Math 531 Tom Tucker
NOTES FROM CLASS 10/8

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

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

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

$$\Delta(F) = \left(-1\right)^{n(n-1)/2} N_{L/K}(F'(\alpha)).$$

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

Recall this key fact from last time:

**Corollary 17.1.** Let $A$ be a Dedekind domain with field of fractions $K$ and let $\mathcal{P}$ be a maximal prime in $A$ and suppose that $A/\mathcal{P} = k$ is a perfect field. 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 $\Delta(F) \notin \mathcal{P}$.

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 $Z[\sqrt[3]{5}]$. We see that the minimal polynomial of $\sqrt[3]{5}$ is $F(X) = X^3 - 5$, which has derivative $3X^2$, so

$$\Delta(F) = N_{\mathbb{Q}(\sqrt[3]{5})}(F'((\sqrt[3]{5}))) = N_{\mathbb{Q}(\sqrt[3]{5})}(3\sqrt[3]{5}^2) = 3^35^2.$$

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

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 \(Q\). 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 \(\beta\) in an integral extension ring is to see if \(n\) is the ideal generated by the norm of \(\beta\). Let’s apply this idea to the above we see that

\[
N_{Q, \sqrt[3]{5}/Q}(\sqrt[3]{5} - 5) = (1 - \sqrt[3]{5})(1 + \sqrt[3]{5} + \sqrt[3]{5}^2) = 5 - 125 = -120 = (-40) \cdot 3.
\]

Since \(-40\) is unit in \(\mathbb{Z}[\sqrt[3]{5}]\), it follows that \(\mathbb{Z}[\sqrt[3]{5}]/Q (\sqrt[3]{5} - 5) = \mathbb{Z}[\sqrt[3]{5}]Q\), so \(Q\) is locally principal, as desired. Thus, we see that \(\mathbb{Z}[\sqrt[3]{5}]\) is a Dedekind domain as desired.

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

\[
(X - 19)^3 = X - 19 \pmod{3}.
\]

From some work from last time, \((\sqrt{19} - 19, 3)\) is invertible if and only if the remainder of \(X^3 - 19\) modulo \(X - 19\) is divisible 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 \((\sqrt{19} - 19, 3)\) 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 \(\mathbb{Z}[\sqrt{a}]\) is Dedekind if and only if \(a^p - a \not\equiv 0 \pmod{p^2}\). This will be on your homework.