... Commutative Algebra... integral extensions, finite-generation, Noetherian-ness...

**Example:** Function fields in one variable... are very similar to \( \mathbb{Z}, \mathbb{Q}, \) and integral extensions of \( \mathbb{Z} \) in finite (separable) field extensions of \( \mathbb{Q}. \)

Polynomial rings \( \mathbb{F}_q[X] \) are as well-behaved as \( \mathbb{Z}. \) Their fields of fractions \( \mathbb{F}_q(X), \) rational functions in \( X \) with coefficients in \( \mathbb{F}_q, \) are as well-behaved as \( \mathbb{Q}. \)

For *any* field \( E, \) \( E[X] \) is Euclidean, a PID and a UFD. \( E \) finite is most similar to \( \mathbb{Z}, \) in that the residue fields are finite: quotient \( \mathbb{F}_q[X]/\langle f \rangle \) with \( f \) a prime are finite fields.

To exploit the geometric aspect, it is useful to practice on \( \mathbb{C}[X]... \)
The affine line

\( \mathbb{C} \) is the affine complex line (not plane)

Since \( \mathbb{C} \) is algebraically closed, the non-zero prime ideals in \( \mathbb{C}[X] \) are \( \langle X - z \rangle \), for \( z \in \mathbb{C} \).

The point \( z \in \mathbb{C} \) is the simultaneous vanishing set of the ideal \( \langle X - z \rangle \).

Discussion of the point at infinity \( \infty \) is postponed a bit: arguably, \( \infty \) is the vanishing set of \( 1/X \) .... but where?? Also, \( 1/X \) is not in \( \mathbb{C}[X] \), so we can’t talk about the ideal generated by it...
From one viewpoint, a (compact, connected) Riemann surface $M$ is/corresponds (!?) to a finite field extension $K$ of $k = \mathbb{C}(X)$.

Since $\mathbb{C}(X)$ has characteristic 0, $K/k$ is separable, so is generated by a single element $Y$, satisfying a monic $f(Y) = 0$, where $f$ has coefficients in $\mathbb{C}(X)$: with $a_j(X), b_j(X) ∈ \mathbb{C}[X]$, assuming $a_j(X)/b_j(X)$ in lowest terms,

$$Y^n + \frac{a_{n-1}(X)}{b_{n-1}(X)}Y^{n-1} + \ldots + \frac{a_1(X)}{b_1(X)}Y + \frac{a_0(X)}{b_0(X)} = 0$$

To get rid of the denominators, replace $Y$ by $Y/b_{n-1}(X) \ldots b_1(X)b_0(X)$ and multiply through by

$$(b_{n-1}(X) \ldots b_1(X)b_0(X))^n$$

After relabelling, without loss of generality, with $a_j(X) ∈ \mathbb{C}[X]$,

$$Y^n + a_{n-1}(X)Y^{n-1} + \ldots + a_1(X)Y + a_0(X) = 0$$

Note that these normalizations make $Y$ integral over $\mathbb{C}[X]$. 
The most immediate description of (the not-at-infinity points of) the Riemann surface associated to

\[ f(X, Y) = Y^n + a_{n-1}(X)Y^{n-1} + \ldots + a_1(X)Y + a_0(X) = 0 \]

is that, for each \( z \in \mathbb{C} \), the \( n \) solutions \( w_1, \ldots, w_n \in \mathbb{C} \) to

\[ f(z, w) = w^n + a_{n-1}(z)w^{n-1} + \ldots + a_1(z)w + a_0(z) = 0 \]

specify the points \textit{above} \( z \), or \textit{over} \( z \). That is, the Riemann surface is the graph of \( f(z, w) = 0 \) in \((z, w) \in \mathbb{C}^2\), and the normalizations above arrange the projection to the first coordinate an everywhere-defined at-most-\( n \)-to-one map.

The values of \( z \) for which the equation has \textit{multiple roots} are the \textit{ramified points}. 
Ramification refers to the projection \( \{ (z, w) : f(z, w) = 0 \} \to \mathbb{C} \) to the \( z \)-plane.

\( F(w) = f(z, w) \) has repeated roots exactly when \( F, F' \) have a common factor. Apply Euclidean algorithm in \( \mathbb{C}(X)[Y] \):

**Example:** Ramification of \( F(Y) = f(X, Y) = Y^5 - 5XY + 4 \). Here \( F'(Y) = 5Y^4 - 5X \), but discard the unit 5. One step of Euclid is

\[
(Y^5 - 5XY + 4) - Y(Y^4 - X) = -4XY + 4
\]

\(-4X \in \mathbb{C}(X)^\times\), so replace \(-4XY + 4\) with \( Y - \frac{1}{X} \). The next step of Euclid would divide \( Y^4 - X \) by \( Y - \frac{1}{X} \). By the division algorithm, the remainder is the value of \( Y^4 - X \) at \( Y = 1/X \), namely, \( \frac{1}{X^4} - X \).

Thus, the five ramified points of \( f(z, w) = 0 \) are where \( z^5 = 1 \).
But, also, ...

The (not-at-infinity) points of the Riemann surface $M$ are the zero-sets of non-zero prime ideals of the integral closure $\mathfrak{O}$ of $\mathfrak{o} = \mathbb{C}[X]$ in $K$. (In fact, the ring $\mathfrak{O}$ is Dedekind.)

**Claim:** For typical $z \in \mathbb{C}$, the prime ideal $(X - z) = (X - z)\mathbb{C}[X]$ gives rise to $(X - z)\mathfrak{O} = \mathfrak{P}_1 \ldots \mathfrak{P}_n$, where $n = [K : k]$. That is, $n$ points on $M$ lie over $z \in \mathbb{C}$.

The ramified points are exactly those $z$ such that $(X - z) \cdot \mathfrak{O}$ has a repeated factor!!! (We’re not set up to address that yet...)

**Proof:** As above, take $K = \mathbb{C}(X, Y)$ with $Y$ satisfying a monic polynomial equation $f(X, Y) = 0$ with coefficients in $\mathbb{C}[X]$, and $f$ of degree $[K : k]$. 
Then do the usual computation

\[
\mathcal{O}/(X - z)\mathcal{O} = \mathbb{C}[X, T]/\langle X - z, f(X, T) \rangle
\]

\[
\approx \mathbb{C}[T]/\langle f(z, T) \rangle
\]

\[
\approx \mathbb{C}[T]/\langle (T - w_1)(T - w_2) \ldots (T - w_n) \rangle
\]

\[
\approx \frac{\mathbb{C}[T]}{\langle T - w_1 \rangle} \oplus \frac{\mathbb{C}[T]}{\langle T - w_2 \rangle} \oplus \ldots \oplus \frac{\mathbb{C}[T]}{\langle T - w_n \rangle}
\]

\[
\approx \mathbb{C} \oplus \mathbb{C} \oplus \ldots \oplus \mathbb{C}
\]

assuming \(f(z, T)\) factors with distinct \(w_j\). By the earlier Lemma, \((X - z)\mathcal{O}\) is an intersection of \(n\) prime (maximal!) ideals. 

///

Of course, the \(w_j\)'s are the solutions to \(f(z, w) = 0\).
For example, for the elliptic curve

$$Y^2 = X^3 + aX + b$$  \hspace{1cm} \text{(with } a, b \in \mathbb{C})$$

where \(X^3 + aX + b = 0\) has distinct roots, we have (!?) \(\mathcal{O} = \mathbb{C}[X, Y] \approx \mathbb{C}[X, T]/\langle T^2 - X^3 - aX - b \rangle\) with a second indeterminate \(T\), and the usual trick gives

$$\mathcal{O}/(X - z)\mathcal{O} = \mathbb{C}[X, T]/\langle X - z, T^2 - X^3 - aX - b \rangle$$

\[ \approx \mathbb{C}[T]/\langle T^2 - z^3 - az - b \rangle \]

\[ \approx \mathbb{C}[T]/\langle (T - w_1)(T - w_2) \rangle \]

\[ \approx \mathbb{C}[T]/\langle T - w_1 \rangle \oplus \mathbb{C}[T]/\langle T - w_2 \rangle \]

\[ \approx \mathbb{C} \oplus \mathbb{C} \]

for distinct \(w_j\): \((X - z)\mathcal{O}\) is an intersection of 2 prime ideals.
Example computation of integral closure: *hyperelliptic curves* (quadratic extensions of \( \mathbb{C}(X) \))

\[
Y^2 = P(X) = (X - z_1) \cdots (X - z_n) \quad \text{(distinct } z_j)\]

**Claim:** The integral closure \( \mathcal{O} \) of \( \mathfrak{o} = \mathbb{C}[X] \) in \( K = \mathbb{C}(X,Y) \) is \( \mathcal{O} = \mathbb{C}[X,Y] \).

**Proof:** Obviously \( \mathbb{C}[X,Y] \subset \mathcal{O} \). An element of \( K = \mathbb{C}(X,Y) \) can be written uniquely as \( a + bY \) with \( a, b \in \mathbb{C}(X) \). For \( b \neq 0 \), the minimal polynomial of \( a + bY \) is *monic*, with coefficients *trace* and *norm*, so integrality over \( \mathfrak{o} = \mathbb{C}[X] \) is equivalent to trace and norm in \( \mathbb{C}[X] \). The Galois conjugate of \( Y \) is \(-Y\), so

\[
2a \in \mathbb{C}[X] \quad \quad \quad \quad \quad a^2 - b^2 \cdot P \in \mathbb{C}[X]
\]

\( 2 \in \mathbb{C}[X]^{\times} \), so \( a \in \mathbb{C}[X] \). Thus, \( b^2 \cdot P \in \mathbb{C}[X] \). Since \( P \) is square-free, writing \( b = C/D \) with relatively prime polynomials \( C, D \), we find \( D \in \mathbb{C}[X]^{\times} \). Thus, \( a, b \in \mathbb{C}[X] \).

///
Completions!

Pick a constant \( C > 1 \). Doesn’t matter much...

For each \( z \in \mathbb{C} \cup \{\infty\} \), there is the \((X - z)\)-adic, or just \( z \)-adic, norm

\[
\left| (X - z)^n \cdot \frac{P(X)}{Q(X)} \right|_z = C^{-n}
\]

The \( z \)-adic completions of \( \mathbb{C}[X] \) and of \( \mathbb{C}(X) \) are defined as usual, denoted \( \mathbb{C}[[X - z]] \) and \( \mathbb{C}((X - z)) \). High powers of \( X - z \) are tiny, and any infinite sum

\[
c_0 + c_1(X - z) + c_2(X - z)^2 + c_3(X - z)^3 + \ldots \quad \text{(with } c_j \in \mathbb{C} \text{)}
\]

is convergent, by the ultrametric inequality. This warrants calling \( \mathbb{C}[[X - z]] \) a formal power series ring, and \( \mathbb{C}((X - z)) \) the field of formal finite Laurent series. But the convergence is genuine.
Hensel’s lemma applies: With monic \( F(T) \in \mathbb{C}[[X]][T] \), given \( \alpha_1 \in \mathbb{C}[[X-z]] \) with \( F(\alpha_1) = 0 \mod X-z \) with \( F'(\alpha_1) \neq 0 \mod X-z \), the recursion

\[
\alpha_{n+1} = \alpha_n - \frac{F(\alpha_n)}{F'(\alpha_n)} \mod (X-z)^{n+1}
\]

gives \( \alpha_\infty = \lim_n \alpha_n \in \mathbb{C}[[X-z]] \) with \( F(\alpha_\infty) = 0 \) in \( \mathbb{C}[[X-z]] \), and \( \alpha_\infty \) is the unique solution congruent to \( \alpha_1 \mod X-z \).

Example: Any \( \beta = c_0 + c_1(X-z) + c_2(X-z)^2 + \ldots \) with \( c_o \neq 0 \) is a unit in \( \mathbb{C}[[X-z]] \).

Proof: Take \( F(T) = \beta \cdot T - 1 \) (actually, not monic, but nevermind...) and \( \alpha_1 = c_o^{-1} \).

Example: Any \( \beta = c_0 + c_1(X-z) + c_2(X-z)^2 + \ldots \) with \( c_o \neq 0 \) has an \( n^{th} \) root in \( \mathbb{C}[[X-z]] \).

Proof: Take \( F(T) = T^n - \beta \) and \( \alpha_1 \in \mathbb{C} \) any \( \sqrt[n]{c_o} \).
Example: For \( f(X,T) \in \mathbb{C}[X,T] \), for \( z, w_o \in \mathbb{C} \) such that \( f(z, w_o) = 0 \) but \( \frac{\partial}{\partial w} f(z, w_o) \neq 0 \), there is a unique \( \alpha \in \mathbb{C}[[X - z]] \) of the form
\[
\alpha = w_o + \text{higher powers of } X - z
\]
giving
\[
f(z, \alpha) = 0
\]

**Proof:** The hypothesis is a very slight paraphrase of the hypothesis of Hensel’s lemma. ///

**Theorem:** All finite field extensions of \( \mathbb{C}((X - z)) \) are by adjoining solutions to \( Y^e = X - z \) for \( e = 2, 3, 4, \ldots \). [Pf later.]

These are (formal) *Puiseux expansions*.

The simplicity of the theorem is surprising.

It approximates the assertion that, *locally*, Riemann surfaces are either *covering spaces* of the \( z \)-plane, or concatenations of \( w^e = z \).
The local ring inside the field $\mathbb{C}(X)$ corresponding to $z \in \mathbb{C}$, consisting of all rational functions defined at $z$, is

$$\mathfrak{o}_z = \mathbb{C}(X) \cap \mathbb{C}[[X - z]]$$

with unique maximal ideal

$$\mathfrak{m}_z = \mathbb{C}(X) \cap (X - z) \cdot \mathbb{C}[[X - z]]$$

The point at infinity can be discovered by noting a further local ring and maximal ideal:

$$\mathfrak{o}_\infty = \mathbb{C}(X) \cap \mathbb{C}[[1/X]] \quad \mathfrak{m}_\infty = \mathbb{C}(X) \cap \frac{1}{X} \mathbb{C}[[1/X]]$$

Note that using $1/(X + 1)$ achieves the same effect, because

$$\frac{1}{X + 1} = \frac{1}{X} \cdot \frac{1}{1 + \frac{1}{X}} = \frac{1}{X} \cdot \left(1 - \frac{1}{X} + \left(\frac{1}{X}\right)^2 - \cdots\right) \in \frac{1}{X} \cdot \mathbb{C}[[1/X]]^\times$$