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**:

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* $S^{-1}\mathfrak{o}$ 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* (why!?!?) $\mathfrak{o} = \mathfrak{o}_k$ 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. Reasonably-enough, $\alpha = a + b\sqrt{D}$ with $a, b \in \mathbb{Z}$ is integral, satisfying

$$\alpha^2 - 2a\alpha + (a^2 - b^2 D) \;=\; 0$$

For $D = 1 \bmod 4$, there are *more* algebraic integers in $\mathbb{Q}(\sqrt{D})$ ...

Let tr and N be Galois trace and norm $k \to \mathbb{Q}$. In terms of these, we know the minimal polynomial for α is $x^2 - \mathrm{tr}\alpha \cdot x + N\alpha$. Thus, in a quadratic extension, α is an algebraic integer if and only both *trace* and *norm* are in $\mathbb{Z}$. Write $\alpha = a + b\sqrt{D}$ with $a, b \in \mathbb{Q}$.

The integrality condition is that $2a \in \mathbb{Z}$ and $a^2 - b^2 D \in \mathbb{Z}$. Try to *solve* for *rational integrality* conditions on a, b.

From the first condition, at worst $a \in \frac{1}{2}\mathbb{Z}$. With $a = a'/2$ and $b = b'/2$, the second condition becomes $a'^2 - b'^2 D \in 4\mathbb{Z}$.

Since the only squares mod 4 are $0, 1$, for $D = 2, 3 \bmod 4$ actually $a', b' \in 2\mathbb{Z}$, so $a, b \in \mathbb{Z}$.

But for $D = 1 \bmod 4$, the condition is met for $a' = b' \bmod 2$!!!

That is, the ring $\mathfrak{o}$ of algebraic integers in $k = \mathbb{Q}(\sqrt{D})$ for square-free integer D is

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

Indeed, we already knew an example of the sense of this: the cube root of unity $\omega = \frac{-1+\sqrt{-3}}{2}$ satisfies $\omega^2 + \omega + 1 = 0$.

Caution: We will see that *ignoring* these 'extra' algebraic integers would be a fatal mistake: the resulting rings are very bad, *not* Dedekind rings, exactly because they are *not integrally closed*, that is, they omit elements of their *fraction fields* integral over $\mathbb{Z}$.

Example: Cyclotomic fields $k = \mathbb{Q}(\omega)$, where ω is a primitive n^{th} root of unity. Since cyclotomic polynomials Φ_n are monic with integer coefficients, certainly ω is an algebraic integer.

So the ring $\mathfrak{o}$ of algebraic integers in $k = \mathbb{Q}(\omega)$ *contains* $\mathbb{Z}[\omega]$.

In fact, $\mathfrak{o} = \mathbb{Z}[\omega]$, but this is not so easy to prove for $n \geq 5$.

The sane proof uses ideas about *localization*, *completion*, *discriminant*, *different* [sic], and *ramification*.

It is a fool's errand to try to prove $\mathfrak{o} = \mathbb{Z}[\omega]$ by writing out the minimal polynomial of $a + b\omega + c\omega^2 + \ldots$ and examining the integrality conditions.

Example: Adjoining roots, for example, prime p-order roots $k = \mathbb{Q}(\sqrt[p]{D})$ of square-free integers D. Certainly $\sqrt[p]{D}$ is an algebraic integer, so the ring $\mathfrak{o}$ of algebraic integers *contains* $\mathbb{Z}[\sqrt[p]{D}]$.

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 $\mathbb{Z}[\sqrt[3]{D}]$, 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

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

As with cyclotomic fields, it is unwise to try prove this *directly*.

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, $\mathfrak{o}$ a ring in k with field of fractions k.

We already know that $\alpha \in K$ is *integral over* $\mathfrak{o}$ if $f(\alpha) = 0$ for *monic* f in $\mathfrak{o}[x]$.

Claim: Integrality of α over $\mathfrak{o}$ is equivalent to the condition that there is a non-zero, finitely-generated $\mathfrak{o}$-module M inside K such that $\alpha M \subset M$.

Proof: On one hand, for α integral, with $n = [k(\alpha) : k]$, the $\mathfrak{o}$-module generated by $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ is finitely-generated and is stabilized by α...

On the other hand, suppose $\alpha M \subset M$, where M has $\mathfrak{o}$-generators $m_1, \ldots, m_n$. Then there are $c_{ij} \in \mathfrak{o}$ such that $\alpha m_i = \sum_j c_{ij} m_j$, giving a system of n linear equations inside the field K:

$$\left\{ \begin{array}{ccccccccc} \alpha m_1 & = & c_{11} m_1 & + & c_{12} m_2 & + \ldots + & c_{1n} m_n \\ & \ldots & & & & & \\ \alpha m_n & = & c_{n1} m_1 & + & c_{n2} m_2 & + \ldots + & c_{nn} m_n \end{array} \right.$$

or

$$\left\{ \begin{array}{ccccccc} 0 & = & (c_{11} - \alpha) m_1 & + & c_{12} m_2 & + \ldots + & c_{1n} m_n \\ & \ldots & & & & & \\ 0 & = & c_{n1} m_1 & + & c_{12} m_2 & + \ldots + & (c_{nn} - \alpha) m_n \end{array} \right.$$

Existence of a non-zero solution $m_1, \ldots, m_n$ implies vanishing of determinant of

$$\begin{pmatrix} (c_{11} - \alpha) & c_{12} & \ldots & c_{1n} \\ & & \ldots & \\ c_{n1} & c_{12} & \ldots & (c_{nn} - \alpha) \end{pmatrix}$$

giving a monic equation satisfied by α !!! ///

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*.

Proof: Let $\alpha, \beta \in \mathfrak{O}$, stabilizing non-zero, finitely-generated $\mathfrak{o}$-modules $M = \langle m_1, \ldots, m_\mu \rangle$ and $N = \langle n_1, \ldots, n_\nu \rangle$. Then the $\mathfrak{o}$-module $M \cdot N$ generated by all products $m_i n_j$ is non-zero, finitely-generated, and is stabilized by $\alpha + \beta$ and by $\alpha \cdot \beta$ (!) ///

Corollary: In the field extension $\overline{\mathbb{Q}}/\mathbb{Q}$, the collection of all algebraic integers really is a *ring*. ///

For a ring $\mathfrak{o}$ inside a field K, the ring $\mathfrak{O}$ of all elements of K *integral over* $\mathfrak{o}$ is the **integral closure** of $\mathfrak{o}$ in K.

Somewhat in parallel to development of 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, by unique factorization. Thus, taking a/b *in lowest terms* shows that b is a unit. ///