Recall from last time:

Let \( A \) be Dedekind. Let \( \mathcal{P} \) be a maximal ideal of \( A \) and let \( \alpha \) be an integral element of a finite separable extension of the field of fractions of \( A \). Suppose that \( G \) is the minimal monic for \( \alpha \) over \( A \) and that the reduction mod \( \mathcal{P} \) of \( G \), which we call \( \bar{G} \) factors as

\[
\bar{G} = \bar{g}_1^r \cdots \bar{g}_m^r
\]

with the \( \bar{g}_i \) distinct, irreducible, and monic.

**Proposition 16.1.** With notation as above, if \( r_i = 1 \) then the prime \( A[\alpha](\mathcal{P}, g_i(\alpha)) \) is invertible. If \( r_i > 1 \), then \( Q_i \) is invertible if and only if all the coefficients of the remainder mod \( g_i \) of \( G \) are not in \( \mathcal{P}^2 \), i.e. if writing

\[
G(x) = q(x)g_i(x) + r(x),
\]

we have \( r(x) \notin \mathcal{P}^2[x] \).

**Proof.** We did the \( r_i = 1 \) part last time. Now, for \( r_i > 1 \). We may as well work over \( A[\alpha] \) rather than \( A[\alpha] \) we write \( A[\alpha] \mathcal{P} = A[\alpha]\pi \).

Let \( \phi : A[\alpha][x] \rightarrow A[\alpha][\alpha] \) be the natural quotient map obtained by sending \( x \) to \( \alpha \). The kernel of this map is \( A[\alpha][x]G \). The prime \( Q_i \) in \( A[\alpha] \) is generated by \( (\pi, g_i(\alpha)) \), so \( \phi^{-1}(Q_i) \) is generated by \( (\pi, g_i(x)) \) since \( G(x) \) is in the ideal generated by \( (\pi, g_i(x)) \) (since \( g_i(x) \) divides \( G \) modulo \( \mathcal{P} \)). Denote \( \phi^{-1}(Q_i) \) as \( J \). It is easy to see that

\[
\dim_{A_P/A_P^2} J/J^2 = 2d
\]

where \( d \) is the degree of \( g_i \) since

\[
\{\pi, \pi x, \ldots, \pi x^{d-1}, g_i, g_ix, \ldots, g_ix^{d-1}\}
\]

is a basis for \( J/J^2 \) as a \( A_P/A_P^2 \)-module. We see that \( \phi \) induces a map

\[
\bar{\phi} : J/J^2 \rightarrow Q_i/Q_i^2
\]

which has kernel \( A_P[x]G(x) \) (mod \( J^2 \)). From (1), this is generated by the remainder \( r(x) \). Since \( \deg r < \deg g \), we have \( r \in J^2 \) if and only if \( r \in \pi^2 A_P[x] \). Thus, we see that

\[
\dim_{A_P/A_P^2}(Q_i/Q_i^2) < 2d
\]

if and only if \( r \notin \pi^2 A_P[x] \). Since

\[
\dim_{A_P/A_P^2}(Q_i/Q_i^2) = d \dim_{A[\alpha][Q_i]/A[\alpha][Q_i]} (Q_i/Q_i^2)
\]

we thus have

\[
\dim_{A_P/A_P^2}(Q_i/Q_i^2) = 1
\]
if and only if \( r \notin \pi^2 A_P[x] \).

How can we tell which primes we have to worry about (by this, I mean those for which some \( r_i \) is greater than 1)? We can use something called the discriminant of a finitely generated integral extension of rings \( B \) over \( A \). We will work with several formulations, all of which are equivalent. Here’s the definition of the discriminant of a polynomial.

**Definition 16.2.** 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 \( \alpha_i \) 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:

\( \Delta(F) \neq 0 \iff F \) 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 16.3.** Let \( F \) be a polynomial in a Dedekind domain \( A \) 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 \( \bar{\Delta}(F) \) be the reduction of \( \Delta(F) \) modulo \( \mathcal{P} \). Then, we have \( \bar{\Delta}(F) = \Delta(\bar{F}) \).

**Proof.** Let \( F = \prod_{i=1}^{n}(X - \alpha_i) \) where the \( \alpha_i \). Let \( B = A[\alpha_1, \ldots, \alpha_n] \). Then there is a maximal \( \mathcal{Q} \) in \( \mathcal{P} \) such that \( \mathcal{Q} \cap A = \mathcal{P} \). Let \( \phi : B \to B/\mathcal{Q} \) be the polynomial \( \prod_{i=1}^{n}(X - \phi(\alpha_i)) \). 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 elementary symmetric polynomial in \( n \)-variables. Since \( \phi \) 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

\[
\Delta(h) = (-1)^{n(n-1)/2} \prod_{i \neq j} (\phi(\alpha_i) - \phi(\alpha_j)) = \prod_{i < j} (\phi(\alpha_i) - \phi(\alpha_j))^2 = \bar{\Delta}(F).
\]
This has the following corollary.

**Corollary 16.4.** 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 $\Delta(F) \notin \mathcal{P}$. 