We will later elaborate the ideas mentioned earlier: relations of primes to zeros of zetas, reciprocity laws, p-adic and adelic methods. Now... **Commutative Algebra**: again,

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* $f \in \mathfrak{o}[x]$

prime (ideal) $\mathfrak{P}$ of $\mathfrak{O}/\mathfrak{o}$ *lying over* prime ideal $\mathfrak{p}$ of $\mathfrak{o}$, and *residue field* extension $\mathfrak{O}/\mathfrak{P}$ over $\mathfrak{o}/\mathfrak{p}$. Galois theory!

Helpful auxiliary ideas: *localization* S^{-1} of a ring $\mathfrak{o}$ to force invertibility of elements of S, and v-adic *completions* $\mathfrak{o}_v, k_v$ of $\mathfrak{o}$ and fraction field k, to squash field extensions of k.

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

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

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

Example: Inside quadratic field extensions $k = \mathbb{Q}(\sqrt{D})$ of $\mathbb{Q}$, with D a square-free integer.

$$\mathfrak{o} \;=\; \begin{cases} \mathbb{Z}[\sqrt{D}] & (\text{for } D = 2, 3 \bmod 4) \\ \mathbb{Z}[\frac{1+\sqrt{D}}{2}] & (\text{for } D = 1 \bmod 4) \end{cases}$$

Example: Cyclotomic fields $k = \mathbb{Q}(\omega)$, where ω is a primitive n^{th} root of unity. In fact, $\mathfrak{o} = \mathbb{Z}[\omega]$, not so easy to prove for $n \geq 5$.

Example: Adjoining roots, for example, prime p-order roots $k = \mathbb{Q}(\sqrt[p]{D})$ of square-free integers D. For $D \neq 1 \bmod p^2$, in fact, $\mathfrak{o} = \mathbb{Z}[\sqrt[p]{D}]$. For $D = 1 \bmod p^2$, in parallel with the square-root story, $\mathfrak{o}$ is of index p above $\mathbb{Z}[\sqrt[p]{D}]$, also containing

$$\frac{1 + \sqrt[p]{D} + \ldots + \sqrt[p]{D}^{p-1}}{p}$$

For example, the ring $\mathfrak{o}$ of integers in $\mathbb{Q}(\sqrt[3]{10})$ is

$$\mathfrak{o} \;=\; \mathbb{Z} \;+\; \mathbb{Z} \cdot \sqrt[3]{10} \;+\; \mathbb{Z} \cdot \frac{1 + \sqrt[3]{10} + \sqrt[3]{10}^2}{3}$$

Why are these *rings*? Why are sums and products of algebraic integers again integral?

This issue is similar to the issue of proving that sums and products of *algebraic* numbers α, β (over $\mathbb{Q}$, for example) are again *algebraic*. Specifically, do *not* try to explicitly find a polynomial P with rational coefficients and $P(\alpha + \beta) = 0$, in terms of the minimal polynomials of α, β.

The methodological point in the latter is first that it is not *required* to explicitly determine the minimal polynomial of $\alpha + \beta$.

Second, about algebraic extensions, to *avoid* computation, *recharacterization* of the notion of *being algebraic over...* is needed: an element α of a field extension K/k is *algebraic* over k if $k[\alpha]$, the ring of values of polynomials on α, is a finite-dimensional k-vectorspace.

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 $\mathfrak{o}[x]$.

The *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 last time.]

Corollary: In an algebraic field extension K/k, where k is the field of fractions of a ring $\mathfrak{o}$, the set $\mathfrak{O}$ of elements of K *integral* over $\mathfrak{o}$ is a *ring*.

Somewhat as in the basics of *algebraic field theory*, some unexciting things need to be checked. First, from the monic-polynomial definition,

• 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.

Let's prove the less-intuitive facts that need the recharacterization:

For $\mathfrak{O}$ finitely-generated as an $\mathfrak{o}$-*algebra*, use induction on the number of algebra generators. This reduces to the step where $\mathfrak{O} = \mathfrak{o}[\alpha]$, and α is integral over $\mathfrak{o}$. Ah! But proving that $\mathfrak{o}[\alpha]$ is a finitely-generated $\mathfrak{o}$-*module* in this induction step is exactly the recharacterization of integrality! Ha. ///

Use the previous to prove the more interesting-sounding *transitivity* of integrality. In $A \subset B \subset C$, any $z \in C$ satisfies an integral equation $z^n + b_{n-1}z^{n-1} + \ldots + b_1 z + b_o = 0$ with $b_i \in B$. The ring $B' = A[b_{n-1}, \ldots, b_o]$ is a finitely-generated A-*algebra*, so by the previous it is a finitely-generated A-*module*. Since z satisfies that monic, $B'[z]$ is also a finitely-generated A-*module*. And since z satisfies that monic, multiplication by z stabilizes $B'[z]$. The latter is finitely-generated over A, so z is integral over A. ///

Caution: Returning to the point that it would be a fatal mistake to ignore the notion of integrality, for example, by discarding algebraic numbers that *are* integral over $\mathbb{Z}$, but meet naive expectations:

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

Proof: Let a/b be integral over $\mathfrak{o}$, satisfying

$$(a/b)^n + c_{n-1}(a/b)^{n-1} + \ldots + c_o \;=\; 0$$

with $c_i \in \mathfrak{o}$. Multiplying out,

$$a^n + c_{n-1}a^{n-1}b + \ldots + b^n c_o \;=\; 0$$

If a prime π in $\mathfrak{o}$ divides b, then it divides a^n, and, thus divides a, by unique factorization. Thus, taking a/b *in lowest terms* shows that b is a unit. ///

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. In fact, 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!

Separability: This is 'just' field theory... Recall: α in an algebraic field extension K/k is *separable* over k when its minimal polynomial over k has no repeated factors. Equivalently, there are $[k(\alpha) : k]$ *different* imbeddings of $k(\alpha)$ into an algebraic closure $\overline{k}$.

A finite field extension K/k is *separable* when there are $[K : k]$ different imbeddings of K into $\overline{k}$.

The *theorem of the primitive element* asserts that a finite separable extension can be generated by a single element.

A less-often emphasized, but important, result:

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.

For fields of characteristic 0, this non-degeneracy is easy: for $[K:k]=n$ and for $\alpha\in k$,

$$\mathrm{tr}_{K/k}\frac{1}{n}\alpha \;=\; \frac{1}{n}\mathrm{tr}_{K/k}\alpha \;=\; \frac{1}{n}(\underbrace{\alpha+\ldots+\alpha}_{n}) \;=\; \alpha$$

But we need/want this non-degeneracy for finite fields $\mathbb{F}_q$ and for *function fields* $\mathbb{F}_q(x)$, in positive characteristic.

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,

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

Proof: Suppose $\alpha_1\chi_1 + \ldots + \alpha_n\chi_n = 0$ is the *shortest* such non-trivial relation, renumbering so that no $\alpha_j = 0$. The meaning of the equality is that

$$\alpha_1\chi_1(x) + \ldots + \alpha_n\chi_n(x) \;=\; 0 \in \Omega \qquad\qquad (\text{for all } x \in K^\times)$$

Since $\chi_1 \neq \chi_2$, there is $y \in K^\times$ such that $\chi_1(y) \neq \chi_2(y)$. Replace x by xy:

$$\alpha_1\chi_1(y)\chi_1(x) + \ldots + \alpha_n\chi_n(y)\chi_n(x) \;=\; 0 \qquad\qquad (\text{for all } x \in K^\times)$$

Divide the latter relation by $\chi_1(y)$, and subtract from the first:

$$\alpha_2\big(1 - \chi_2(y)\big)\chi_2 + \ldots + \alpha_n\big(1 - \chi_n(y)\big)\chi_n \;=\; 0$$

This is shorter, contradiction. ///

To prove that the Galois trace map on a finite separable K/k is not identically 0, observe that the distinct field imbeddings $\sigma_j : K \to \overline{k}$ *are* (distinct) multiplicative characters $K^\times \to \overline{k}^\times$.

Trace is $\mathrm{tr}_{K/k} = \sum_j \sigma_j = \sum_j 1 \cdot \sigma_j$. This linear combination is not identically 0. ///

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

• Any ascending chain of ideals $I_1 \subset I_2 \subset \ldots$ 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!

Proof: Let $\bar{x}_1\rangle \subset \langle x_2\rangle \subset \ldots$ be a chain of (principal!) ideals. Let I be the *union* I. It is a principal ideal $\langle y\rangle$. There is a *finite* expression $y = r_1 x_{i_1} + \ldots + r_n x_{i_n}$ with $r_i \in R$. Letting j be the max of the i_ℓ's, all x_{i_j}'s are in $\langle x_j\rangle$, so $y \in \langle x_j\rangle$, and the chain stabilizes at $\langle x_j\rangle$. ///
