... **Commutative Algebra**...

integral extension of commutative rings $\mathfrak{O}/\mathfrak{o}$: every $r \in \mathfrak{O}$ satisfies $f(r) = 0$ for *monic* $f \in \mathfrak{o}[x]$

Recharacterization of integrality: α in a field extension K of field of fractions k of $\mathfrak{o}$ is *integral* when there is a non-zero, finitely-generated $\mathfrak{o}$-module M inside K such that $\alpha M \subset M$. [Proven]

• For $\mathfrak{O}$ integral over $\mathfrak{o}$, if $\mathfrak{O}$ is finitely-generated as an $\mathfrak{o}$-*algebra*, then it is finitely-generated as an $\mathfrak{o}$-*module*.

• *Transitivity:* For rings $A \subset B \subset C$, if B is integral over A and C is integral over B, then C is integral over A.

Example: Function fields in one variable

Claim: For a PID $\mathfrak{o}$ with fraction field k, for a finite *separable* field extension K/k, the integral closure $\mathfrak{O}$ of $\mathfrak{o}$ in K is a *free* $\mathfrak{o}$-module of rank $[K:k]$.

Comment on proof: $\mathfrak{O}$ is torsion-free as $\mathfrak{o}$-module, but *finite-generation*, to invoke the structure theorem, seems to need the *separability*:

Claim: For an *integrally closed* (in its fraction field k), *Noetherian* ring $\mathfrak{o}$, the integral closure $\mathfrak{O}$ of $\mathfrak{o}$ in a finite *separable* field extension K/k is a finitely-generated $\mathfrak{o}$-module.

Comment: For such reasons, *Dedekind domains* (below) need Noetherian-ness, as a partial substitute for PID-ness. *Separability* of field extensions seems important, too!

Claim: For a finite separable field extension K/k, the *trace pairing* $\langle \alpha, \beta \rangle = \mathrm{tr}_{K/k}(\alpha\beta)$ is *non-degenerate*, in the sense that, given $0 \neq \alpha \in K$, there is $\beta \in K$ such that $\mathrm{tr}_{K/k}(\alpha\beta) \neq 0$.

Equivalently, $\mathrm{tr}_{K/k} : K \to k$ is not the 0-map.

This follows from *linear independence of characters*: given $\chi_1, \ldots, \chi_n$ distinct group homomorphisms $K^\times \to \Omega^\times$ for fields K, Ω, for any coefficients α_j's in Ω,

$$\alpha_1\chi_1 + \ldots + \alpha_n\chi_n = 0 \implies \text{all } \alpha_j = 0$$

Corollary: For $\mathfrak{O}$ the integral closure of Noetherian, integrally closed $\mathfrak{o}$ (in its fraction field k) in a finite separable field extension K/k,

$$\mathrm{tr}_{K/k}\,\mathfrak{O} \subset \mathfrak{o}$$

Critical point in proofs of the above: *Finitely-generated* modules over Noetherian rings are Noetherian *modules*, and submodules $\mathfrak{O}$ of Noetherian modules are Noetherian, so $\mathfrak{O}$ is a finitely-generated $\mathfrak{o}$-module.

A *module* M over a commutative ring R (itself not necessarily Noetherian) is *Noetherian* when it satisfies any of the following (provably, below) equivalent conditions:

• Every submodule of M is finitely-generated.

• Every ascending chain of submodules $M_1 \subset M_2 \subset \ldots$ eventually *stabilizes*, that is, $M_i = M_{i+1}$ beyond some point.

• Any non-empty set S of submodules has a *maximal element*, that is, an element $M_o \in S$ such that $N \supset M_o$ and $N \in S$ implies $N = M_o$.

Claim: Submodules and quotient modules of Noetherian modules are Noetherian. Conversely, for $M \subset N$, if M and N/M are Noetherian, then N is. That is, in a *short exact sequence*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

(meaning that $A \to B$ is *injective*, that the image of $A \to B$ is the kernel of $B \to C$, and that $B \to C$ is *surjective*), Noetherian-ness of B is equivalent to Noetherian-ness of A and C.

Corollary: For M, N Noetherian, $M \oplus N$ is Noetherian. Arbitrary finite sums of Noetherian modules are Noetherian.

Again, a commutative *ring* R is Noetherian if it is Noetherian as a module over itself. This is equivalent to the property that every submodule (=ideal) is finitely-generated.

Claim: A finitely-generated module M over a Noetherian ring R is a Noetherian module.

Proof: Let $m_1, \ldots, m_n$ generate M, so there is a surjection $\underbrace{R \oplus \ldots \oplus R}_{n} \longrightarrow M$ by

$$r_1 \oplus \ldots \oplus r_n \longrightarrow \sum_i r_i \cdot m_i$$

The sum $R \oplus \ldots \oplus R$ is Noetherian, and the image/quotient is Noetherian. ///

This completes the discussion of the proof that the *integral closure* $\mathfrak{O}$ of *Noetherian, integrally closed* $\mathfrak{o}$ in a finite, separable field extension K/k is a *finitely-generated* $\mathfrak{o}$-module.

The end of the proof had $\mathfrak{O}$ inside a finitely-generated module:

$$\mathfrak{O} \;\subset\; c^{-1} \cdot \Big(\mathfrak{o} \cdot \alpha_1 + \ldots + \mathfrak{o} \cdot \alpha_n\Big)$$

Finitely-generated modules over Noetherian rings $\mathfrak{o}$ are Noetherian, and submodules $\mathfrak{O}$ of Noetherian modules are Noetherian, so $\mathfrak{O}$ is Noetherian, so finitely-generated. ///

Then, for $\mathfrak{o}$ a PID, since $\mathfrak{O}$ is *finitely-generated* over $\mathfrak{o}$, structure theory of finitely-generated modules over PIDs says $\mathfrak{O}$ is *free*... it's not hard to show that an $\mathfrak{o}$-basis for $\mathfrak{O}$ is also a k-basis for K...

Example: Function fields in one variable (over finite fields):

The 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 that matter, for *any* field E, $E[X]$ is Euclidean, so is a PID and a UFD. E *finite* is most similar to $\mathbb{Z}$, especially that the *residue fields are finite:* quotient $\mathbb{F}_q[X]/\langle f\rangle$ with f a *prime* (=positive-degree monic polynomial) are finite fields.

The algebra of integral closures of $\mathfrak{o} = \mathbb{F}_q[X]$ in finite separable fields extensions of $k = \mathbb{F}_q(X)$ is identical to that with $\mathbb{Z}$ and $\mathbb{Q}$ at the bottom.

But to talk about the *geometry*, it is useful to think about $\mathbb{C}[X]$...

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

That is, the point $z \in \mathbb{C}$ is the simultaneous vanishing set of the ideal $\langle X - z \rangle$.

The *point at infinity* ∞ is the vanishing set of $1/X$, but $1/X$ is not in $\mathbb{C}[X]$, so we can't talk about the ideal generated by it...

Revise: points $z \in \mathbb{C}$ are in bijection with *local rings* $\mathfrak{o} \subset \mathbb{C}(X)$, meaning $\mathfrak{o}$ has a *unique maximal (proper) ideal* $\mathfrak{m}$, by

$$z \longleftrightarrow \mathfrak{o}_z = \{\frac{P}{Q} \ : \ P, Q \in \mathbb{C}[X], \ Q(z) \neq 0\}$$

$$\mathfrak{m}_z \ = \ \{\frac{P}{Q} \ : \ P, Q \in \mathbb{C}[X], \ Q(z) \neq 0, \ P(z) = 0\}$$

That is, $\mathfrak{o}_z$ is the ring of rational functions *defined at* z, and its unique maximal ideal $\mathfrak{m}_z$ is the functions *(defined and) vanishing at* z. These are also referred to as

$$\begin{aligned} \mathfrak{o}_z &= \textit{localization} \text{ at } \langle X - z \rangle \text{ of } \mathbb{C}[X] \\ &= S^{-1} \cdot \mathbb{C}[X] \qquad\qquad (\text{where } S = \mathbb{C}[X] - (X - z)\mathbb{C}[X]) \end{aligned}$$

These *localizations* of the PID $\mathbb{C}[X]$ are still PIDs.

In fact, again, each such has a single non-zero prime ideal $\langle X - z \rangle$.

In $\mathfrak{o}_z$ every proper ideal is of the form $(X - z)^n \cdot \mathfrak{o}_z$ for some $0 < n \in \mathbb{Z}$.

Again, the unique maximal ideal is $\mathfrak{m}_z = (X - z) \cdot \mathfrak{o}_z$.

As usual, instead of trying to evaluate something at $X = \infty$, evaluate $1/X$ at 0:

$$\begin{aligned}
\mathfrak{o}_\infty &= \{f(X) = g(1/X) \ : \ g \text{ is defined at } 0\} \\
&= \{\frac{P(1/X)}{Q(1/X)} \ : \ P, Q \in \mathbb{C}[X],\ Q(0) \neq 0\}
\end{aligned}$$

$$\begin{aligned}
\mathfrak{m}_\infty &= \{f(X) = g(1/X) \in \mathfrak{o}_\infty \ : \ g(0) = 0\} \\
&= \{\frac{P(1/X)}{Q(1/X)} \ : \ P, Q \in \mathbb{C}[X],\ Q(0) \neq 0,\ P(0) = 0\}
\end{aligned}$$

From one viewpoint, a (compact, connected) *Riemann surface* M is/corresponds (!?) to a finite field extension K of $k = \mathbb{C}(X)$.

The finite 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 $\langle X - z \rangle = (X - z)\mathbb{C}[X]$ 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* $z \in \mathbb{C}$:

Proof: We can reduce to the case that $K = \mathbb{C}(X, Y)$ 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

$$\begin{aligned}
\mathfrak{O}/(X-z)\mathfrak{O} &= \mathbb{C}[X,T]/\langle X-z,\ f(X,T)\rangle \\
&\approx \mathbb{C}[T]/\langle f(z,T)\rangle \\
&\approx \mathbb{C}[T]/\langle (T-w_1)(T-w_2)\ldots(T-w_n)\rangle \\
&\approx \frac{\mathbb{C}[T]}{\langle T-w_1\rangle} \oplus \frac{\mathbb{C}[T]}{\langle T-w_2\rangle} \oplus \ldots \oplus \frac{\mathbb{C}[T]}{\langle T-w_n\rangle} \\
&\approx \mathbb{C} \oplus \mathbb{C} \oplus \ldots \oplus \mathbb{C}
\end{aligned}$$

for distinct w_j. By the Lemma proven earlier, $\mathfrak{O}/(X-z)\mathfrak{O}$ is a product of n prime ideals. ///

For example, for the *elliptic curve*

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

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

$$\begin{aligned}
\mathfrak{O}/(X-z)\mathfrak{O} \;&=\; \mathbb{C}[X,T]/\langle X - z,\; T^2 - X^3 - aX - b\rangle \\
&\approx\; \mathbb{C}[T]/\langle T^2 - z^3 - az - b\rangle \\
&\approx\; \mathbb{C}[T]/\langle (T - w_1)(T - w_2)\rangle \\
&\approx\; \frac{\mathbb{C}[T]}{\langle T - w_1\rangle} \oplus \frac{\mathbb{C}[T]}{\langle T - w_2\rangle} \\
&\approx\; \mathbb{C} \oplus \mathbb{C}
\end{aligned}$$

for distinct w_j: $\mathfrak{O}/(X-z)\mathfrak{O}$ is a product of 2 prime ideals.

To talk about *points at infinity*, either replace $\mathfrak{o} = \mathbb{C}[X]$ by $\mathfrak{o} = \mathbb{C}[1/X]$, or use the *local ring* description:

Given a *local* ring $\mathfrak{o}_z \subset k = \mathbb{C}(X)$ corresponding to either $z \in \mathbb{C}$ or $z = \infty$, let $\mathfrak{O}$ be the integral closure of $\mathfrak{o}_z$ in $K = \mathbb{C}(X, Y)$.

The maximal ideal $\mathfrak{m}_z$ of $\mathfrak{o}_z$ generates a product of prime (maximal) ideals in $\mathfrak{O}$:

$$\mathfrak{m}_z \cdot \mathfrak{O} \;=\; \mathfrak{P}_1 \ldots \mathfrak{P}_n \qquad\qquad (\text{with } n = [K : k])$$

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

$$\left|(X-z)^n \cdot \frac{P(X)}{Q(X)}\right| \;=\; C^{-n}$$

The z-adic completions of $\mathbb{C}[X]$ and $\mathbb{C}(X)$ are defined as usual.

Hensel's lemma applies.

For $\mathbb{F}_q[X]$, the *zeta function* is

$$Z(s) = \sum_{\text{monic } f} \frac{1}{(\#\mathbb{F}_p[X]/\langle f\rangle)^s} = \sum_{\text{monic } f} \frac{1}{q^{s \deg f}}$$

$$\#\text{irred monics deg } d = \frac{\#\text{ elements degree } d \text{ over } \mathbb{F}_q}{\#\text{in each Galois conjugacy class}}$$

$$= \frac{1}{d}\Big(q^d - \sum_{\text{prime } p|d} q^{d/p} + \sum_{\text{distinct } p_1, p_2|d} q^{d/p_1p_2} - \sum_{\text{distinct } p_1, p_2, p_3|d} q^{d/p_1p_2p_3} + \ldots\Big)$$

[continued...]