... Commutative Algebra...

algebraic integer $\alpha \in \overline{\mathbb{Q}}$: satisfies $f(\alpha) = 0$, $f \in \mathbb{Z}[x]$ *monic*

Dedekind domains: unique factorization of *ideals* into *prime* ideals

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

Also say α is *integral over* $\mathbb{Z}$, or simply *integral*.

In a finite algebraic field extension k of $\mathbb{Q}$, the *ring* $\mathfrak{o} = \mathfrak{o}_k$ of algebraic integers in k is

$$\mathfrak{o} = \{\alpha \in k \ : \ \alpha \text{ is integral over } \mathbb{Z}\}$$

Shown: UFD's $\mathfrak{o}$ are *integrally closed* (in their fraction fields k).

Recharacterization of integrality: Let K/k be a field extension of field of fractions k of $\mathfrak{o}$. $\alpha \in K$ is *integral over* $\mathfrak{o}$ if $f(\alpha) = 0$ for *monic* f in $\mathfrak{o}[x]$.

Recharacterization: integrality of α over $\mathfrak{o}$ is equivalent to the condition that there is a non-zero, finitely-generated (non-zero) $\mathfrak{o}$-module M inside K such that $\alpha M \subset M$. [Proven]

• For $\alpha \in K$, an algebraic field extension of the field of fractions k of $\mathfrak{o}$, for some $0 \neq c \in \mathfrak{o}$ the multiple $c \cdot \alpha$ is *integral* over $\mathfrak{o}$.

• For $\mathfrak{O}$ integral over $\mathfrak{o}$, for any ring hom f sending $\mathfrak{O}$ somewhere, $f(\mathfrak{O})$ is integral over $f(\mathfrak{o})$.

Using the *recharacterization:*

• 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.

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 $[K : k]$.

Preliminary view of proof: $\mathfrak{O}$ is certainly torsion-free as $\mathfrak{o}$-module, but how to get *finite-generation*, to invoke the structure theorem? The presence of the separability hypothesis is a hint that something is more complicated than one might imagine. It is wise to prove a technical-sounding thing:

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

Comment: For such reasons, *Dedekind domains* (below) need Noetherian-ness. Once things are not quite PIDs, Noetherian-ness is needed. *Separability* of field extensions is essential, 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.

The decisive preliminary is *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,

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

[Done]

Claim: 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,

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

Proof: Let σ_j be all the field maps $\sigma_j : K \to \overline{k}$ that are the identity map on k. Then

$$\mathrm{tr}_{K/k} = \sum_j \sigma_j$$

For $\alpha \in \mathfrak{O}$, each $\sigma_j(\alpha)$ is still integral over $\sigma(\mathfrak{o}) = \mathfrak{o}$, because homomorphisms preserve integrality. Sums of integral elements are integral, too, so $\mathrm{tr}_{K/k}(\alpha)$ is in k, by separability. Since $\mathfrak{o}$ is integrally closed in k, the trace is in $\mathfrak{o}$. ///

Recall that a commutative ring R is *Noetherian* when any of the following equivalent conditions is met:

• Any ascending chain of ideals $I_1 \subset I_2 \subset \dots$ in R *stops*, in the sense that there is n_o such that $I_n = I_{n_o}$ for $n \geq n_o$.

• Every ideal in R is a finitely-generated R-module

Example: PIDs R are Noetherian!

We will eventually need a big theorem:

Hilbert Basis Theorem: For Noetherian commutative R, the polynomial ring $R[x]$ is Noetherian.

The tangible case $R = k[x_1, \dots, x_n]$ with a field k was treated by Hilbert pre-1900. The Noetherian condition was abstracted 20+ years later by Noether.

Proof that the integral closure $\mathfrak{O}$ of Noetherian, integrally closed $\mathfrak{o}$ (in its fraction field k) in a finite, separable field extension K/k is a *finitely-generated* $\mathfrak{o}$-module... *not* assuming $\mathfrak{o}$ is a PID or Dedekind... but assuming things about Noetherian rings and modules for a moment...

Subclaim: non-degeneracy of the trace pairing $\langle \alpha, \beta \rangle = \mathrm{tr}_{K/k}(\alpha\beta)$ as a non-degenerate k-valued k-bilinear form on $K \times K$, viewing K as a k-vectorspace, implies that

$$\alpha \longrightarrow \Big(\beta \longrightarrow \langle \alpha, \beta \rangle\Big)$$

gives an *isomorphism* $K \to K^* = \mathrm{Hom}_k(K, k)$, the k-linear *dual* of K. Indeed, the non-degeneracy proves that the kernel of the map is $\{0\}$, and then dimension-counting proves it's an isomorphism.

[cont'd...]

Let $\alpha_1, \ldots, \alpha_n$ be a k-basis for K. Multiplying each α_i by a suitable $0 \neq c_i \in \mathfrak{o}$, we can assume $\alpha_i \in \mathfrak{O}$. Let α_j' be the dual basis, that is, $\langle \alpha_i', \alpha_j \rangle = \delta_{ij}$. Let $0 \neq c \in \mathfrak{o}$ be such that $c\alpha_i' \in \mathfrak{O}$ for all i.

For $\beta \in \mathfrak{O}$, $\beta \cdot c\alpha_i' \in \mathfrak{O}$, and $\mathrm{tr}(\beta \cdot c\alpha) \in \mathfrak{o}$. The coefficients $c_i \in k$ in an expression $\beta = \sum_i c_i \alpha_i$ are picked off by $\mathrm{tr}_{K/k}(\beta \cdot c\alpha_j') = cc_j$. Since $\mathfrak{o}$ is integrally closed, $cc_j \in \mathfrak{o}$. This holds for all $\beta \in \mathfrak{O}$, so

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

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

Better prove those last points about Noetherian-ness! ...
Important features of modules over Noetherian rings! ...

So, step back...: as in many sources, e.g., Lang's *Algebra*, ... This algebra is *important* in algebraic number theory, and in all forms of algebraic geometry... because Noetherian-ness is the non-negotiable thing that makes many *other* things work...

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 $M_1 \subset M_2 \subset \dots$ 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 $N = M_o$.

Proof of equivalence: Assume the first condition, and prove the second. By assumption, the $N = \bigcup_i M_i$ is finitely-generated, by some $m_1, \ldots, m_n$. Each m_i occurs in some one of the M_j, so there is some index j so that *all* m_i are in M_j. Thus, $M_j = M_{j+1} = \ldots$.

Assume the second condition, and prove the third. Take $M_1 \in S$. If it is maximal, we're done. If not, let $M_2 \supset M_1$ be strictly larger. By induction, either construct an infinite ascending chain, which is assumed impossible, or find a maximal element.

Assume the third condition, and prove the first. Fix a submodule N of M. If a given element $n_1 \in N$ generates N, we're done, otherwise choose $n_2 \in N$ but not in $\langle n_1 \rangle$. Continuing, either we find a finite set of generators for N, or obtain a ascending chain

$$\langle n_1 \rangle \subset \langle n_1, n_2 \rangle \subset \ldots$$

By assumption, the set of these has a maximal element, some $\langle n_1, \ldots, n_j \rangle$, which is N, proving finite generation. ///

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.

Proof: The first characterization of Noetherian-ness gives the assertion for submodules. For quotients $q : N \to Q$, for any chain $Q_1 \subset Q_2 \subset \ldots$ inside Q, the inverse images $q^{-1}Q_i$ make a chain in N, which must stabilize, proving that the images stabilize.

Conversely, attach to $X \subset N$ the pair $pX = (X \cap M, (X + M)/M)$. We claim that a chain $X_1 \subset X_2 \subset \ldots$ stabilizes if and only if $X_i \cap M$ and $(X_i + M)/M$ stabilize: *Subclaim:* if $X \subset Y$ and $pX = pY$, then $X = Y$. Indeed, for $y \in Y$, $(X + M)/M = (Y + M)/M)$ implies existence of $m \in M$ and $x \in X$ such that $x + m = y$. Thus,

$$x - y \;=\; -m \;\in\; Y \cap M \;=\; X \cap M$$

Then $y = x + m \in X + (X \cap M) \subset X$, proving the subclaim. For $X_1 \subset X_2 \subset \ldots$, the associated pairs are ascending chains in M and N/M, so stabilize, and then X_i stabilizes. ///

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.

Proof: $0 \to M \to M \oplus N \to N \to 0$ is exact. Induction. ///

Now we need to connect to (probably finitely-generated) modules over a *Noetherian ring*. The Noetherian-ness of the ring itself has a (not-surprising) impact on the behavior of modules over it.

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, that is, every 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. ///

Don't forget: 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 $\mathfrak{O}$ sitting inside a finitely-generated module:

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

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

Finally, this returns to the proof that, for $\mathfrak{o}$ a PID, $\mathfrak{O}$ is a *free* $\mathfrak{o}$-module of rank $[K : k]$.

By now, we know that $\mathfrak{O}$ is *finitely-generated* over $\mathfrak{o}$. It is *torsionless* because $\mathfrak{o} \subset \mathfrak{O} \subset K$, a field. Invoking the structure theory of finitely-generated modules over PIDs, $\mathfrak{O}$ is *free*. Let $\alpha_1, \ldots, \alpha_n$ be an $\mathfrak{o}$-basis.

We claim that $\{\alpha_i\}$ is also a k-basis for K, which would prove $[K : k] = n$. They *span*, because, given $\beta \in K$, there is $0 \neq c \in \mathfrak{o}$ such that $c\beta \in \mathfrak{O}$. There are $c_j \in \mathfrak{o}$ such that $c\beta = \sum_i c_j \alpha_j$. Then $\beta = \sum_i c^{-1} c_j \alpha_i$.

They are *linearly independent* over k: for $\sum_i x_i \alpha_i = 0$ with $x_i \in k$, take $0 \neq c \in k$ such that all $cx_i \in \mathfrak{o}$. Then $\sum_i (cx_i)\alpha_i = 0$ is a non-trivial relation over $\mathfrak{o}$, contradiction. ///
