Math 430
Notes from Class 10/7

We will use the following (proof done earlier) to calculate rings of integers.

Recall that the discriminant of a monic polynomial h with roots $\alpha_1, \ldots, \alpha_n$ (with multiplicity) is defined to be

$$\Delta(h) = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

What happens when we reduce a polynomial modulo a maximal ideal $\mathfrak{p}$ in a Dedekind domain A.

Proposition 12.1. *Let F be a monic polynomial in a Dedekind domain A. Let $\mathfrak{p}$ be a prime of A and let $\bar{F}$ be the reduction of F mod $\mathfrak{p}$. Let $\bar{F}$ be the reduction of F modulo $\mathfrak{p}$ and let $\overline{\Delta}(F)$ be the reduction of $\Delta(F)$ modulo $\mathfrak{p}$. Then, we have $\overline{\Delta}(F) = \Delta(\bar{F})$.*

Proof. Let $F = \prod_{i=1}^{n}(X - \alpha_i)$ where the α_i. Let $B = A[\alpha_1, \cdots, \alpha_n]$. Then there is a maximal $\mathfrak{q}$ in B such that $\mathfrak{q} \cap A = \mathfrak{p}$. Let $\phi : B \longrightarrow B/\mathfrak{q}$. Let $h \in (B/\mathfrak{q})[X]$ be the polynomial $\prod_{i=1}^{m}(X - \phi(\alpha_i))$. Now, the $i - i$-th coefficient of $h(x)$ is $(-1)^i S_i(\phi(\alpha_1), \ldots, \phi(\alpha_n))$ where S_{i+1} is the $i + 1$-st elelementary symmetric polynomial in n-variables. Since ϕ is homomorphism, $(-1)^{-i} S_i(\phi(\alpha_1), \ldots, \phi(\alpha_n))$ is also the $n - i$-th coefficient of $\bar{F}$, so $\bar{F} = h$ and it is clear that

$$\Delta(h) = (-1)^{n(n-1)/2} \prod_{i \neq j} (\phi(\alpha_i) - \phi(\alpha_j)) = \prod_{i<j} (\phi(\alpha_i) - \phi(\alpha_j))^2 = \overline{\Delta}(F).$$

□

This has the following corollary for monic polynomials F over Dedekind domains.

Corollary 12.2. *Let A be a Dedekind domain with field of fractions K and let $\mathfrak{p}$ be a maximal prime in A. Then the reduction $\bar{F}$ of F modulo $\mathfrak{p}$ has distinct roots in the algebraic closure of $A/\mathfrak{p}$ if and only if $\Delta(F) \notin \mathfrak{p}$.*

It is easy to see that $\Delta(F) \in K$. To see this, note that if the roots of F are distinct, then $K(\alpha_1, \ldots, \alpha_n)$ is Galois over K and $\prod_{i \neq j}(\alpha_i - \alpha_j)$ is certainly invariant under the Galois group of $K(\alpha_1, \ldots, \alpha_n)$ over K. It follows that $\Delta(F) \in K$. To see this, note that if the roots of F are distinct, then $K(\alpha_1, \ldots, \alpha_n)$ is Galois over K and $\prod_{i \neq j}(\alpha_i - \alpha_j)$ is certainly invariant under the Galois group of $K(\alpha_1, \ldots, \alpha_n)$ over K.

Here are some other, often easier ways of writing the discriminant...

Let F be monic over K. Then

$$\Delta(F) = (-1)^{n(n-1)/2} \prod_{i=1}^{n} F'(\alpha_i).$$

This is quite easy to see, since if $F(X) = \prod_{i=1}^{n}(X - \alpha_i)$, then by the product rule, $F'(X) = \sum_{i=1}^{m} \prod_{i \neq j}(\alpha_i - \alpha_j)$, so $F'(\alpha_i) = \prod_{j \neq i}(\alpha_i - \alpha_j)$ and $\prod_{i=1}^{n} F'(\alpha_i) = \prod_{i \neq j}(\alpha_i - \alpha_j)$.

When F is monic and irreducible with and $L = K(\alpha)$ is separable for a root α of F, this yields

$$\Delta(F) = (-1)^{n(n-1)/2}\, \mathrm{N}_{L/K}(F'(\alpha)).$$

Since F' has coefficients in K, we see that if $\alpha_1, \ldots, \alpha_n$ are the conjugates of α, then $\mathrm{N}_{L/K}(F'(\alpha)) = \prod_{i=1}^{m} F'(\alpha_i)$ and we are done.

Let's do some more examples of Dedekind domains today. We'll start with $\mathbb{Q}(\sqrt[3]{5})$, which we will show is Dedekind. First of all, we'll calculate the discriminant of $\mathbb{Z}[\sqrt[3]{5}]$. We see that the minimal polynomial of $\sqrt[3]{5}$ is $F(X) = X^3 - 5$, which has derivative $3X^2$, so

$$\Delta(F) = \mathrm{N}_{\mathbb{Q}(\sqrt[3]{5})/\mathbb{Q}}(F'(\sqrt[3]{5})) = \mathrm{N}_{\mathbb{Q}(\sqrt[3]{5})/\mathbb{Q}}(3\sqrt[3]{5}^2) = 3^3 5^2,$$

so we know that any non-invertible primes must lie over 3 or 5, since a prime $(\mathcal{Q}, g_i(\sqrt[3]{5}))$ can fail to be invertible if and only if $g^2 \mid F \pmod{p\mathbb{Z}}$ where $\mathcal{Q} \cap \mathbb{Z} = p\mathbb{Z}$.

Let's factor over 5 and see what happens... We get $X^3 - 5 \equiv X^3 \pmod 5$, so we get the prime $(\sqrt[3]{5}, 5)$ which is certainly generated by $\sqrt[3]{5}$ and hence is principal and thus invertible. Over 3, things are a bit more complicated. We factor as $X^3 - 5 \equiv (X-5)^3 \pmod 3$, so we have the ideal $(\sqrt[3]{5} - 5, 3)$, which we denote as $\mathcal{Q}$. How can we tell whether or not this is locally principal? One way is by using the remainder term as mentioned before. When we divide $(X - 5)$ into $X^3 - 5$ we get a remainder of $5^3 - 5 = 120$, which is not divisible by 9. So the prime $(\sqrt[3]{5} - 5, 3)$ is invertible.

Here's another explanation with norms.

One way to check if an integer n is in the ideal generated by an element β in an integral extension ring is to see if n is the ideal generated by the norm of β. Let's apply this idea to the above we see that

$$\mathrm{N}_{\mathbb{Q}(\sqrt[3]{5})/\mathbb{Q}}(\sqrt[3]{5} - 5) = (1 - \sqrt[3]{5})(1 + \sqrt[3]{5} + \sqrt[3]{5}^2) = 5 - 125 = -120 = (-40) \cdot 3.$$

Since -40 is unit in $\mathbb{Z}[\sqrt[3]{5}]_{\mathcal{Q}}$, it follows that

$$\mathbb{Z}[\sqrt[3]{5}]_{\mathcal{Q}}(\sqrt[3]{5}-5) = \mathbb{Z}[\sqrt[3]{5}]_{\mathcal{Q}}\mathcal{Q},$$

so $\mathcal{Q}$ is locally principal, as desired. Thus, we see that $\mathbb{Z}[\sqrt[3]{5}]$ is a Dedekind domain as desired.

What about $\mathbb{Z}[\sqrt[3]{19}]$? Calculating the discriminant yields $3^3 \cdot 19^2$. Again, it is easy to see that the prime lying over 19 is just $\sqrt[3]{19}$. But the prime lying over 3 is trickier. We see that the only prime $\mathbb{Q} \in \mathbb{Z}[\sqrt[3]{19}]$ such that $\mathbb{Q} \cap \mathbb{Z} = 3\mathbb{Z}$ is the prime $(\sqrt[3]{19}-19, 3)$. Modulo 3 we have

$$(X-19)^3 = X - 19 \pmod 3.$$

From some work from last time, $(\sqrt[3]{19}-19, 3)$ is invertible if and only if the remainder of $X^3 - 19$ modulo $X - 19$ is divisble by 3^2. We see that

$$(X^3 - 19) = (X-19)(X^2 + 19X + 19^2) + 19^3 - 19.$$

Since

$$19^3 - 19 \equiv -18 \pmod 9 \equiv 0 \pmod{19}$$

we see that $(\sqrt[3]{19}-19, 3)$ is not invertible.

In fact, we can generalize this to show that if a is a square-free integer and p is a prime, then $\mathbb{Z}[\sqrt[p]{a}]$ is Dedekind if and only if $a^p - a \not\equiv 0 \pmod{p^2}$. This will be on your homework.

For an element $\alpha \notin A$ that is integral over A, we define the discriminant $\Delta(\alpha/A)$ to be $\Delta(F)$ where F is the minimal monic for α over A. We also define the discriminant $\Delta(A[\alpha])$ to be $\Delta(A[\alpha])$.

Given a Dedekind domain A with field of fractions K and a finite separable extension L of K of degree n we want to be able to define a discriminant $\Delta(B'/A)$ of *any* subring B' of L. This will involve working with a basis for L over K that consists entirely of elements contained in B'

A bit more on subrings of the integral closure.

Proposition 12.3. *Let A be an integral domain with field of fractions K and let L be a finite extension of K. Suppose that $B' \subset L$ has field of fractions L and is integral over A. Then, for every element $y \in L$ there exists $a \in A$ such that $ay \in B'$.*

Proof. Let $y = \alpha/\beta$ for $\alpha, \beta \in B'$ with $\alpha, \beta \neq 0$. We will show that $\alpha/\beta = b/a$ for $b \in B'$ and $a \in A$. We know that the ideal $B'\beta$ has nonzero intersection with A by taking the constant term of the minimal monic polynomial for β over A. Thus, we can write $\gamma\beta = a$ for some nonzero $a \in A$. Then $1/\beta = \gamma/a$, so $\alpha/\beta = \alpha\gamma/a$ and we are done, since this means that $a(\alpha/\beta) \in B'$. □

For the rest of class, A is Dedekind with field of fractions K, the field L is a finite separable extension of K of degree n, and B' is a subring of L that is integral over A. We will also assume that for every maximal ideal $\mathfrak{p}$ of A, the residue field $A/\mathfrak{p}$ is perfect.

We'll begin with a definition that works when B' is a free A-module, i.e. when B' is isomorphic as an A-module to A^n, where $n = [L : K]$. In this case, we choose a basis $w_1, \ldots, w_n$ for B' over A and we let M be the matrix $[m_{ij}]$ where $m_{ij} = \mathrm{T}_{L/K}(w_i w_j)$. Then we define

$$\Delta(B') = \det M. \tag{1}$$

How do we know that this agrees with our earlier definition in the case $B' = A[\alpha]$? In fact, it more or less follows from some earlier work we did. Recall that in this case, we can choose the basis $1, \alpha, \ldots, \alpha^{n-1}$, so that $[m_{ij}] = [\mathrm{T}_{L/K}(\alpha^{i+j-2})]$, which we recall is equal to

$$\sum_{\ell=1}^{n} \alpha_\ell^{i+j-2}.$$

As we saw earlier, letting N be the van der Monde matrix

$$\begin{pmatrix} 1 & \cdots & 1 \\ \alpha_1 & \cdots & \alpha_n \\ \cdots & \cdots & \cdots \\ \alpha_1^{n-1} & \cdots & \alpha_n^{n-1} \end{pmatrix},$$

we have $NN^t = M$, so

$$\det M = (\det N)^2 = \prod_{i<j} (\alpha_i - \alpha_j)^2,$$

which is the same as $\Delta(\alpha)$, so our definitions agree.

Not all B' will be free A-modules, however, so we have the more general definition below.

Definition 12.4. With notation as above $\Delta(B'/A)$ is defined to be ideal generated by the determinants of all matrices $M = [\mathrm{T}_{L/K}(w_i w_j)]$ as $w_1, \ldots, w_n$ range over all bases for L consisting of elements contained in B'.