Math 568 Tom Tucker
NOTES FROM CLASS 10/20

Definition 11.1. Let K be a field and let F be the monic polynomial

$$F(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0.$$

Then, writing

$$F(x) = \prod_{i=1}^{n}(x - \alpha_i)$$

where α_i are the roots of F in some algebraic closure of K, the discriminant $\Delta(F)$ is defined to be

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

Why is this discriminant useful? Because of the following obvious fact:

$$\Delta(F) \neq 0 \Leftrightarrow F \text{ does not have multiple roots.}$$

This is clear because an algebraic closure of K is certainly an integral domain.

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

Proposition 11.2. *Let F be a monic polynomial in $A[x]$ where A is a Dedekind domain. Let $\mathcal{P}$ be a prime of A and let $\bar{F}$ be the reduction of F mod $\mathcal{P}$. Let $\bar{F}$ be the reduction of F modulo $\mathcal{P}$ and let $\overline{\Delta}(F)$ be the reduction of $\Delta(F)$ modulo $\mathcal{P}$. 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 $\mathcal{Q}$ in $\mathcal{P}$ such that $\mathcal{Q} \cap A = \mathcal{P}$. Let $\phi : B \longrightarrow B/\mathcal{Q}$. Let $h \in (B/\mathcal{Q})[X]$ be the polynomial $\prod_{i=1}^{m}(X - \phi(\alpha_i))$. Now, the i-th coefficient of $h(x)$ is $(-1)^{n-i}S_{i+1}(\phi(\alpha_1), \ldots, \phi(\alpha_n))$ where S_{i+1} is the $i+1$-st elelementary symmetric polynomial in n-variables. Since ϕ is homomorphism, $(-1)^{n-i}S_{i+1}(\phi(\alpha_1), \ldots, \phi(\alpha_n))$ is also the 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 $F \in A[x]$.

Corollary 11.3. *Let A be a Dedekind domain with field of fractions K and let $\mathcal{P}$ be a maximal prime in A. Then the reduction $\bar{F}$ of F modulo $\mathcal{P}$ has distinct roots in the algebraic closure of $A/\mathcal{P}$ if and only if $\Delta(F) \notin \mathcal{P}$.*

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 $\prod_{i=1}^{n} F'(\alpha_i) = \prod_{i \neq j}(\alpha_i - \alpha_j) = \pm\Delta(F)$.

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 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

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

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? Let's recall a bit about the norm.

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 not divisble by 3^2. We see that

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

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.