_j)^2.$$

Remark 6. The discriminant plays a famous role in galois theory in the following way. Let F be the splitting field of a polynomial f of degree n with rational coefficients. Then elements of the galois group $G := \operatorname{Aut}(f)$ permute the roots of f, and distinct elements induce distint permutations of the roots. It follows that G can be identified with a subgroup of the symmetric group S_n.

Theorem 7. *The galois group G is contained in the alternating group A_n if and only if the discriminant of f is a perfect square in* $\mathbf{Q}$.

Example 8. Why does the determinant of the Vandermonde matrix have the specific value that it does? Well, as is often a bright idea in algebraic environments, we replace numbers by variables, i.e., let a_i, $1 \le i \le n$ be indeterminates and consider

$$\det\begin{bmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-1} \end{bmatrix}.$$

Clearly this is zero if equal values are substituted for any of the variables. This means that the polynomial in question is divisible by $a_i - a_j$ for all distinct i and j. However, the degree of the product

$$\prod_{i<j}(a_j-a_i)$$

is $n(n-1)/2$, and this is also the degree of the indicated determinant. Thus the Vandermonde determinant is equal to this product times a constant. The diagonal term in the determinant expansion is

$$a_2a_3^2\cdots a_n^{n-1}$$

and one checks that this occurs in the product with coefficient 1. Thus the Vandermonde determinant is equal to the product.