The discriminant

First and raw version 0.1 — 23. september 2013 klokken 13:45

One of the most significant invariant of an algebraic number field is *the discriminant*. One is tempted to say, apart from the degree, the most fundamental invariant. In simplest case of a quadratic equation, the discriminant tells us the behavior of solution, and of course, even its square roots gives us the solutions. To some extent the same is true for cubic equations, and the higher the degree of an equation less the influence of the discriminant is, but it always plays an important role.

For a field extension we shall define a discriminant for any basis. Of course this depends on the basis, but in a very perspicuous way. In the case of a number field, the ring of algebraic integers A is a free module over $\mathbb{Z}$, and if the basises are confined to be $\mathbb{Z}$-basis for A, the discriminant is an integer independent of the the basis, is an invariant of the number field.

The discriminant serves several purposes at. Its main main feature is that it tells us in which primes a number fields ramify, or more generally, in which prime ideals an extension ramifies.

Additionally the discriminant is a valuable tool to find $\mathbb{Z}$-basis for the ring A of algebraic integers in a number field. To describe A is in general a difficult task, and the discriminant is some times helpful.

In relative situation, the situation is somehow more complicated, and the discriminant is well-defined just as an ideal.

The discriminant of a basis

The scenario is the usual one: A denotes a Dedekind ring with quotient field K, and L a finite, separable extension of K. The integral closure of A in L is B. In *Separability* we defined the trace form $\mathrm{tr}_{L/K}(xy)$. It is a symmetric and quadratic form on L taking values in K, and since L is separable over K, it is non-degenerate after theorem 1 on page 10 of *Separability*.

Let $\alpha_1, \ldots, \alpha_n$ be a K-basis for L and denote it by $\mathcal{B}$. One may form—as one may do for any quadratic form—the *matrix M of the trace form* by putting $M = (\mathrm{tr}_{L/K}(\alpha_i\alpha_j))$. If $\alpha_{\mathcal{B}}$ and $\beta_{\mathcal{B}}$ are the coordinate vectors relative to the basis $\mathcal{B}$ of two elements α and β of L, the value of the trace form $\mathrm{tr}_{L/K}(\alpha\beta)$ is given as

$$\mathrm{tr}_{K\mathbb{Q}}(\alpha\beta) = \alpha_{\mathcal{B}}^t M \beta_{\mathcal{B}}$$

We define *the discriminant of the basis $\mathcal{B}$* as the determinant of the matrix M. That is

$$\Delta_{\mathcal{B}} = \Delta(\alpha_1, \ldots, \alpha_n) = \det(\mathrm{tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j)).$$

The discriminant depends of course on the basis, but in a very clean way. Assume that $\mathcal{B}'$ is another basis and denote by M' the matrix of the trace form in that basis.

If V denotes the transition matrix between the two basis—that is $\alpha_{\mathcal{B}} = V\alpha_{\mathcal{B}'}$ for all α —then

$$\alpha_{\mathcal{B}}^t M\beta_{\mathcal{B}} = (V\alpha_{\mathcal{B}'})^t M(V\beta_{\mathcal{B}'}) = \alpha_{\mathcal{B}'}^t(V^t MV)\beta_{\mathcal{B}'},$$

and as this holds for all α and β, one draws the conclusion that $M' = V^t MV$. Taking determinants, one obtains:

Lemma 1 *Assume that $\mathcal{B}$ and $\mathcal{B}'$ are two K-basises for the field L with transitions matrix V (from $\mathcal{B}'$ to $\mathcal{B}$). Then the relation between the corresponding discriminants is given as:*

$$\Delta_{\mathcal{B}'} = (\det V)^2\Delta_{\mathcal{B}}$$

An important observation is, that if $\mathcal{B}$ is an *integral basis*, *i.e.,* the basis elements are all lying in B, then the discriminant belongs to A. Indeed, already the all the traces $\mathrm{tr}_{L/K}(\alpha_i\alpha_j)$ lie in A.

EXAMPLE 1. — THE CASE OF A PRIMITIVE BASIS. Assume that the field L has a primitive element x , *i.e.,* $L = K(x)$, and let n be the degree of x. Then L has the special basis $1, x, \ldots, x^{n-1}$ formed by the n first powers of x. There is a nice expression for the discriminant of L over K in that particular basis, it equals the discriminant of the minimal polynomial of x as defined in *Separability*. To realize this, let $\omega_1, \ldots, \omega_n$ be the roots of the minimal polynomial of x in some big field Ω. In other words, the values the different embeddings of L in Ω take at x. The ω_k's are the eigenvalues in Ω of the multiplication map ρ_x, and therefore $\mathrm{tr}_{L/K}(x^i) = \sum_k \omega_k^i$.

Let $V = (\omega_i^{j-1})$ be the van der Monde matrix formed by the $\omega_i's$. Then, forming the product of V and its transposed, we get

$$V^tV = (\omega_j^{i-1})(\omega_i^{j-1}) = (\sum_k \omega_k^{i-1}\omega_k^{j-1}) = (\sum_k \omega_k^{i+j-2}) = (\mathrm{tr}_{L/K}(x^{i-1}x^{j-1})),$$

and therefore $\Delta_{1,x,\ldots,x^{n-1}} = (\det V)^2$. Combining this with xxxx, we obtain

Proposition 1 *Given a field extension $L = K(x)$ of degree n with primitive element x. Assume that x has the minimal polynomial $f(t)$ over K. Then the discriminant of the power basis $1, x \ldots, x^{n-1}$ is equal to the discriminant of the polynomial f. That is $\Delta_f = \Delta_{1,x,\ldots,x^{n-1}}$.*

❄

The case of extensions of a PID

Assume now that in the standard setup A is a principal ideal domain, and $n = [L : K]$.

The two main cases that concerns us are the case of a number field whose with ring of integers extends the principal ideal domain $\mathbb{Z}$ and the case that A is a DVR . If A is

a PID , any finitely generated and torsion free module over A is a free module and thus has an A-basis. The transition matrix between two such $\mathbb{Z}$-basises belongs to group $\mathrm{Gl}(n)A$ of invertible $n \times n$-matrices with coefficients in A, and its determinant belongs therefore to groups A^* of units.

The case of a number field

In the all-important case of a number field the ring of integers A is a free $\mathbb{Z}$-module, and the determinant of a transition matrix between two basises equals ± 1. The formula in lemma 1 above shows that the discriminant $\Delta_{\mathcal{B}}$ is *independent* of $\mathcal{B}$ as long as we restrict $\mathcal{B}$ to be a $\mathbb{Z}$-basis of A. This number i called *the discriminant of K* and it is denoted by δ_K.

Proposition 2 *Assume that K is a number field and that A is the ring of integers in K. Then the discriminant $\Delta_{\mathcal{B}}$ is independent of the basis $\mathcal{B}$ as long as $\mathcal{B}$ is a $\mathbb{Z}$-basis for A. It is called* the discriminant *of K and denoted by δ_K.*

EXAMPLE 2. The discriminant of the quadratic field $\mathbb{Q}(\sqrt{d})$ depends on the residue class of d mod 4. The discriminant is $4d$ in case $d \not\equiv 1 \mod 4$ and equals d if $d \equiv 1 \mod 4$. ❄

THE DISCRIMINANT AND THE RAMIFIED PRIMES The most important application of the discriminant is that it detects ramification. In the case that A has a primitive element, say $A = \mathbb{Z}[\xi]$, this is reasonable, since then a prime p ramifies exactly when the minimal polynomial $f(x)$ of ξ has a multiple root modulo p, and the discriminant of $f(x)$ is made to detect this. However, in general A does not have a primitive element and this complicates the matter substantially, but still the discriminant behaves well:

Theorem 1 *Assume that K is a number field with discriminant δ_K. Then a prime p is ramified in K if and only if p divides the discriminant δ_K.*

PROOF: There are three points, the first one being that the trace is functorial in the following sense. Let $p \in \mathbb{Z}$ be a prime and let $a_1, \ldots, a_n$ be a $\mathbb{Z}$ basis for A. Then of course $\bar{a}_1, \ldots, \bar{a}_n$ is a $k(\mathfrak{p})$ basis for A/pA. Clearly if one reduces the multiplication map ρ_a in A modulo p one obtains the multiplication map $\rho_{\bar{a}}$ in A/pA. Now using an $\mathbb{Z}$-basis for A to compute $\mathrm{tr}_{K/\mathbb{Q}}(a)$, one sees that the integer $\mathrm{tr}_{K/\mathbb{Q}}(a)$ reduces to $\mathrm{tr}_{A/pA/k(\mathfrak{p})}(a)$ mod p. Applying this to all the coefficients of the matrix $(\mathrm{tr}_{K/\mathbb{Q}}(a_i a_j))$, one obtains that $\det(\mathrm{tr}_{K/\mathbb{Q}}(a_i a_j))$ reduces to $\det(\mathrm{tr}_{(A/pA)/k(\mathfrak{p})}(\bar{a}_i \bar{a}_j))$ mod p, and as $\delta_K = \det(\mathrm{tr}_{K/\mathbb{Q}}(a_i a_j))$, it follows that p divides δ_K if and only if the trace form on the $k(\mathfrak{p})$-algebra A/pA is degenerate.

The second point is that trace form on A/pA is non-degenerate if and only if A/pA is a product of separable field extensions of $k(\mathfrak{p})$. But as $k(\mathfrak{p})$ is a finite field, all field extensions are separable, so this happens if and only if A/pA is a product of fields. That is, if and only if it has no nilpotent elements.

The third and final point is that $A/pA = \prod_{1 \le i \le s} A/\mathfrak{q}_i^{e_i}$ is without nilpotents if and only if all the e_i's are equal to one, that is if and only if p is non-ramified. ❑

THE DISCRIMINANT AND THE RING OF INTEGERS. The discriminant can sometimes be of great help to find the ring of integers in a number field. Assume we have at our disposal an integral basis $\mathcal{B}$ of K, that is a $\mathbb{Q}$-basis for K contained in A. Assume that $\mathcal{B}'$ is a $\mathbb{Z}$-basis for A and let V be the transition matrix between these two basises. The known basis $\mathcal{B}$ will be a $\mathbb{Z}$-basis for A if and only if V is invertible in $\mathrm{Gl}(\mathbb{Z})n$, that is, if and only if $\det V$ is plus or minus one. But by lemma 1 above the two discriminant $\Delta_{\mathcal{B}}$ and $\mathcal{B}'$ differ by the factor $(\det V)^2$, hence if $\Delta_{\mathcal{B}}$ is a *square free integer*, it must be so that $\det V = \pm 1$, and our basis $\mathcal{B}$ is a $\mathbb{Z}$-basis for A.

Proposition 3 *Assume that K is a number field with ring of integers is A. If an integral basis for K has a square free determinant, then it is a $\mathbb{Z}$-basis for A.*

EXAMPLE 3. Let $f(x) = x^3 - x - 1$, then $f(x)$ is irreducible (only possible roots are ± 1). Let $K = \mathbb{Q}(\xi)$ where ξ is one of the roots of f. The polynomial $f(x)$ has discriminant $-4(-1)^3 - 27 \cdot 1^2 = -23$ which coincides with the diskriminant of the basis $1, \xi, \xi^2$. This is obviously an integral basis, and -23 is square free. It follows that $1, \xi, \xi^2$ is a basis for the ring of integers. ❄

PROBLEM 1. Let $f(x) = x^3 - x + 3$. Show that $f(x)$ is irreducible over $\mathbb{Q}$ and if ξ denotes a root of $f(x)$, find a basis for the ring of integers $K = \mathbb{Q}(\xi)$. HINT: Compute the discriminant by the formula $-4a^3 - 27b^2$ (see *Separability* for this formula) ✸

PROBLEM 2. Let $g(x) = x^3 - 3x + 9$. Show that g is irreducible and compute the discriminant of f. Let η be a root of $g(x)$. Show that $\mathbb{Q}(\eta) = \mathbb{Q}(\xi) = K$ (where ξ is as in the previous problem). Show that $\mathbb{Z}[\eta]$ is not the ring of integers in K. HINT: $3/\xi$ is a root of $g(x)$. ✸

PROBLEM 3. Assume that $a_1, \ldots, a_n$ is an integral basis for A. Show that if $d = \Delta(a_1, \ldots, a_n)$, then $dA \subseteq a_1\mathbb{Z} + \cdots + a_n\mathbb{Z}$. ✸

PROBLEM 4. Let $\sigma_1, \ldots, \sigma_n$ be the different embeddings of the number field K into some big field Ω. Let $\alpha_1, \ldots, \alpha_n$ be a basis for K over $\mathbb{Q}$. Show that

$$\Delta(\alpha_1, \ldots, \alpha_n) = (\det(\sigma_i(\alpha_j)))^2$$

✸

PROBLEM 5. Let $(\sigma_i(\alpha_j))$ be the $n \times n$-matrix from problem 4. Let $P = \sum_{\tau \text{ even}} \sigma_{\tau(1)}(\alpha_1) \cdot \cdots \sigma_{\tau(n)}(\alpha_n)$ and $N = \sum_{\tau \text{ odd}} \sigma_{\tau(1)}(\alpha_1) \cdots \sigma_{\tau(n)}(\alpha_n)$ where τ runs through the permutations of $\{1, \ldots, n\}$. Show that $\det(a_{ij}) = P - N$, and that both $P + N$ and PN are invariant under the action of τ that permutes the different embeddings σ_i. Then show that P and N both lie in $\mathbb{Z}$. ✸

PROBLEM 6. *(Stickelberger).* Let δ_K be the discriminant of the number field K. Show that δ_K is a square modulo 4, hence $\delta_K \equiv 0$ or $\delta_K \equiv 1$ modulo 4. HINT: Write $\delta = (P - N)^2 = (P + N)^2 - 4PN$ with a smart choice of P an N. ✸

The general case and the diskriminant ideal

In the general case, there is no way of getting *one* element in A that plays the role of *the discriminant* as for a number field. There are two reasons for this. First of all, the ring B is not necessarily is a free A-module and we do have A-basises for B at our disposal. Secondly, even if B were a free A-module, the group A^* of units in A is in general much more complicated than the one of $\mathbb{Z}$ and $(A^*)^2$ can be highly non-trivial.

However one may define a *discriminant ideal* $\mathfrak{d}_{B/A}$ that does the job. It is defined as the ideal in A generated by $\Delta(b_1,\dots,b_n)$ as the $b_1,\dots,b_n$ run through all *integral basises* for L over K. Recall that this means that $b_1,\dots,b_n$ is a basis for L contained in B.

In case K is number field with ring of integers A, the discriminant δ_K is a slightly more subtle invariant than the discriminant ideal $\mathfrak{d}_{A/\mathbb{Z}}$. Of course, δ_K will be one of the two generators of $\mathfrak{d}_{A/\mathbb{Z}}$, the subtility lies in the fact that one of them is preferred over the other.

Just like for the discriminant, the interest of the discriminant deal lies in the fact that it detects ramification:

Theorem 2 (Dedekind) *Let A be a Dedekind ring with quotient field K and let B be the integral closure of A in a finite and separable extension L of K. Then a prime $\mathfrak{p}$ of A ramifies in B if and only if $\mathfrak{d}_{B/A}\subseteq\mathfrak{p}$.*

PROOF: The proof has three ingredient. The first one is that the discriminant ideal localizes well. That is

☐ If S is a multiplicative system in A, we have $\mathfrak{d}_{B_S/A_S}=(\mathfrak{d}_{B/A})_S$

Clearly if $\alpha_1,\dots,\alpha_n$ is a K-basis for L contained in B, it is a K-basis for L contained in B_S. Hence the inclusion $(\mathfrak{d}_{B/A})_S\subseteq\mathfrak{d}_{B_S/A_S}$. On the other hand, if $\alpha_1,\dots,\alpha_n$ is a K basis for L contained in the localization B_S, then $s\alpha_1,\dots,s\alpha_n$ is contained in B for a suitable $s\in S$, and it is still a K basis for L. Obviously $\Delta(s\alpha_1,\dots,s\alpha_n)=s^{2n}\Delta(\alpha_1,\dots,\alpha_n)$. This shows that $\mathfrak{d}_{B_S/A_S}\subseteq(\mathfrak{d}_{B/A})_S$.

The second ingredient is that the ramification behavior of a prime ideal localizes. This somehow vague statement, means the following:

☐ If $\mathfrak{p}$ is a prime ideal i A, then $\mathfrak{p}$ ramifies in B if and only if $\mathfrak{p}A_\mathfrak{p}$ ramifies in $B_\mathfrak{p}$.

Indeed, this is an immediate consequence of the isomorphism $B/\mathfrak{p}\simeq B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p}$ and the fact that $\mathfrak{p}$ ramifies (respectively $\mathfrak{p}A_\mathfrak{p}$) if and only if $B/\mathfrak{p}B$ (resp. $B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p}$) has non-trivial nilpotent elements.

The third and final ingredient is that the theorem holds for the local rings $A_\mathfrak{p}$, in fact it holds whenever A is a PID :

☐ If A is a PID , then $\mathfrak{p}$ ramifies if and only if $\mathfrak{d}_{B/A}\subseteq\mathfrak{p}$.

Indeed, it follows from lemma 1 on page 2 that if $\alpha_1,\dots,\alpha_n$ is an integral basis for L, then $\Delta(\alpha_1,\dots,\alpha_n)$ is a generator for the discriminant ideal $\mathfrak{d}_{B/A}$. And as B is a free A-module (any torsion free and finitely generated A-module is since A is, a PID) the proof of theorem 1 shows *mutatis mutandi* that $\mathfrak{p}$ ramifies if and only if $\Delta(\alpha_1,\dots,\alpha_n)\notin\mathfrak{p}$. ❑

An observation which is not *a priori* clear, is that in the standard situation, only *finitely many* prime ideals ramify in B.