Contents

0 Algebraic Number Theory **1**

0.1 (Sep 4) Overview, Number Fields and Algebraic Integers 1

0.2 (Sep 5) Rings of Integers, Trace and Norm 1 3

0.3 (Sep 9) Complex Embeddings, Trace and Norm 2 5

0.4 (Sep 11) The Group Structure of $\mathcal{O}_K$, Discriminants 1 8

0.5 (Sep 12) Discriminants 2 11

0.6 (Sep 16) Constructing Integral Bases for $\mathcal{O}_K$ 13

0.7 (Sep 18) Some Examples of Integral Bases for $\mathcal{O}_K$ 16

0.8 (Sep 19) The Ring of Integers in $\mathbb{Q}(\zeta_n)$ 18

0 Algebraic Number Theory

These are lecture notes for the graduate course Math 7315: Algebraic Number Theory, taught at Northeastern in Fall 2024.

0.1 (Sep 4) Overview, Number Fields and Algebraic Integers

- The goal of this course is to provide an introduction to algebraic number theory, which (broadly speaking) uses the language and tools of abstract algebra to study number theory.
    - To illustrate, here are some fundamental things from classical number theory: primes, unique factorizations, congruences and modular arithmetic, Fermat's and Euler's theorems, the prime number theorem, quadratic reciprocity (and higher reciprocity), and the prime number theorem.
    - It was observed in the 1700s and early 1800s that many of these same ideas extend in fundamentally similar ways to other kinds of numbers beyond the integers – various natural examples being the Gaussian integers, other kinds of algebraic numbers such as the nth roots of unity, and polynomials with coefficients in the field $\mathbb{F}_p$.
    - However, it was not until some of the fundamental constructions from abstract algebra were better understood that these ideas coalesced into an understandable form – precisely, the central ideas are the closely-related notions of a ring, a module, and of an integral extension – which arose between the 1860s and 1880s in the work of Dedekind and Kronecker, and were extended greatly over the subsequent decades by Noether, Hilbert, Krull, and others.
    - As a matter of history, the questions we will study about unique factorization and algebraic number fields motivated the development of a great deal of abstract algebra, but we will reverse the historical trend and start by developing the needed algebraic facts before applying them to study number theory.
- Our general goal is to study the problem of unique factorization (and quite often its failure!) in the ring of integers of a number field.
    - Now, one may certainly adopt the position that the existence or nonexistence of unique factorization in an integral domain is already an intrinsically interesting question by itself, but the question is rather trivialized simply by noting that such rings are, by definition, unique factorization domains.

- The more specific question of whether we can tell if a particular ring has unique factorization is more interesting, but still, we are really interested only in rings of interest for their utility in answering questions about number theory.
- So let us first formulate the proper class of rings that we will study.

- Definition: A number field is a field extension $K/\mathbb{Q}$ whose vector space dimension over $\mathbb{Q}$ is finite.
  - Equivalently, a number field is a finite-degree extension of $\mathbb{Q}$.
  - Since the complex field $\mathbb{C}$ is algebraically closed and contains $\mathbb{Q}$, by standard facts about algebraic field extensions, K can be embedded into $\mathbb{C}$.
  - As such, we may equivalently think of a number field as a subfield of $\mathbb{C}$ that has finite degree over $\mathbb{Q}$.

- Example: The quadratic field $\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} : a, b \in \mathbb{Q}\}$ for any squarefree integer $D \neq 1$ is a number field of degree 2 over $\mathbb{Q}$.
  - For positive D the field $\mathbb{Q}(\sqrt{D})$ is a real quadratic field, while for negative D the field $\mathbb{Q}(\sqrt{D})$ is an imaginary quadratic field.
  - We could spend a tremendous amount of time just studying properties of factorization in quadratic fields, since even by themselves they already provide interesting examples of unique and non-unique factorization.
  - As is well known (and which we will prove properly later), the ring $\mathbb{Z}[i]$ of Gaussian integers, which is a subring of the quadratic field $\mathbb{Q}(i)$, has unique factorization.
  - On the other hand, in $\mathbb{Z}[\sqrt{-3}]$, a subring of $\mathbb{Q}(\sqrt{-3})$, we have $4 = 2 \cdot 2 = (1 + \sqrt{-3}) \cdot (1 - \sqrt{-3})$, and these two factorizations are inequivalent because the terms are all irreducible but are not associates of one another.
  - However, this "example" is not really so interesting, because inside the corresponding field $\mathbb{Q}(\sqrt{-3})$ there does exist a subring where these two factorizations are equivalent up to unit factors: namely, the subring $\mathbb{Z}[\omega] = \mathbb{Z}[\frac{-1 + \sqrt{-3}}{2}]$.
  - More interestingly, in the ring $\mathbb{Z}[\sqrt{-5}]$, a subring of $\mathbb{Q}(\sqrt{-5})$, we have a similar lack of unique factorization: $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$. Yet as we will see, there is no similar way to "enlarge" this subring (while still maintaining the desired kind of integrality of the elements) in order to salvage unique factorization of elements.

- Example: For a primitive nth root of unity ζ_n such as $\zeta_n = e^{2\pi i/n}$, the cyclotomic field $\mathbb{Q}(\zeta_n)$ is a number field of degree $\varphi(n)$ over $\mathbb{Q}$, since the minimal polynomial of ζ_n over $\mathbb{Q}$ is the nth cyclotomic polynomial which has degree $\varphi(n)$.
  - There are many properties of the roots of unity, and some simple ones lead to relations among the cyclotomic fields.
  - Exercise: If a and b are relatively prime, show that $\mathbb{Q}(\zeta_{ab}) = \mathbb{Q}(\zeta_a, \zeta_b)$. Deduce that $\mathbb{Q}(\zeta_{2n}) = \mathbb{Q}(\zeta_n)$ for odd integers n. Do there exist distinct even integers $2m$ and $2n$ such that $\mathbb{Q}(\zeta_{2m}) = \mathbb{Q}(\zeta_{2n})$?

- We can generalize the two examples above rather substantially:

- Example: For any irreducible polynomial $p(x) \in \mathbb{Q}[x]$ of degree n with a complex root α, the field $\mathbb{Q}(\alpha) = \{c_0\alpha + \cdots + c_{n-1}\alpha^{n-1} : c_i \in \mathbb{Q}\}$ generated by α over $\mathbb{Q}$ is a number field of degree n.
  - In fact, every number field is really of this form:
  - Exercise: Suppose $K/\mathbb{Q}$ is a number field. Show that $K = \mathbb{Q}(\alpha)$ for some complex number α. [Hint: Apply the primitive element theorem.]

- Now, in order to discuss unique factorization fruitfully, we need to identify the analogue of the integers $\mathbb{Z}$ inside our number field K, which will give us (in a very strong sense) the "proper" subring of K in which to consider factorizations:

- Definition: For a number field K, an algebraic number $\alpha \in K$ is an algebraic integer if there exists a monic polynomial $p(x)$ with integer coefficients such that $p(\alpha) = 0$.
  - Examples: Integers are algebraic integers, as are $\sqrt{2}$ and i, and more generally $a^{1/n}$ for any integer a and positive integer n. The roots of $x^3 - x - 1 = 0$ are algebraic integers.
  - Indeed, it is not so trivial to show that a given complex number is *not* an algebraic integer using this definition, since it would require showing that there is no monic polynomial with integer coefficients of which it is a root.
  - Let us give a better way to determine whether an algebraic number is an algebraic integer, while also reviewing some properties of algebraic numbers in general:

- Proposition (Algebraic Integers I): Suppose α is an algebraic number, so that α is the root of some nonzero polynomial $q(x) \in \mathbb{Q}[x]$.

  1. The set of all polynomials $p(x) \in \mathbb{Q}[x]$ for which $p(\alpha) = 0$ is an ideal of $\mathbb{Q}[x]$. The unique monic generator $m(x)$ of this ideal is the minimal polynomial of α, and is the unique monic polynomial in $\mathbb{Q}[x]$ of smallest degree having α as a root.
     - Proof: It is easy to see that the set of $p(x)$ with $p(\alpha) = 0$ is an ideal. Since $\mathbb{Q}[x]$ is a principal ideal domain, this ideal is principal, and therefore has a unique monic generator.
     - Since $m(x)$ divides all elements of this ideal, its degree is smallest among all nonzero elements of the ideal.
     - Exercise: Show that the minimal polynomial $m(x)$ is irreducible in $\mathbb{Q}[x]$.
  2. The algebraic number α is an algebraic integer if and only if its minimal polynomial (over $\mathbb{Q}$) has integer coefficients.
     - Proof: If the minimal polynomial $m(x)$ has integer coefficients, then $m(x)$ itself is a monic polynomial with integer coefficients of which α is a root, so obviously α is an algebraic integer.
     - Conversely, suppose α is an algebraic integer. Let $p(x)$ be the monic polynomial of minimal degree such that $p(\alpha) = 0$ and $p(x)$ has integer coefficients. If $p(x)$ were reducible in $\mathbb{Q}[x]$, then by Gauss's lemma[1] $p(x)$ would have a factorization in $\mathbb{Z}[x]$: say $p(x) = f(x)g(x)$. But then at least one of f and g would have α as a root, contradicting the minimality of p.
     - Thus p is irreducible. Now, since $p(\alpha) = 0$, we see that $m(x)$ divides $p(x)$, so since p is irreducible we must have $p(x) = c \cdot m(x)$ for some $c \in \mathbb{Q}$, but as both p and m are monic, we have $c = 1$. Thus, $m(x) \in \mathbb{Z}[x]$ as claimed.

0.2 (Sep 5) Rings of Integers, Trace and Norm 1

- Using the criterion in (2) above allows us to compute the algebraic integers in a number field K by finding the elements of K whose minimal polynomials have integer coefficients.
  - Exercise: Show that the set of algebraic integers of $\mathbb{Q}$ is $\mathbb{Z}$.
  - Exercise: Suppose D is squarefree. Show that the set of algebraic integers of $\mathbb{Q}(\sqrt{D})$ is $\mathbb{Z}[\sqrt{D}]$ when $D \equiv 2, 3 \pmod 4$ and that it is $\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ when $D \equiv 1 \pmod 4$. [Hint: First verify that for $b \neq 0$ the minimal polynomial of $a + b\sqrt{D}$ is $m(x) = x^2 - 2a + (a^2 - Db^2)$, and then classify when the coefficients are integers.]

- In the examples above note that the algebraic integers in these number fields both form rings. In fact, the algebraic numbers in any number field always form a ring, as we will now show.
  - After noting rather obviously that 0 is an algebraic integer and the negative of an algebraic integer is an algebraic integer, the claimed fact is equivalent to proving that the set of algebraic integers is closed under addition and multiplication.

[1] The formulation of Gauss's lemma we use here is that if a polynomial with integer coefficients factors in $\mathbb{Q}[x]$, then in fact it factors in $\mathbb{Z}[x]$.

- This fact can be proven directly from the definition using rather tedious polynomial elimination: the idea is that if α and β are algebraic integers with integer polynomials p, q with $p(\alpha) = q(\beta) = 0$, then one may do polynomial elimination on the sets $\{p(x), q(y), z - x - y\}$ and $\{p(x), q(y), z - xy\}$ to obtain a single monic polynomial in z with integer coefficients in each case, which then establishes that $\alpha + \beta$ and $\alpha\beta$ are algebraic integers.
- But this approach is very tedious to implement in practice, and is not particularly enlightening. Let us give a much more natural approach using modules.

- Proposition (Rings of Integers): Suppose K is a number field.

  1. For $\alpha \in K$, the following are equivalent:
     (a) α is an algebraic integer.
     (b) The ring $\mathbb{Z}[\alpha]$ is finitely generated as an additive group (i.e., as a $\mathbb{Z}$-module).
     (c) α is an element of some subring of $\mathbb{C}$ that is finitely generated as an additive group.
     (d) There exists some finitely generated additive subgroup G of $\mathbb{C}$ with $\alpha G \subseteq G$.
     - Proof: $(a) \Rightarrow (b)$: If the minimal polynomial of α is $m(x) = x^n + c_n x^{n-1} + \cdots + c_1 x + c_0$ then we claim $\{1, \alpha, \ldots, \alpha^{n-1}\}$ generates $\mathbb{Z}[\alpha]$ as an additive group. To see this it suffices to observe that each power of α is an integral linear combination of $\{1, \alpha, \ldots, \alpha^{n-1}\}$, which follows by an easy induction relying on the fact that $\alpha^n = -c_0 - c_1\alpha - \cdots - c_n\alpha^{n-1}$.
     - $(b) \Rightarrow (c)$: Obvious, since $\alpha \in \mathbb{Z}[\alpha]$.
     - $(c) \Rightarrow (d)$: Obvious by taking L to be the given subring.
     - $(d) \Rightarrow (a)$: Suppose G is generated by $\beta_1, \ldots, \beta_n$. Then $\alpha\beta_1, \ldots, \alpha\beta_n$ are all elements of G hence can be expressed as integral linear combinations of $\beta_1, \ldots, \beta_n$: thus, $\alpha \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix} = M \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix}$ for an appropriate $M \in M_{n\times n}(\mathbb{Z})$. This means α is an eigenvalue of the matrix M, and so the characteristic polynomial $p(x) = \det(xI - M)$ has α as a root; as M has integer entries, $p(x)$ is then a monic polynomial with integer coefficients having α as a root.
  2. The set of all algebraic integers forms a ring. The set of algebraic integers in K also forms a ring, which is called the ring of integers of K and is denoted $\mathcal{O}_K$.
     - Proof: Suppose α and β are algebraic integers. Then $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are finitely-generated $\mathbb{Z}$-modules, hence so is $\mathbb{Z}[\alpha, \beta]$ since it is generated by the pairwise products of the generating sets. Hence so are the submodules $\mathbb{Z}[\alpha - \beta]$ and $\mathbb{Z}[\alpha\beta]$.
     - We deduce that the set of all algebraic integers is closed under subtraction and multiplication, so it is ring. The intersection of it with K is therefore also a ring.
     - Remark: All of the argument above can be made completely explicit: if $\mathbb{Z}[\alpha]$ has basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$ and $\mathbb{Z}[\beta]$ has basis $\{1, \beta, \ldots, \beta^{m-1}\}$ then $\mathbb{Z}[\alpha, \beta]$ is spanned by $\{\alpha^i\beta^j\}_{1\le i\le n, 1\le j\le mn}$. Then to compute a polynomial with, say, $\alpha + \beta$ as a root, simply compute the coefficients of multiplication by $\alpha + \beta$ on this spanning set, and evaluate the appropriate determinant.
     - Exercise: Use the procedure described above to find a monic integer polynomial satisfied by $\sqrt{2} + \sqrt[3]{3}$ and by $\sqrt{2} \cdot (\sqrt[3]{3} - 1)$.
  3. For every element $\alpha \in K$ there is some nonzero $d \in \mathbb{Z}$ such that $d\alpha$ is an algebraic integer.
     - Proof: Suppose that the minimal polynomial of α is $m(x) = x^n + c_n x^{n-1} + \cdots + c_1 x + c_0 \in \mathbb{Q}[x]$ and let d be the lcm of the denominators appearing in m.
     - Then $0 = d^n m(\alpha) = (d\alpha)^n + c_n d(d\alpha)^{n-1} + \cdots + c_1 d^{n-1}(d\alpha) + c_0 d^n$, so for $\tilde{m}(x) = x^n + c_n d x^{n-1} + \cdots + c_1 d^{n-1} x + c_0 d^n$ we see $\tilde{m}(d\alpha) = 0$. Since $\tilde{m}$ has integer coefficients, we see $d\alpha$ is an algebraic integer, as claimed.
     - Exercise: Show that K is the fraction field of its ring of integers $\mathcal{O}_K$.

- We would like now to study further the structure of the ring of integers $\mathcal{O}_K$, both additively and multiplicatively. In order to do this efficiently, we require a few additional tools from the basic theory of algebraic field extensions, the first two of which are the trace and norm maps. We will give a few different approaches for these constructions.

- The most natural is for Galois extensions, so suppose K/F is a Galois extension with Galois group G. For an element $\alpha \in K$, we define the trace of α to be $\mathrm{tr}_{K/F}(\alpha) = \sum_{g\in G} g(\alpha)$ and the norm to be $N_{K/F}(\alpha) = \prod_{g\in G} g(\alpha)$. In other words, the trace is the sum of all the Galois conjugates of α, while the norm is the product of all the Galois conjugates of α.
- It is easy to see that both the trace and norm are Galois-invariant (simply reindex the sum), so the trace and norm are in fact both elements of the base field F.
- The main reason we are interested in these maps is that the trace is additive and F-linear, while the norm is multiplicative: $\mathrm{tr}_{K/F}(\alpha + c\beta) = \mathrm{tr}_{K/F}(\alpha) + c\mathrm{tr}_{K/F}(\beta)$ for any $c \in F$, and $N_{K/F}(\alpha\beta) = N_{K/F}(\alpha)N_{K/F}(\beta)$, as is easily seen by the definitions (note $g(c) = c$ since $c \in F$).
- Thus, the trace and norm give us convenient ways to relate the respective multiplicative and additive structures of the larger field K to the smaller field F.
- Example: For $K = \mathbb{Q}(\sqrt{D})$ and $L = \mathbb{Q}$, which is Galois with Galois group $G \cong \mathbb{Z}/2\mathbb{Z}$ generated by the conjugation map $\sigma(a + b\sqrt{D}) = a - b\sqrt{D}$, we have $\mathrm{tr}(a + b\sqrt{D}) = 2a$ and $N(a + b\sqrt{D}) = a^2 - Db^2$.

- However, not all extensions are Galois (including many number field extensions we will be interested in, such as $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$). To extend our definitions to this more general situation, suppose now we only have a separable finite-degree extension K/F and suppose $\hat{K}/F$ is its Galois closure (i.e., the smallest Galois extension of F containing K) now with Galois group G.
  - By the Galois correspondence, the intermediate field K of $\hat{K}/F$ corresponds to a subgroup H of G (namely, the subgroup of G that fixes K). Letting S be a set of coset representatives for H in G, for an element $\alpha \in K$, we define the trace of α to be $\mathrm{tr}_{K/F}(\alpha) = \sum_{g\in S} g(\alpha)$ and the norm to be $N_{K/F}(\alpha) = \prod_{g\in S} g(\alpha)$.
  - The trace and norm are well defined because the value $g(\alpha)$ is independent of which coset representative is used: if g_1 and g_2 represent the same coset, then $g_1^{-1}g_2 \in H$ hence $g_1^{-1}g_2$ fixes all elements of K; then $g_1^{-1}g_2(\alpha) = \alpha$ so $g_1(\alpha) = g_2(\alpha)$.
  - Exercise: For a separable extension K/F, show that the trace and norm as defined above are still Galois-invariant, that the trace is additive and F-linear, and that the norm is multiplicative.
  - Example: Consider $K = \mathbb{Q}(\sqrt[3]{2})$ and $L = \mathbb{Q}$, whose Galois closure is $\hat{K} = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ with Galois group isomorphic to S_3 with generators σ, τ with $\sigma(\sqrt[3]{2}, \zeta_3) = (\zeta_3\sqrt[3]{2}, \zeta_3)$ and $\tau(\sqrt[3]{2}, \zeta_3) = (\sqrt[3]{2}, \zeta_3^2)$. Then K is the fixed field of the subgroup $H = \langle\tau\rangle$ so we can take coset representatives $\{1, \sigma, \sigma^2\}$ for H in K. Then for any $\alpha \in K$ we have $\mathrm{tr}(\alpha) = \alpha + \sigma(\alpha) + \sigma^2(\alpha)$ and $N(\alpha) = \alpha \cdot \sigma(\alpha) \cdot \sigma^2(\alpha)$. Explicitly, for $\alpha = a + b\sqrt[3]{2} + c\sqrt[3]{4}$ we see $\sigma(\alpha) = a + b\zeta_3\sqrt[3]{2} + c\zeta_3^2\sqrt[3]{4}$ and $\sigma^2(\alpha) = a + b\zeta_3^2\sqrt[3]{2} + c\zeta_3\sqrt[3]{4}$, so $\mathrm{tr}(\alpha) = 3a$ and $N(\alpha) = a^3 + 2b^3 + 4c^3 - 6abc$ after some simplification.
  - In the example above, notice that the three Galois conjugates α, $\sigma(\alpha)$, $\sigma^2(\alpha)$ correspond to the three different complex embeddings of α (this is more obvious with the specific choice $\alpha = \sqrt[3]{2}$, where $\sigma(\alpha) = \zeta_3\sqrt[3]{2}$ and $\sigma^2(\alpha) = \zeta_3^2\sqrt[3]{2}$ are the other two complex cube roots of 2).

0.3 (Sep 9) Complex Embeddings, Trace and Norm 2

- We will now give another approach to the trace and norm that is more amenable to explicit calculations, in terms of the complex embeddings of the number field K.
  - Let us review some of the basic properties of complex embeddings, which are the nonzero ring homomorphisms from a field to $\mathbb{C}$.
  - The connection to our previous discussion is that the various complex embeddings of K are simply the images of K under the Galois group of the Galois closure of K.

- Proposition (Complex Embeddings): Suppose K/F is an extension of number fields of degree n, with K and F explicitly considered as subfields of $\mathbb{C}$.

  1. For a fixed embedding $\sigma : F \to \mathbb{C}$, there exist exactly n embeddings $\tau : K \to \mathbb{C}$ extending σ (i.e., with $\tau|_K = \sigma$).
     - Proof: For $n = 1$ the result is trivial so now assume $n > 1$.

- For an embedding $\tau : K \to \mathbb{C}$, since we know the value of τ on F and since $K = F(\alpha)$, the choice of $\tau(\alpha)$ determines τ uniquely, so we just have to determine the possible values of $\tau(\alpha)$.
- Let $K = F(\alpha)$, let $m(x)$ be the minimal polynomial of α over F (which necessarily has degree n), and let $\tilde{m}(x)$ be the polynomial obtained by applying σ to all the coefficients of $m(x)$. Then $\tilde{m}(x) \in \sigma K[x]$ is the minimal polynomial of $\sigma(\alpha)$, as it is clearly irreducible and has $\sigma(\alpha)$ as a root.
- Any embedding $\tau : K \to \mathbb{C}$ restricting to σ on F must map $m(x)$ to $\tilde{m}(x)$, and so τ must map the root α of $m(x)$ to some root β of $\tilde{m}(x)$.
- On the other hand, for any root β of $\tilde{m}(x)$, there is a unique isomorphism from $F(\alpha)$ to $\sigma F(\beta)$ that restricts to σ on F and that sends α to β; such a map must take $c_0\alpha + \cdots + c_{n-1}\alpha^{n-1}$ to $\sigma(c_0)\beta + \cdots + \sigma(c_{n-1})\beta^{n-1})$, but this determines it uniquely, and we can see it is well defined by noting that it is obtained as the composition of the isomorphisms $F(\alpha) \overset{\alpha \mapsto x}{\to} F[x]/(m(x)) \overset{\sigma}{\to} \sigma F[x]/(\tilde{m}(x)) \overset{x \mapsto \beta}{\to} \sigma F(\beta)$.
- Since the degree of $\tilde{m}(x)$ is the same as the degree of $m(x)$, namely n, the degree of the extension L/K, we conclude that there are exactly n embeddings $\tau : K \to \mathbb{C}$ extending σ.

2. For any number field $K/\mathbb{Q}$ of degree n, there are exactly n complex embeddings $\tau : K \to \mathbb{C}$.
   - Proof: Apply (1) with $F = \mathbb{Q}$, noting that there is only one embedding of $\mathbb{Q}$ into $\mathbb{C}$ (as 0 must map to 0 and 1 must map to 1).
3. If $\sigma_1, \ldots \sigma_n$ denote the n complex embeddings of K fixing F, then for $\alpha \in K$ we have $\mathrm{tr}_{K/F}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha)$ and $N_{K/F}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha)$.
   - Proof: Consider the Galois closure $\hat{K}/F$ as a subfield of $\mathbb{C}$, and consider the action of the Galois group $G = \mathrm{Gal}(\hat{K}/F)$ on K.
   - For any $\sigma \in G$ we see that $\sigma(K)$ is a subfield of $\mathbb{C}$ isomorphic to K (as the inverse isomorphism is simply σ^{-1}), and so $\sigma : K \to \mathbb{C}$ yields a complex embedding of K.
   - Conversely, by (1), any complex embedding of K extends to one of $\hat{K}$ but since $\hat{K}$ is Galois, any complex embedding is an automorphism of $\hat{K}$: thus, all of the complex embeddings of K are obtained as $\sigma(K)$ for some $\sigma \in G$.
   - Two complex embeddings σ_1 and σ_2 of K are equal when $\sigma_1(\alpha) = \sigma_2(\alpha)$ for $\alpha \in K \iff \sigma_1^{-1}\sigma_2(\alpha) = \alpha$ for all $\alpha \in K \iff \sigma_1^{-1}\sigma_2$ fixes $K \iff \sigma_1^{-1}\sigma_2$ lies in the subgroup H of G fixing $K \iff \sigma_1$ and σ_2 represent the same coset of H in G.
   - Thus, the n possible complex embeddings σ_i of K are given precisely by a set of a coset representatives for H in G. The claimed formulas for the trace and norm then reduce immediately to our earlier definition.

- Example: The quadratic field $K = \mathbb{Q}(\sqrt{D})$ has two complex embeddings: the identity embedding $\sigma_1(a + b\sqrt{D}) = a + b\sqrt{D}$, and the conjugate embedding with $\sigma_2(a + b\sqrt{D}) = a - b\sqrt{D}$.
  - Here, we can see that both embeddings represent field automorphisms of $\mathbb{Q}(\sqrt{D})$; that is because $\mathbb{Q}(\sqrt{D})$ is Galois over $\mathbb{Q}$.
  - We then have $\mathrm{tr}_{K/\mathbb{Q}}(a+b\sqrt{D}) = 2a$ and $N_{K/\mathbb{Q}}(a+b\sqrt{D}) = a^2 - Db^2$, just as we computed in our example earlier.

- Example: The cubic field $K = \mathbb{Q}(\sqrt[3]{2})$ has three complex embeddings: the identity embedding and the two embeddings obtained by mapping $\sqrt[3]{2}$ to the other roots of its minimal polynomial $p(x) = x^3 - 2$: namely, $\zeta_3\sqrt[3]{2}$ and $\zeta_3^2\sqrt[3]{2}$, the other two complex cube roots of 2.
  - Explicitly, these maps σ_1, σ_2, σ_3 send $a+b\sqrt[3]{2}+c\sqrt[3]{4}$ respectively to $a+b\sqrt[3]{2}+c\sqrt[3]{4}$, to $a+b\zeta_3\sqrt[3]{2}+c\zeta_3^2\sqrt[3]{4}$, and to $a + b\zeta_3^2\sqrt[3]{2} + c\zeta_3\sqrt[3]{4}$.
  - Here, we can see that only the identity embedding maps K back to itself, illustrating that K is not Galois over $\mathbb{Q}$. The other two embeddings map K to its Galois conjugates $\sigma_2(K) = \mathbb{Q}(\zeta_3\sqrt[3]{2})$ and $\sigma_3(K) = \mathbb{Q}(\zeta_3^2\sqrt[3]{2})$, the fields generated by the other two roots of the minimal polynomial.
  - We can as before compute the trace and norm $\mathrm{tr}_{K/\mathbb{Q}}(a+b\sqrt[3]{2}+c\sqrt[3]{4}) = 3a$ and $N_{K/\mathbb{Q}}(a+b\sqrt[3]{2}+c\sqrt[3]{4}) = (a + b\sqrt[3]{2} + c\sqrt[3]{4})(a + b\zeta_3\sqrt[3]{2} + c\zeta_3^2\sqrt[3]{4})(a + b\zeta_3^2\sqrt[3]{2} + c\zeta_3\sqrt[3]{4}) = a^3 + 2b^3 + 4c^3 - 6abc$.

- Example: The cyclotomic field $\mathbb{Q}(\zeta_n)$ has $\varphi(n)$ complex embeddings, obtained by mapping ζ_n to the $\varphi(n)$ roots of its minimal polynomial[2], which are ζ_n^a for $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ (i.e., relatively prime to n).
  - Writing these maps in general is rather cumbersome, so we will just give a few examples for specific n.
  - For $n = 8$, we see that $\mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2})$ has $\varphi(8) = 4$ complex embeddings obtained by mapping $\zeta_8 = (\sqrt{2}+i\sqrt{2})/2$ to the roots $\zeta_8, \zeta_8^3, \zeta_8^5, \zeta_8^7 = (\pm\sqrt{2}\pm i\sqrt{2})/2$ of the cyclotomic polynomial $\Phi_8(x) = x^4+1$ over $\mathbb{Q}$.
  - Noting that $\mathbb{Q}(\zeta_8)$ has a basis $\{1, \zeta_8, \zeta_8^2, \zeta_8^3\}$ over $\mathbb{Q}$, we may compute the embeddings $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ explicitly as the maps sending $a+b\zeta_8+c\zeta_8^2+d\zeta_8^3$ respectively to $a+b\zeta_8+c\zeta_8^2+d\zeta_8^3$, to $a+b\zeta_8^3+c\zeta_8^6+d\zeta_8$, to $a+b\zeta_8^5+c\zeta_8^2+d\zeta_8^7$, and to $a+b\zeta_8^7+c\zeta_8^6+d\zeta_8^5$.
  - Then we have $\mathrm{tr}_{K/\mathbb{Q}}(a+b\zeta_8+c\zeta_8^2+d\zeta_8^3) = 4a$ and $N_{K/\mathbb{Q}}(a+b\zeta_8+c\zeta_8^2+d\zeta_8^3) = (a^2+c^2)^2+(b^2+d^2)^2-4(ab+cd)(ad-bc)$ after some simplification.
  - Exercise: Compute the four complex embeddings of $\mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2})$ instead using the $\mathbb{Q}$-basis $\{1, \sqrt{2}, i, i\sqrt{2}\}$, and find the trace and norm of $p+q\sqrt{2}+ri+si\sqrt{2}$.
- These definitions of trace and norm also have a convenient, and in some sense even more natural, interpretation in terms of the linear transformation given by multiplication by α, which also explains the linearity of the trace (and its name) and the multiplicativity of the norm:
- Exercise: Let K/F be an extension of number fields with $\alpha \in K$ and define $T_\alpha : K \to K$ to be the F-linear transformation of multiplication by α, namely with $T_\alpha(x) = \alpha x$ for all $x \in K$.
  1. Show that the minimal polynomial of the linear transformation T_α is the minimal polynomial of the algebraic number α. [Hint: Show that $F[T_\alpha]$ is ring-isomorphic to $F[\alpha]$.]
  2. Show that the eigenvalues of T_α in $\mathbb{C}$ are the elements $\sigma_i(\alpha)$, where $\sigma_1, \ldots, \sigma_n$ are the complex embeddings of K fixing F.
  3. Show that the characteristic polynomial $p(x) = \det(xI - T_\alpha)$ of T_α is $m(x)^{[K:F(\alpha)]}$ where $m(x)$ is the minimal polynomial of α over F.
  4. Show that $\mathrm{tr}(T_\alpha) = \mathrm{tr}_{K/F}(\alpha)$ and that $\det(T_\alpha) = N_{K/F}(\alpha)$.
  5. Use (a) and (d) to compute the trace, norm, and minimal polynomial of $\alpha = \sqrt[3]{2} + \sqrt{7}$ from $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt{7})$ to $\mathbb{Q}$. [Suggestion: Compute the matrix T_α with respect to the basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}, \sqrt{7}, \sqrt[3]{2}\sqrt{7}, \sqrt[3]{4}\sqrt{7}\}$.]
- Let us now prove a few other basic properties of the trace and norm:
- Proposition (Trace and Norm): Let K/F be an extension of number fields of degree n. Then the following hold:
  1. For any $r \in \mathbb{Q}$ and $\alpha \in K$ we have $\mathrm{tr}_{K/F}(r) = nr$, $\mathrm{tr}_{K/F}(r\alpha) = r\mathrm{tr}_{K/F}(\alpha)$, $N_{K/F}(r) = r^n$, and $N_{K/F}(r\alpha) = r^n N_{K/F}(\alpha)$.
     - Proof: The complex embeddings of K all fix $\mathbb{Q}$, so $\sigma_i(r) = r$ for each $1 \le i \le n$. The claimed formulas then follow immediately from the linearity of the trace and multiplicativity of the norm.
  2. (Transitivity) If L/K is another extension of number fields and $\alpha \in L$, we have $\mathrm{tr}_{L/F}(\alpha) = \mathrm{tr}_{K/F}(\mathrm{tr}_{L/K}(\alpha))$ and $N_{L/F}(\alpha) = N_{K/F}(N_{L/K}(\alpha))$.
     - Proof: Consider the Galois closure $\hat{L}$ of L/F with Galois group G. Let H_K be the subgroup of G fixing K and H_L be the subgroup of G fixing L.
     - Let $\sigma_1, \ldots, \sigma_n$ be a set of coset representatives for H_K in G (these represent the complex embeddings of K fixing F) and $\tau_1, \ldots \tau_m$ be a set of coset representatives for H_L in H_K (these represent the complex embeddings of L fixing K). Then the set of pairwise products $\{\sigma_i\tau_j\}_{1\le i\le n, 1\le j\le m}$ is a set of coset representatives for H_L in G.
     - Thus $\mathrm{tr}_{L/F}(\alpha) = \sum_{i,j}\sigma_i\tau_j(\alpha) = \sum_{i=1}^n\sum_{j=1}^m \sigma_i(\tau_j(\alpha)) = \sum_{i=1}^n \sigma_i[\sum_{j=1}^m \tau_j(\alpha)] = \sum_{i=1}^n \sigma_i(\mathrm{tr}_{L/K}(\alpha)) = \mathrm{tr}_{K/F}(\mathrm{tr}_{L/K}(\alpha))$, and finally the norm formula is the same with sums replaced by products.

[2] As we will prove along the way later, the nth cyclotomic polynomial $\Phi_n(x)$, which is the minimal polynomial of ζ_n, factors in $\mathbb{C}$ as $\Phi_n(x) = \prod_{z\in(\mathbb{Z}/n\mathbb{Z})^\times}(x - \zeta_n^a)$. In particular, its degree is $\varphi(n)$.

3. If α has minimal polynomial $m(x) = x^d + c_{n-1}x^{n-1} + \cdots + c_0$ over F, then $\mathrm{tr}_{K/F}(\alpha) = -\frac{n}{d}c_{n-1}$ and $N_{K/F}(\alpha) = (-1)^n c_0^{n/d}$.
   - Proof: The possible Galois conjugates of α are the d different roots of its minimal polynomial over F.
   - By our earlier result on extensions of embeddings, for any other root β of $m(x)$, there is a unique embedding of $F(\alpha)$ fixing F that maps α to β. Then applying the result again, there are exactly $[K : F(\alpha)] = n/d$ embeddings of K fixing F that map α to β.
   - We conclude that in the list of values $\sigma_i(\alpha)$ for $1 \le i \le n$, the value β occurs exactly n/d times, and this holds for all d possible roots β.
   - Then $\mathrm{tr}_{K/F}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha)$ is n/d times the sum of the roots of $m(x)$ while $N_{K/F}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha)$ is the product of the roots of $m(x)$ to the n/dth power. The formulas follow immediately.
4. If α is an algebraic integer, then $\mathrm{tr}_{K/F}(\alpha)$ and $N_{K/F}(\alpha)$ are both algebraic integers in F. In particular, $\mathrm{tr}_{K/\mathbb{Q}}(\alpha)$ and $N_{K/\mathbb{Q}}(\alpha)$ are both integers.
   - Proof: If α is an algebraic integer, its Galois conjugates are also algebraic integers, hence so too are the sum and product of all these conjugates.
   - By the argument in (3) above, $\mathrm{tr}_{K/F}(\alpha)$ is an integer times the sum of the Galois conjugates of α while $N_{K/F}(\alpha)$ is an integer power of the product of the Galois conjugates of α. The result follows immediately.
5. The units in the ring of integers $\mathcal{O}_K$ are precisely the elements of norm ± 1 (i.e., the $\alpha \in \mathcal{O}_K$ with $N_{K/\mathbb{Q}}(\alpha) = \pm 1$).
   - Proof: If $\alpha \in \mathcal{O}_K$ is a unit with multiplicative inverse $\beta \in \mathcal{O}_K$, then $\alpha\beta = 1$ so taking norms yields $N_{K/\mathbb{Q}}(\alpha)N_{K/\mathbb{Q}}(\beta) = N_{K/\mathbb{Q}}(\alpha\beta) = N_{K/\mathbb{Q}}(1) = 1$ by multiplicativity and (1).
   - But now by (4), both $N_{K/\mathbb{Q}}(\alpha)$ and $N_{K/\mathbb{Q}}(\beta)$ are integers, so we must have $N_{K/\mathbb{Q}}(\alpha) = \pm 1$.
   - Conversely, if $N_{K/\mathbb{Q}}(\alpha) = \pm 1$, then this says α times a product of its Galois conjugates $\beta_1 \cdots \beta_n$ equals ± 1. But then $\pm\beta_1 \cdots \beta_n$ is an algebraic integer that is a multiplicative inverse of α, so it lies in $\mathcal{O}_K$ and thus α is a unit in $\mathcal{O}_K$.

0.4 (Sep 11) The Group Structure of $\mathcal{O}_K$, Discriminants 1

- Using this convenient characterization of units in $\mathcal{O}_K$ we can easily test whether specific elements of $\mathcal{O}_K$ are in fact units, and in some simple cases we can characterize all of the units.
   - Example: In the quadratic field $K = \mathbb{Q}(\sqrt{D})$ with $D \equiv 2, 3 \pmod 4$ so that $\mathcal{O}_K = \mathbb{Z}[\sqrt{D}]$, we see that $N(a + b\sqrt{D}) = a^2 - Db^2$, so the element $a + b\sqrt{D}$ is a unit if and only if $a^2 - Db^2 = \pm 1$. When $D \equiv 1 \pmod 4$ so that $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$, we see that $N(a + b\frac{1+\sqrt{D}}{2}) = a^2 + ab + \frac{1-D}{4}b^2$, so the element $a + b\sqrt{D}$ is a unit if and only if $a^2 + ab + \frac{1-D}{4}b^2 = \pm 1$.
   - The unit behavior actually is quite different for real and imaginary quadratic fields. Imaginary quadratic fields have only finitely many units:
   - Exercise: Show that when $D < 0$, the only units of $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ are ± 1, except in the case $D = -1$ with units $\pm 1, \pm i$ and in the case $D = -3$ with units $\pm 1, \pm\zeta_3, \pm\zeta_3^2$.
   - However, real quadratic fields always have infinitely many units: we will show more general results later, but this claim follows from the fact that Pell's equation[3] $a^2 - Db^2 = 1$ always has a nontrivial solution (i.e., one with $b > 0$) for any squarefree positive integer D. If $u = a + b\sqrt{D}$ represents such a solution, then since $u > 1$ we see easily that the powers u^n yield infinitely many distinct units in $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$.
- We now exploit the trace and norm maps to establish some other basic information about the structure of $\mathcal{O}_K$ as an additive abeliam group and as a module.

[3] To summarize this argument: first one shows (via the pigeonhole principle or via continued fractions) that for any real number x there are infinitely many $p/q \in \mathbb{Q}$ with $|x - p/q| < 1/q^2$. Taking $x = \sqrt{D}$ yields infinitely many positive (p, q) with $\left|\sqrt{D} - p/q\right| < 1/q^2$ whence $|p^2 - Dq^2| < 2\sqrt{D} + 1$. Picking some r for which $p^2 - Dq^2 = r$ has infinitely many solutions, if (p, q) and (p', q') are solutions congruent mod r then $(a, b) = (pp' - Dqq', |pq' - p'q|)/r$ has $a^2 - Db^2 = 1$ and $b > 0$.

- Recall in particular that we showed earlier that for every element $\alpha \in K$ there is some nonzero $d \in \mathbb{Z}$ such that $d\alpha$ is an algebraic integer.

- Proposition (Additive Structure of $\mathcal{O}_K$): Suppose K is a number field.

1. The ring of integers $\mathcal{O}_K$ is a torsion-free, finitely generated abelian group.
   - Proof: Clearly $\mathcal{O}_K$ is torsion-free since it is a subset of $\mathbb{C}$; it remains to show finite generation.
   - Suppose $K/\mathbb{Q}$ has degree n and let $\alpha_1, \dots, \alpha_n$ be a $\mathbb{Q}$-basis for K; by scaling these basis elements by integers as needed, we may assume the α_i are elements of $\mathcal{O}_K$.
   - For each nonzero $\beta \in K$, consider the map $\varphi_\beta : K \to \mathbb{Q}$ given by $\varphi_\beta(\alpha) = \mathrm{Tr}_{K/\mathbb{Q}}(\beta\alpha)$. This map is $\mathbb{Q}$-linear and nonzero since $\varphi_\beta(\beta^{-1}) = \mathrm{Tr}_{K/\mathbb{Q}}(1) = n$, and so the map from the vector space K to its dual space $\hat{K} = \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{Q})$ sending β to φ_β is injective. However, because both vector spaces are n-dimensional, it is in fact an isomorphism.
   - Therefore, we see that every linear functional on K is of the form φ_β for some $\beta \in K$.
   - Consider the elements $\alpha_1', \dots, \alpha_n' \in K$ giving the dual basis to $\alpha_1, \dots, \alpha_n$: in other words, with $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i'\alpha_j) = 1$ for $i = j$ and 0 otherwise. (Such elements exist because any linear functional, such as the one mapping all of the basis elements $\alpha_1, \dots, \alpha_n$ to zero except for α_i which is mapped to 1, is of the form $\varphi_{\alpha_i'}$ for some α_i'.)
   - Since $\alpha_1', \dots \alpha_n'$ are then clearly linearly independent, they are a $\mathbb{Q}$-basis for K.
   - Now suppose β is some element of $\mathcal{O}_K$: since $\{\alpha_1', \dots \alpha_n'\}$ is a basis for K, there exist some $c_i \in \mathbb{Q}$ with $\beta = c_1\alpha_1' + \cdots + c_n\alpha_n'$.
   - Multiplying by α_i and taking the trace then yields $\mathrm{Tr}_{K/\mathbb{Q}}(\beta\alpha_i) = c_1\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_1') + \cdots + c_n\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_n')$. But all of the traces are 0 except for the trace of $\alpha_i\alpha_i'$ which equals 1, so the trace is simply c_i. But because $\beta\alpha_i$ is an algebraic integer, its trace is an integer, so we see each $c_i \in \mathbb{Z}$.
   - We conclude that $\beta \in \mathbb{Z}\alpha_1' + \mathbb{Z}\alpha_2' + \cdots + \mathbb{Z}\alpha_n'$, so $\mathcal{O}_K \subseteq \mathbb{Z}\alpha_1' + \mathbb{Z}\alpha_2' + \cdots + \mathbb{Z}\alpha_n'$. Thus $\mathcal{O}_K$ is contained in a finitely generated abelian group, hence is itself a finitely generated abelian group.
2. If K/F is an extension of number fields of degree n, then $\mathcal{O}_K$ is a torsion-free $\mathcal{O}_F$-module of rank n.
   - Note here that the $\mathcal{O}_F$-module structure of $\mathcal{O}_K$ is inherited from the ring structure of $\mathcal{O}_K$.
   - Proof: To show that it has rank n, suppose that $K = F(\alpha)$, where (by rescaling) we may assume α is an algebraic integer.
   - Then the set $\{1, \alpha, \dots, \alpha^{n-1}\}$ is F-linearly independent and consists of elements of $\mathcal{O}_K$, so it yields an $\mathcal{O}_F$-linearly independent set in $\mathcal{O}_K$. Thus $\mathcal{O}_K$ has rank at least n.
   - On the other hand, if $\beta_1, \dots, \beta_{n+1}$ are any elements of $\mathcal{O}_K$, then there exists some F-linear dependence $c_1\beta_1 + \cdots + c_{n+1}\beta_{n+1} = 0$ for $c_i \in F$.
   - Scaling by an appropriate integer d such that $dc_i \in \mathcal{O}_F$ for all i yields an $\mathcal{O}_F$-linear dependence of these β_i. Thus the maximal size of an $\mathcal{O}_F$-linearly independent set in $\mathcal{O}_K$ is n, so since by (1) $\mathcal{O}_K$ is finitely generated, we see that $\mathcal{O}_K$ has rank n.
3. If K is a number field of degree n over $\mathbb{Q}$, then $\mathcal{O}_K$ is a free abelian group of rank n: in other words, there exist $\beta_1, \beta_2, \dots, \beta_n \in \mathcal{O}_K$ such that $\mathcal{O}_K = \mathbb{Z}\beta_1 \oplus \mathbb{Z}\beta_2 \oplus \cdots \oplus \mathbb{Z}\beta_n$.
   - Proof: By (1) we know that $\mathcal{O}_K$ is a torsion-free finitely generated abelian group, and by (2) we know it has rank n. by the structure theorem for finitely generated abelian groups, such an abelian group is free of rank n.
   - The second statement is then simply the definition of a free rank-n abelian group.
   - Exercise: Show more generally that if $\mathcal{O}_F$ is a PID, and K/F has degree n, then $\mathcal{O}_K$ is a free $\mathcal{O}_F$-module of rank n.
   - Remark: In general, $\mathcal{O}_K$ need not be a free $\mathcal{O}_F$-module. (In other words, although there exist $\mathcal{O}_F$-linearly independent sets of size n, none of them span $\mathcal{O}_K$, but rather, will give some proper submodule.) Later, once we study the multiplicative structure of rings of integers further, we will be able to give explicit examples, which (per the exercise above) can only happen when $\mathcal{O}_F$ is not a PID.
4. The ring $\mathcal{O}_K$ is Noetherian (i.e., every ideal is finitely generated).

- ◦ Proof: Any ideal I of $\mathcal{O}_K$ is (a fortiori) an additive subgroup of $\mathcal{O}_K$, which per (3) is a free abelian group of rank n. Then I is also a free abelian group of rank at most n, and a set of additive-group generators for I certainly also generates I as an ideal.
- ◦ Hence every ideal I is generated by at most n elements, so $\mathcal{O}_K$ is Noetherian.
- ◦ Remark: This bound of n generators is not sharp: in fact, as we will show later, every ideal of $\mathcal{O}_K$ is generated by at most *two* elements. (And of course, saying that $\mathcal{O}_K$ is a PID is the same as saying every ideal is generated by just one element.)

- While the general results we have just shown are useful in understanding the abstract structure of $\mathcal{O}_K$ as an abelian group (and to some extent as a ring), they are not sufficiently explicit to allow us to compute an actual integral basis for $\mathcal{O}_K$. In order to make calculations, we require one more tool: the discriminant.

- Definition: Let K/F be an extension of number fields of degree n, and let $\sigma_1, \dots, \sigma_n : K \to \mathbb{C}$ be the complex embeddings of K fixing F. For an ordered n-tuple $(\alpha_1, \dots, \alpha_n) \in K$, we define the discriminant $\mathrm{disc}_{K/F}(\alpha_1, \dots, \alpha_n)$ of the tuple $(\alpha_1, \dots, \alpha_n)$ to be $\mathrm{disc}_{K/F}(\alpha_1, \dots, \alpha_n) = \begin{vmatrix} \sigma_1(\alpha_i) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{vmatrix}^2$, the square of the determinant of the $n \times n$ matrix whose (i,j)-entry is $\sigma_i(\alpha_j)$.
  - ◦ We note immediately that taking the square of the determinant means that the ordering of the embeddings σ_i and of the elements α_j is irrelevant, since swapping rows or columns will not affect the value.
  - ◦ Example: For $K = \mathbb{Q}(\sqrt{2})$ we have $\mathrm{disc}_{K/\mathbb{Q}}(1, \sqrt{2}) = \begin{vmatrix} 1 & \sqrt{2} \\ 1 & -\sqrt{2} \end{vmatrix}^2 = 8$ and $\mathrm{disc}_{K/\mathbb{Q}}(1 + 2\sqrt{2}, 3) = \begin{vmatrix} 1+2\sqrt{2} & 3 \\ 1-2\sqrt{2} & 3 \end{vmatrix}^2 = 288$.
  - ◦ Example: For $K = \mathbb{Q}(\sqrt[3]{2})$ we have $\mathrm{disc}_{K/\mathbb{Q}}(1, \sqrt[3]{2}, \sqrt[3]{4}) = \begin{vmatrix} 1 & \sqrt[3]{2} & \sqrt[3]{4} \\ 1 & \zeta_3\sqrt[3]{2} & \zeta_3^2\sqrt[3]{4} \\ 1 & \zeta_3^2\sqrt[3]{2} & \zeta_3\sqrt[3]{4} \end{vmatrix}^2 = -108$.

- Here are some basic properties of the discriminant:

- Proposition (Properties of Discriminants): Let K/F be a degree-n extension of number fields.

1. $\mathrm{disc}_{K/F}(\alpha_1, \dots, \alpha_n)$ is equal to the determinant of the $n \times n$ matrix whose (i,j)-entry is $\mathrm{tr}_{K/F}(\alpha_i\alpha_j)$. In particular, $\mathrm{disc}_{K/F}(\alpha_1, \dots, \alpha_n) \in F$.
   - ◦ Proof: Let M be the matrix whose (i,j)-entry is $\sigma_i(\alpha_j)$, so that $\mathrm{disc}_{K/F}(\alpha_1, \dots, \alpha_n) = \det(M)^2$.
   - ◦ Then the (i,j)-entry of the product $M^T M$ is $\sum_{k=1}^n \sigma_k(\alpha_i)\sigma_k(\alpha_j) = \sum_{k=1}^n \sigma_k(\alpha_i\alpha_j) = \mathrm{tr}_{K/F}(\alpha_i\alpha_j)$. The result follows immediately by taking determinants.
   - ◦ The second statement follows immediately from the fact that the discriminant is the determinant of a matrix with entries in F (since the traces are all in F).
2. If $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$, then $\mathrm{disc}_{K/F}(\alpha_1, \dots, \alpha_n) \in \mathcal{O}_F$. In particular, $\mathrm{disc}_{K/\mathbb{Q}}(\alpha_1, \dots, \alpha_n)$ is always an integer.
   - ◦ Proof: From (1) we see that $\mathrm{disc}_{K/F}(\alpha_1, \dots, \alpha_n) \in F$. Furthermore, if all of the α_i are algebraic integers, then so are all of the entries in the determinant expression (either the one from the definition or the one in (1)), so the discriminant is also an algebraic integer.
3. The discriminant $\mathrm{disc}_{K/F}(\alpha_1, \dots, \alpha_n) = 0$ if and only if the α_i are F-linearly dependent.
   - ◦ Proof: Clearly if the α_j are F-linearly dependent, then so are the columns of the matrix with entries $\sigma_i(\alpha_j)$, since the embeddings σ_i preserve F-linear dependence, and so the determinant (hence discriminant) will be zero.
   - ◦ Conversely, suppose $\mathrm{disc}_{K/F}(\alpha_1, \dots, \alpha_n) = 0$: then the rows of the matrix $\{\mathrm{tr}_{K/F}(\alpha_i\alpha_j)\}_{1 \le i,j \le n}$ are F-linearly dependent, so there exist some $c_i \in F$, not all zero, with $c_1\mathrm{tr}_{K/F}(\alpha_1\alpha_j) + \cdots + c_n\mathrm{tr}_{K/F}(\alpha_n\alpha_j) = 0$ for each $1 \le j \le n$.

- But by linearity of the trace, for $\beta = c_1\alpha_1 + \cdots + c_n\alpha_n$ this means $\mathrm{tr}_{K/F}(\beta\alpha_j) = 0$ for each $1 \leq j \leq n$. However, this implies $\beta = 0$, since as we noted earlier, the linear map $\varphi_\beta : K \to F$ given by $\varphi_\beta(\alpha) = \mathrm{Tr}_{K/F}(\beta\alpha)$ is nonzero for $\beta \neq 0$.
- This means there exists some $c_i \in F$, not all zero, with $c_1\alpha_1 + \cdots + c_n\alpha_n = 0$, so the α_i are F-linearly dependent.

4. If $\underline{\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K}$ and $\mathrm{disc}_{K/F}(\alpha_1, \ldots, \alpha_n) \neq 0$, then $\mathcal{O}_F\alpha_1 \oplus \mathcal{O}_F\alpha_2 \oplus \cdots \oplus \mathcal{O}_F\alpha_n$ is an $\mathcal{O}_F$-submodule of $\mathcal{O}_K$ of finite index (as an additive group).
   - Proof: By (3), if $\mathrm{disc}_{K/F}(\alpha_1, \ldots, \alpha_n) \neq 0$ then $\alpha_1, \ldots, \alpha_n$ are F-linearly independent (hence $\mathcal{O}_F$-linearly independent, so they generate a free submodule $M = \mathcal{O}_F\alpha_1 \oplus \mathcal{O}_F\alpha_2 \oplus \cdots \oplus \mathcal{O}_F\alpha_n$ of $\mathcal{O}_K$ of rank n.
   - But as we proved earlier $\mathcal{O}_K$ is finitely generated and has rank n, so the quotient $\mathcal{O}_K/M$ is finitely generated and has rank 0: in other words, it is finite.
5. Suppose that $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ and $\beta_1, \ldots, \beta_n \in \mathcal{O}_K$ span the same additive subgroup of $\mathcal{O}_K$: $\mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n = \mathbb{Z}\beta_1 \oplus \cdots \oplus \mathbb{Z}\beta_n$. Then $\mathrm{disc}_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) = \mathrm{disc}_{K/\mathbb{Q}}(\beta_1, \ldots, \beta_n)$.
   - Proof: If the subgroup has rank less than n, both discriminants are zero by (3). So now assume both subgroups have rank n. By hypothesis, there exist $n \times n$ integer matrices A and B with $\begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix} = A \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}, \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = B \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix}$.
   - Then since each set is an F-basis of K (since the rank is n) we see $AB = I_n$ and so $\det(A) = \det(B) = \pm 1$ since both matrices have integer determinant.
   - Applying σ_i to each side of the first matrix equation yields $\begin{bmatrix} \sigma_i(\beta_1) \\ \vdots \\ \sigma_i(\beta_n) \end{bmatrix} = A \begin{bmatrix} \sigma_i(\alpha_1) \\ \vdots \\ \sigma_i(\alpha_n) \end{bmatrix}$.
   - Thus, $\mathrm{disc}_{K/\mathbb{Q}}(\beta_1, \ldots, \beta_n) = \det[\{\sigma_i(\beta_j)\}_{1 \leq i,j \leq n}]^2 = \det[A\{\sigma_i(\alpha_j)\}_{1 \leq i,j \leq n}]^2 = \det(A)^2 \mathrm{disc}_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)$, and since $\det(A) = \pm 1$ the result follows.
6. Suppose $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ are two integral bases for $\mathcal{O}_K$. Then $\mathrm{disc}_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) = \mathrm{disc}_{K/\mathbb{Q}}(\beta_1, \ldots, \beta_n)$.
   - Proof: Immediate from (5).

0.5 (Sep 12) Discriminants 2

- From (6) above we see that the discriminants for any two integral bases of the ring of integers $\mathcal{O}_K$ are the same, and more generally (5) says that the same is true for any rank-n subgroup of $\mathcal{O}_K$. We may therefore view the discriminant as an invariant of the ring of integers (or, as is exceedingly common) the number field K itself:
- Definition: For a number field K, the discriminant of K (or of its ring of integers $\mathcal{O}_K$) is defined to be the discriminant of any integral basis of $\mathcal{O}_K$. The discriminant is variously denoted $\mathrm{disc}(K)$, $\mathrm{disc}(\mathcal{O}_K)$, or D_K, or Δ_K. When S is a subgroup of finite index in $\mathcal{O}_K$, we likewise define $\mathrm{disc}(S)$ to be the discriminant of any integral basis of S.
  - We will mention here that we can also define the discriminant for a relative extension K/F, but it is more complicated because $\mathcal{O}_K$ need not possess an $\mathcal{O}_F$-basis. Instead, the approach is to consider the discriminant ideal $D_{K/F}$, an ideal of $\mathcal{O}_F$, generated by the discriminants of all n-tuples of elements of $\mathcal{O}_K$.
- Example: For $K = \mathbb{Q}(\sqrt{D})$, we have an integral basis for $\mathcal{O}_K$ given by $\{1, \sqrt{D}\}$ when $D \equiv 2, 3 \pmod 4$ and by $\{1, \frac{1+\sqrt{D}}{2}\}$ when $D \equiv 1 \pmod 4$.
  - For $D \equiv 2, 3 \pmod 4$ we have $\mathrm{disc}(K) = \mathrm{disc}(1, \sqrt{D}) = \begin{vmatrix} 1 & \sqrt{D} \\ 1 & -\sqrt{D} \end{vmatrix}^2 = 4D$.

- For $D \equiv 1 \pmod 4$ we have $\text{disc}(K) = \text{disc}(1, \frac{1+\sqrt{D}}{2}) = \begin{vmatrix} 1 & (1+\sqrt{D})/2 \\ 1 & (1-\sqrt{D})/2 \end{vmatrix}^2 = D$.

- We would now like to use discriminants to construct integral bases for additional rings of integers $\mathcal{O}_K$. To do this, it is useful to broaden our focus to the wider array of rank-n subgroups of $\mathcal{O}_K$.

- Definition: Suppose K is a number field of degree n over $\mathbb{Q}$ with ring of integers $\mathcal{O}_K$. An order of $\mathcal{O}_K$ is a rank-n subgroup S of $\mathcal{O}_K$.

  - Since $\mathcal{O}_K$ is also free abelian of rank n, orders in $\mathcal{O}_K$ are necessarily free abelian groups of rank n, hence are of the form $\mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$ for some (necessarily linearly-independent) $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$; conversely, any such subgroup is an order of $\mathcal{O}_K$.
  - We can also see easily that for any order S, the quotient group $\mathcal{O}_K/S$ is finite, since it is a quotient of two finitely-generated abelian groups of the same rank, and as we will see, the index $[\mathcal{O}_K : S]$ is closely related to the discriminant.

- Let us now illustrate further how discriminants arise in the context of an integral basis for $\mathcal{O}_K$:

- Proposition (Discriminants and Bases): Let K be a number field of degree n over $\mathbb{Q}$.

  1. Suppose that $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ are $\mathbb{Q}$-linearly independent. Then any $\beta \in \mathcal{O}_K$ can be written in the form $\beta = \frac{1}{d}(c_1\alpha_1 + \cdots + c_n\alpha_n)$ where $d = \text{disc}_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)$ and each $c_i \in \mathbb{Z}$, where furthermore $d | c_i^2$ for each i.
     - Proof: Since $\alpha_1, \ldots, \alpha_n$ are a $\mathbb{Q}$-basis for K, we may write $\beta = e_1\alpha_1 + \cdots + e_n\alpha_n$ for unique $e_i \in \mathbb{Q}$.
     - Now let $\sigma_1, \ldots, \sigma_n$ be the complex embeddings of K, and observe that applying each σ_i to the equation above yields a system of n linear equations of the form $\sigma_i(\beta) = e_1\sigma_1(\alpha_1) + \cdots + e_n\sigma_i(\alpha_i)$ for $1 \leq i \leq n$.
     - Solving this system using Cramer's rule yields $e_i = \frac{\det(M_i)}{\det(M)}$ where $M = \begin{bmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{bmatrix}$ and M_i is the matrix obtained by replacing the ith column of M by the vector $[\sigma_1(\beta), \ldots, \sigma_n(\beta)]^T$.
     - Multiplying numerator and denominator by $\det(M)$ yields $e_i = \frac{\det(M)\det(M_i)}{d}$ where $d = \text{disc}_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)$.
     - Observe now that since the entries in M and M_i are algebraic integers, $\det(M)\det(M_i)$ is an algebraic integer, and since e_i and d are both rational, $\det(M)\det(M_i)$ must also be rational, hence it is some integer c_i.
     - Finally, for the last statement, observe that $c_i^2/d = \det(M_i)^2$ is both rational and an algebraic integer, hence is also an integer.
     - Remark: We can see in this argument that the discriminant naturally arises in this context of trying to express $\beta \in \mathcal{O}_K$ as a $\mathbb{Q}$-linear combination of the α_i, and specifically in attempting to compute the denominators of these expressions. The point is that the initial denominator $\det(M)$ is not necessarily rational, but (as we showed) its square is, and this gives a convenient uniform choice for all of the denominators we need to use.
     - Exercise: Use the result above to prove directly that $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n.
  2. If S is any order of $\mathcal{O}_K$, then $\text{disc}_{K/\mathbb{Q}}(S) = [\mathcal{O}_K : S]^2 \text{disc}_{K/\mathbb{Q}}(\mathcal{O}_K)$.
     - Exercise: Suppose G is isomorphic to $\mathbb{Z}^n$ and H is a subgroup of rank n. Show that G/H is isomorphic to a direct sum of n finite cyclic groups. [Hint: How many generators does it have?]
     - Proof 1: By the exercise, we see that $\mathcal{O}_K/S$ is isomorphic to a group of the form $(\mathbb{Z}/d_1\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/d_n\mathbb{Z})$.
     - Letting $\beta_1, \ldots, \beta_n \in \mathcal{O}_K$ be preimages of the generators of each component, we see that $\beta_1, \ldots, \beta_n$ is an integral basis for $\mathcal{O}_K$ while $d_1\beta_1, \ldots, d_n\beta_n$ is an integral basis for S.

- Then $\mathrm{disc}_{K/\mathbb{Q}}(S) = \begin{vmatrix} \sigma_1(d_1\beta_1) & \cdots & \sigma_1(d_n\beta_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(d_1\beta_1) & \cdots & \sigma_n(d_n\beta_n) \end{vmatrix}^2 = (d_1 d_2 \cdots d_n)^2 \begin{vmatrix} \sigma_1(\beta_1) & \cdots & \sigma_1(\beta_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\beta_1) & \cdots & \sigma_n(\beta_n) \end{vmatrix}^2 = [\mathcal{O}_K : S]^2 \mathrm{disc}_{K/\mathbb{Q}}(\mathcal{O}_K)$, as desired.
- Proof 2: Let $\alpha_1, \ldots, \alpha_n$ be an integral basis for S and $\beta_1, \ldots, \beta_n$ be an integral basis for $\mathcal{O}_K$. Since $\beta_1, \ldots, \beta_n$ is an integral basis for $\mathcal{O}_K$, there exists an integer matrix T such that $\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = T \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix}$. By the volume-transforming property of the determinant, we then see that $[\mathcal{O}_K : S] = |\det T|$.
- Applying each of the complex embeddings $\sigma_1, \ldots \sigma_n$ to each side and combining into a matrix then yields $\begin{bmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha_n) \end{bmatrix} = T \begin{bmatrix} \sigma_1(\beta_1) & \cdots & \sigma_1(\beta_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\beta_1) & \cdots & \sigma_n(\beta_n) \end{bmatrix}$.
- Taking determinants and squaring then yields $\mathrm{disc}_{K/\mathbb{Q}}(S) = (\det T)^2 \mathrm{disc}_{K/\mathbb{Q}}(\mathcal{O}_K) = [\mathcal{O}_K : S]^2 \mathrm{disc}_{K/\mathbb{Q}}(\mathcal{O}_K)$, as claimed.

3. If S is any order of $\mathcal{O}_K$, we have $S = \mathcal{O}_K$ if and only if $\mathrm{disc}_{K/\mathbb{Q}}(S) = \mathrm{disc}_{K/\mathbb{Q}}(\mathcal{O}_K)$. Equivalently, a set $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ is an integral basis for $\mathcal{O}_K$ if and only if $\mathrm{disc}_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) = \mathrm{disc}_{K/\mathbb{Q}}(\mathcal{O}_K)$.
   - Proof: Immediate from (2), since $S = \mathcal{O}_K$ if and only if $[\mathcal{O}_K : S] = 1$.
   - Exercise: Show that for $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$, if $\mathrm{disc}_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)$ is squarefree, then $\mathcal{O}_K = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$.

- Let us now try to construct a convenient integral basis for $\mathcal{O}_K$. If $K = F(\alpha)$ where by rescaling we can take $\alpha \in \mathcal{O}_K$, then certainly the "power basis" $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ is a (field) basis for $K/\mathbb{Q}$ and generates an order $S = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \cdots \oplus \mathbb{Z}\alpha^{n-1}$.
  - We might hope that we can always find a basis for $\mathcal{O}_K$ of this form, but (unfortunately) that is not always the case.
  - Nonetheless, we can use this order as a starting point to try to find an integral basis. Obviously, we can certainly find one where each element is a rational polynomial in α, for entirely silly reasons: namely, because every element of K is a polynomial in α because $K = \mathbb{Q}(\alpha)$.
  - What we would like is to have more control on what these polynomials look like.
  - It seems plausible that we should be able to do some sort of "replacement argument" (similar to Gram-Schmidt), starting with the set of powers $1, \alpha, \ldots, \alpha^{n-1}$ that constructs an integral basis one polynomial at a time by dividing α^k by some integer d_i (necessarily dividing $\mathrm{disc}(\mathcal{O}_K)$, since these are the worst denominators needed per (1) above), and then taking a linear combination of the previous basis elements to obtain another algebraic integer.

0.6 (Sep 16) Constructing Integral Bases for $\mathcal{O}_K$

- Our first order of business is to compute the discriminant for the order obtained from a power basis, and then to modify it by introducing appropriate denominators to obtain an integral basis for $\mathcal{O}_K$:

- Proposition (Discriminants and Bases): Suppose $K = \mathbb{Q}(\alpha)$ for an algebraic integer α and let S be the order of $\mathcal{O}_K$ generated by α, so that $S = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \cdots \oplus \mathbb{Z}\alpha^{n-1}$.

1. Suppose α has minimal polynomial $m(x) \in \mathbb{Z}[x]$ with roots $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$. Then $\mathrm{disc}_{K/\mathbb{Q}}(S) = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2 = (-1)^{n(n-1)/2} N_{K/\mathbb{Q}}[m'(\alpha)]$.
   - Note that $\prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2$ is the polynomial discriminant of $m(x)$, so we see that our use of the same word for both quantities is consistent.

- Proof: Label the roots α_i so that $\alpha_i = \sigma_i(\alpha)$. Then $\mathrm{disc}_{K/\mathbb{Q}}(S) = \mathrm{disc}_{K/\mathbb{Q}}(1, \alpha, \ldots, \alpha^{n-1})$ is the square of the Vandermonde determinant $\begin{vmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \cdots & \alpha_n^{n-1} \end{vmatrix}$, whose value is $\prod_{1 \le i < j \le n}(\alpha_i - \alpha_j)$, yielding the first part of the formula.
- For the second part, switch the order on half of the terms (a total of $n(n-1)/2$) to see $\mathrm{disc}_{K/\mathbb{Q}}(S) = (-1)^{n(n-1)/2} \prod_{i=1}^{n} \prod_{j \neq i}(\alpha_i - \alpha_j)$.
- Factoring $m(x) = (x - \alpha_i)q_i(x)$ where $q_i(x) = \prod_{j \neq i}(x - \alpha_j)$, now differentiate to see $m'(x) = q_i(x) + (x - \alpha_i)q_i'(x)$: thus setting $x = \alpha_i$ yields $m'(\alpha_i) = q_i(\alpha_i) = \prod_{j \neq i}(\alpha_i - \alpha_j)$.
- Therefore we see $\prod_{i=1}^{n} \prod_{j \neq i}(\alpha_i - \alpha_j) = \prod_{i=1}^{n} m'(\alpha_i) = N_{K/\mathbb{Q}}[m'(\alpha)]$, whence the second part of the formula.
- Exercise: If $\alpha^3 + \alpha + 1 = 0$, show that the ring of integers of $\mathbb{Q}(\alpha)$ is $\mathbb{Z}[\alpha]$. [Hint: Compute the discriminant of $\{1, \alpha, \alpha^2\}$.]

2. There exists an integral basis for $\mathcal{O}_K$ of the form $\frac{f_0(\alpha)}{d_0}, \frac{f_1(\alpha)}{d_1}, \frac{f_2(\alpha)}{d_2}, \ldots, \frac{f_{n-1}(\alpha)}{d_{n-1}}$ where each $f_i(x) \in \mathbb{Z}[x]$ is monic of degree i and where the d_i are positive integers with $1 = d_0 | d_1 | d_2 | \cdots | d_{n-1} | d$.

- Proof: Let $d = \mathrm{disc}_{K/\mathbb{Q}}(1, \alpha, \ldots, \alpha^{n-1})$. For each $0 \le k \le n-1$, let $F_k = \frac{1}{d}[\mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \cdots \oplus \mathbb{Z}\alpha^k]$ and observe that F_k is a free abelian group of rank $k+1$. Also let $R_k = \mathcal{O}_K \cap F_k$ be the additive group of algebraic integers in F_k.
- We now show by induction that we can select d_i and f_i so that $\frac{f_0(\alpha)}{d_0}, \frac{f_1(\alpha)}{d_1}, \ldots, \frac{f_k(\alpha)}{d_k}$ is an integral basis for R_k.
- For the base case $n = 0$, start with $\beta_0 = 1$.
- Now suppose we have selected $\beta_0, \ldots, \beta_{k-1}$ that is an integral basis for R_{k-1}, where $\beta_i = \frac{f_i(\alpha)}{d_i}$ for integers $1 = d_0 | d_1 | \cdots | d_{k-1}$ and monic polynomials $f_i(x) \in \mathbb{Z}[x]$ of degree i.
- Consider the linear functional $T_k : K \to \mathbb{Q}$ mapping an element $\beta = c_0 + \cdots + c_{n-1}\alpha^{n-1} \in K$ (with the $c_i \in \mathbb{Q}$) to its basis coefficient c_k of α^k. The image $T_k(R_k)$ lies inside $T_k(F_k) = \frac{1}{d}\mathbb{Z}$, which is an infinite cyclic group. Furthermore, since $\alpha^{k-1} \in R_k$, the image contains 1, so the image is itself an infinite cyclic group of the form $\frac{1}{d_k}\mathbb{Z}$ for some $d_k | d$.
- We claim that we can choose any $\beta_k \in R_k$ such that $T_k(\beta_k) = \frac{1}{d_k}$, and it will have the desired properties.
- We can see that for any $x \in R_k$, if $T_k(x) = \frac{c_k}{d_k}$ then $T_k(x - c_k\beta_k) = 0$ whence the α^k-coefficient of x is zero. But then $x - c_k\beta_k \in R_{k-1}$ so by the induction hypothesis we see $x - c_k\beta_k$ is an integer linear combination of $\beta_0, \ldots, \beta_{k-1}$, whence x is an integer linear combination of $\beta_0, \ldots, \beta_{k-1}, \beta_k$.
- Thus $\beta_0, \ldots, \beta_{k-1}, \beta_k$ is an integral basis for R_k. Now we just have to show $\beta = \frac{f_k(\alpha)}{d_k}$ for some monic $f_k \in \mathbb{Z}[x]$ of degree k, and that $d_{k-1} | d_k$.
- For the second statement, observe that $\alpha\frac{f_{k-1}(\alpha)}{d_{k-1}}$ is an algebraic integer and in F_k, hence in R_k. Then since f_{k-1} is monic of degree $k-1$ we see $T_k(\frac{\alpha f_{k-1}(\alpha)}{d_{k-1}}) = \frac{1}{d_{k-1}}$: this means $\frac{1}{d_{k-1}} \in T_k(R_k) = \frac{1}{d_k}\mathbb{Z}$ and thus $d_{k-1} | d_k$.
- Now, observe that $\beta\frac{d_k}{d_{k-1}}$ is an algebraic integer and is in F_k hence is in R_k, as is $\alpha\frac{f_{k-1}(\alpha)}{d_{k-1}}$ as noted above, hence so is their difference $\gamma = \frac{d_k\beta - \alpha f_{k-1}(\alpha)}{d_{k-1}}$.
- But since $T_k[\gamma] = \frac{d_k}{d_{k-1}}T_k[\beta] - \frac{1}{d_{k-1}}T_k[\alpha f_{k-1}(\alpha)] = \frac{1}{d_{k-1}} - \frac{1}{d_{k-1}} = 0$, the α^k-coefficient of γ is zero, so in fact $\gamma \in R_{k-1}$.

- Thus, by hypothesis γ is a $\mathbb{Z}-$linear combination of $\frac{f_0(\alpha)}{d_0}, \frac{f_1(\alpha)}{d_1}, \frac{f_2(\alpha)}{d_2}, \ldots, \frac{f_{k-1}(\alpha)}{d_{k-1}}$, which since $d_0|d_1|\cdots|d_{k-1}$, is of the form $\frac{g(\alpha)}{d_{k-1}}$ for some $g(x) \in \mathbb{Z}[x]$ of degree at most $k-1$.
- This (finally) means we may take $f_k(x) = xf_{k-1}(x) + g(x) \in \mathbb{Z}[x]$; since $\beta = \frac{1}{d_k}[\alpha f_{k-1}(\alpha) + g(\alpha)]$ and $f_k(x)$ is monic of degree k, we have shown all of the required properties.
- Remark: The integers d_i are uniquely determined, but in fact there is a great deal of latitude to choose the polynomials f_i: in fact since the choice of $\beta \in R_k$ was arbitrary aside from requiring its α^k-coefficient to be $1/d_k$, we may take f_i to be any monic polynomial in $\mathbb{Z}[x]$ of degree i such that $f_i(\alpha)/d_i$ is an algebraic integer.

- In principle, the construction given in (2) above can be made mostly effective.
  - To convert (2) to an algorithm clearly requires a way of computing coefficients with respect to an integral basis: that is simply a special case of computing coefficients with respect to a $\mathbb{Q}$-basis, which we can do with linear algebra.
  - We also require a way of computing what the terms d_k are: in principle this could be done by searching for algebraic integers with the desired properties and computing the denominators obtained, since we know the worst possible denominators are the discriminant d. However, it would be more convenient if we could calculate the terms d_k directly, or at least describe them more explicitly.

- Proposition (Polynomial Bases): Suppose K is a degree-n number field, let $\alpha \in \mathcal{O}_K$, and suppose $\mathcal{O}_K$ has an integral basis of the form $\frac{f_0(\alpha)}{d_0}, \frac{f_1(\alpha)}{d_1}, \frac{f_2(\alpha)}{d_2}, \ldots, \frac{f_{n-1}(\alpha)}{d_{n-1}}$ where each $f_i(x) \in \mathbb{Z}[x]$ is monic of degree i and where the d_i are positive integers with $1 = d_0|d_1|d_2|\cdots|d_{n-1}|d = \mathrm{disc}(K)$. Also let $R_k = \mathcal{O}_K \cap \frac{1}{d}[\mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \cdots \oplus \mathbb{Z}\alpha^k]$.

  1. The set $\frac{f_0(\alpha)}{d_0}, \frac{f_1(\alpha)}{d_1}, \frac{f_2(\alpha)}{d_2}, \ldots, \frac{f_k(\alpha)}{d_k}$ is an integral basis of R_k for each $0 \leq k \leq n-1$.
     - Proof: Since $\frac{f_0(\alpha)}{d_0}, \frac{f_1(\alpha)}{d_1}, \frac{f_2(\alpha)}{d_2}, \ldots, \frac{f_k(\alpha)}{d_k}$ is clearly linearly independent, it suffices to show that it spans R_k. So let $\beta \in R_k$: then because $\beta \in \mathcal{O}_K$ we may write $\beta = c_0\frac{f_0(\alpha)}{d_0} + c_1\frac{f_1(\alpha)}{d_1} + \cdots + c_{n-1}\frac{f_{n-1}(\alpha)}{d_{n-1}}$ for unique $c_i \in \mathbb{Z}$, and because $\beta \in \mathrm{span}_{\mathbb{Q}}(1, \alpha, \ldots, \alpha^k)$ we may also write $\beta = e_0\frac{f_0(\alpha)}{d_0} + e_1\frac{f_1(\alpha)}{d_1} + \cdots + e_k\frac{f_k(\alpha)}{d_k}$ for unique $e_i \in \mathbb{Q}$.
     - Comparing the two expressions shows immediately that $c_i = e_i$ for each $i \leq k$ (and $c_i = 0$ for $i > k$) hence all of the e_i are integers. The conclusion follows.
  2. For each k, d_k is the smallest positive integer such that $d_kR_k \subseteq \mathbb{Z}[\alpha]$. In particular, for fixed α, all of the d_k are uniquely determined.
     - Exercise: Suppose α is algebraic of degree n over $\mathbb{Q}$. If $f(x), g(x) \in \mathbb{Q}[x]$ are such that $f(\alpha) = g(\alpha)$ and both f, g have degree less than n, show that $f(x) = g(x)$.
     - Proof: Multiplying any element of R_k by d_k clears all of the denominators d_i from the integral basis expression (thus yielding an integer polynomial in α), so certainly $d_kR_k \subseteq \mathbb{Z}[\alpha]$.
     - On the other hand, since $f_k(\alpha)/d_k \in R_k$ by (1) and because f_k is monic, no smaller multiple of $f_k(\alpha)$ can yield a polynomial with integer coefficients in α (which by reducing modulo its minimal polynomial we can assume is of degree less than n) by the exercise above.
     - Thus, d_k is the smallest positive integer such that $d_kR_k \subseteq \mathbb{Z}[\alpha]$.
  3. For $S = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \cdots \oplus \mathbb{Z}\alpha^{k-1}$, we have $d_1 \cdots d_{n-1} = [\mathcal{O}_K : S]$.
     - Proof: Since f_i is monic of degree i, it is easy to see that $f_0(\alpha), f_1(\alpha), \ldots, f_n(\alpha)$ is an integral basis for S (the change-of-basis matrix is triangular with 1s on its diagonal). We can then see that $\mathcal{O}_K/S \cong (\mathbb{Z}/d_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_n\mathbb{Z})$; taking cardinalities yields the result immediately.

- Remark: Note in fact that the divisibility condition $d_1|\cdots|d_n$ implies that this product of cyclic groups is the elementary divisor form of the finite abelian group $\mathcal{O}_K/S$, which gives another proof that the d_k are unique.

4. We have $d_i d_j | d_{i+j}$.
   - Proof: Note that $\gamma = \dfrac{f_i(\alpha)}{d_i} \cdot \dfrac{f_j(\alpha)}{d_j}$ is an algebraic integer and (when multiplied out) it is a polynomial in α of degree $i+j$, so it is an element of R_{i+j}.
   - By (1), γ is then an integer linear combination of $\dfrac{f_0(\alpha)}{d_0}, \ldots, \dfrac{f_{i+j}(\alpha)}{d_{i+j}}$; comparing coefficients of α^{i+j} then shows that $\dfrac{1}{d_i d_j}$ must be an integer multiple of $\dfrac{1}{d_{i+j}}$, which is to say, $d_i d_j$ divides d_{i+j}.
5. The discriminant $\text{disc}(S)$ is divisible by $d_1^{n(n-1)}$.
   - Proof: By a trivial induction using (4) we see that $d_1^k | d_k$ for each k. Multiplying these and then squaring, we see that $d_1^{n(n-1)}$ divides the product $(d_1 d_2 \cdots d_{n-1})^2$, which by (3) equals $[\mathcal{O}_K : S]^2$.
   - But by our earlier results we know that $\text{disc}(S) = [\mathcal{O}_K : S]^2 \text{disc}(\mathcal{O}_K)$, so the result follows.
   - Remark: The point here is that we can actually compute $\text{disc}(S) = \pm N_{K/\mathbb{Q}}[m'(\alpha)]$ where $m(x)$ is the minimal polynomial of α, and so we obtain a (typically short) list of possible values for d_1. We can use (4) to establish similar divisibility properties for the other d_i which likewise help narrow down their possible values.

0.7 (Sep 18) Some Examples of Integral Bases for $\mathcal{O}_K$

- After all of that effort, we can now actually compute some integral bases for some other $\mathcal{O}_K$.
  - Even in the relatively straightforward situation of cubic extensions, we generally still need to do some nontrivial calculations in order to find the values of d_1 and d_2 to ensure we have the full ring of integers.
  - A centrally useful tool here is the trace map, since it allows us to extract information about individual coefficients. (In cases of extensions having nontrivial proper subfields, the relative trace maps to the subfields are also quite useful, of course.)
- Exercise: Show that the discriminant of the cubic polynomial $p(x) = x^3 + ax + b$ is $-4a^3 - 27b^2$.
- Example: Show that the ring of integers of $\mathbb{Q}(\alpha)$ for $\alpha^3 - \alpha + 1 = 0$ is $\mathbb{Z}[\alpha]$, with integral basis $\{1, \alpha, \alpha^2\}$.
  - The generator α has minimal polynomial $m(x) = x^3 - 2$ over $\mathbb{Q}$ as this polynomial is clearly irreducible.
  - By the exercise above, we have $\text{disc}(\alpha) = 31$.
  - From our results we know that $\mathcal{O}_K$ has an integral basis of the form $1, \dfrac{f_1(\alpha)}{d_1}, \dfrac{f_2(\alpha)}{d_2}$ with $d_1 | d_2$ and where $(d_1 d_2)^2$ divides $\text{disc}(\alpha)$. So we must have $d_1 = d_2 = 1$ hence we may take $f_1(\alpha) = \alpha$ and $f_2(\alpha) = \alpha^2$.
  - We conclude that $\{1, \alpha, \alpha^2\}$ is an integral basis for the ring of integers, meaning it is simply $\mathbb{Z}[\alpha]$.
- Exercise: More generally, suppose $m(x) \in \mathbb{Z}[x]$ is monic, irreducible, and has squarefree discriminant. If α is any root of $m(x)$, prove that the ring of integers of $K = \mathbb{Q}(\alpha)$ is $\mathbb{Z}[\alpha]$.
- Example: Show that the ring of integers of $K = \mathbb{Q}(\sqrt[3]{2})$ is $\mathbb{Z}[\sqrt[3]{2}]$, with integral basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$.
  - The element $\alpha = \sqrt[3]{2}$ has minimal polynomial $m(x) = x^3 - 2$ over $\mathbb{Q}$ as this polynomial is clearly irreducible.
  - Since $m'(x) = 3x^2$ we see $\text{disc}(\alpha) = (-1)^3 N_{K/\mathbb{Q}}(3 \cdot 2^{2/3}) = -2^2 \cdot 3^3$.
  - From our results we know that $\mathcal{O}_K$ has an integral basis of the form $1, \dfrac{f_1(\alpha)}{d_1}, \dfrac{f_2(\alpha)}{d_2}$ where $d_1 | d_2 | d$ and where d_1^6 divides $\text{disc}(\alpha)$. So we must have $d = 1$ and may then clearly take $f_1(\alpha) = \alpha$.

- We also know that $(d_1 d_2)^2 = d_2^2$ divides $\mathrm{disc}(\alpha)$, so d_2 divides 6: thus the other basis element is of the form $\beta = \dfrac{c_0 + c_1\alpha + c_2\alpha^2}{6}$ for some integers c_0, c_1, c_2. Then $\mathrm{tr}(\beta) = c_0/2$ so c_0 is even. Then $\gamma = 3\beta - c_0/2 = \dfrac{c_1\alpha + c_2\alpha^2}{2}$ is also an algebraic integer, but now $\gamma^3 = \dfrac{(c_1 + c_2\alpha)^3}{4}$ has trace $\dfrac{3}{4}(c_1^3 + 2c_2^3)$, which can only be an integer when both c_1 and c_2 are also even.
- We conclude that in fact $\beta = \dfrac{d_0 + d_1\alpha + d_2\alpha^2}{3}$ for some integers d_0, d_1, d_2 which, by subtracting an appropriate polynomial in α, we may assume are each 0, 1, or 2.
- Squaring yields $\beta^2 = \dfrac{(d_0^2 + 2d_1d_2) + (2d_0d_1 + 2d_2^2)\alpha + (d_1^2 + 2d_0d_2)\alpha^2}{9}$. In order for this quantity to be an algebraic integer, each of $d_0^2 + 2d_1d_2$, $d_0d_1 + d_2^2$, and $d_1^2 + 2d_0d_2$ must be divisible by 3 (this follows because $d_2|3$, so we cannot have denominators of 9). If any of d_0, d_1, d_2 is zero, all of them must be zero mod 3; otherwise, in the event all are nonzero, we see $d_0^2 \equiv d_1^2 \equiv d_2^2 \equiv 1 \pmod 3$, whence $d_1d_2 \equiv d_0d_2 \equiv -d_0d_1 \equiv 1 \pmod 3$. But this is a contradiction since the first two equalities require $d_0 \equiv d_1 \equiv d_2 \bmod 3$, which contradicts the third condition.
- Therefore, all of d_0, d_1, d_2 are zero mod 3, and (thus, finally) we see that $\beta \in \mathbb{Z}[\alpha]$. We conclude that we may take $\beta = \alpha^2$ and so we obtain our integral basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$.

- We remark that one may compute the ring of integers of $\mathbb{Q}(\sqrt[3]{m})$ for general (cubefree) m using a similar approach. Here are two examples:

- Exercise: Show that the ring of integers of $\mathbb{Q}(\sqrt[3]{5})$ is $\mathbb{Z}[\sqrt[3]{5}]$. [Hint: First note $d_1 = 1$, then show $d_2|10$. Eliminate the possibility that d_2 is even, then show that $d_2 = 5$ leads to an eventual contradiction modulo 5.]

- Exercise: Show that the ring of integers of $\mathbb{Q}(\sqrt[3]{10})$ has integral basis $\{1, \sqrt[3]{10}, \dfrac{1 + \sqrt[3]{10} + \sqrt[3]{100}}{3}\}$. [Hint: First note $d_1 = 1$, then show $d_2|30$. Use traces to eliminate the possibility that d_2 is even or divisible by 5, and then conclude $d_2 = 3$.]

- Example: Show that the ring of integers of $K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$ is $\mathbb{Z}[\sqrt{2}, \dfrac{1+\sqrt{5}}{2}]$, with integral basis $\{1, \sqrt{2}, \dfrac{1+\sqrt{5}}{2}, \dfrac{\sqrt{2}+\sqrt{10}}{2}\}$
  - Note that K has the three quadratic subfields $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{10})$ with respective rings of integers $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\dfrac{1+\sqrt{5}}{2}]$, $\mathbb{Z}[\sqrt{10}]$.
  - The Galois group of $K/\mathbb{Q}$ is isomorphic to the Klein 4-group, with generators σ, τ obtained by lifting the conjugation automorphisms in the two subfields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$: thus $\sigma(\sqrt{2}, \sqrt{5}) = (-\sqrt{2}, \sqrt{5})$ and $\tau(\sqrt{2}, \sqrt{5}) = (\sqrt{2}, -\sqrt{5})$, so $\sigma\tau(\sqrt{2}, \sqrt{5}) = (-\sqrt{2}, -\sqrt{5})$. (Note that $\sigma\tau$ fixes the other quadratic subfield $\mathbb{Q}(\sqrt{10})$.)
  - Then the algebraic integer $\alpha = \sqrt{2} + \sqrt{5}$ is a generator for this extension, since its Galois conjugates $\pm\sqrt{2} \pm \sqrt{5}$ are all distinct. One option would then be to attempt to construct an integral basis using the powers of α.
  - However, in this situation, since we already know that the ring of integers of $\mathbb{Q}(\sqrt{2})$ is $\mathbb{Z}[\sqrt{2}]$, that the ring of integers of $\mathbb{Q}(\sqrt{5})$ is $\mathbb{Z}[\dfrac{1+\sqrt{5}}{2}]$, and that the ring of integers of $\mathbb{Q}(\sqrt{10})$ is $\mathbb{Z}[\sqrt{10}]$, a more natural choice would be to use the elements from these integral bases as a starting point.
  - So let us instead suppose that $\alpha = a + b\sqrt{2} + c\sqrt{5} + d\sqrt{10}$ is an algebraic integer, for $a, b, c, d \in \mathbb{Q}$.
  - Then in particular, the relative traces (and norms) of α from K to each of the quadratic subfields must be algebraic integers.
  - So, $\mathrm{tr}_{K/\mathbb{Q}(\sqrt{2})}(\alpha) = \alpha + \tau(\alpha) = 2a + 2b\sqrt{2}$ must be in $\mathbb{Z}[\sqrt{2}]$, so $2a$ and $2b$ are integers.
  - Next, $\mathrm{tr}_{K/\mathbb{Q}(\sqrt{10})}(\alpha) = \alpha + \sigma(\alpha) = 2a + 2c\sqrt{5}$ must be in $\mathbb{Z}[\dfrac{1+\sqrt{5}}{2}]$, so since $2a$ is an integer, $2c$ must also be an integer.
  - Finally, $\mathrm{tr}_{K/\mathbb{Q}(\sqrt{10})}(\alpha) = \alpha + \sigma\tau(\alpha) = 2a + 2d\sqrt{10}$ must be in $\mathbb{Z}[\sqrt{10}]$, so $2a$ and $2d$ must be integers.

- Hence we must have $\alpha = \frac{p+q\sqrt{2}+r\sqrt{5}+s\sqrt{10}}{2}$ for integers p,q,r,s. Then $\alpha - r\frac{1+\sqrt{5}}{2} - s\frac{\sqrt{2}+\sqrt{10}}{2} = \frac{(p-r)+(q-s)\sqrt{2}}{2}$ is also an algebraic integer, but this is an element of $\mathbb{Q}(\sqrt{2})$ hence must be of the form $u+v\sqrt{2}$ for integers u,v.
- We conclude that $\alpha = u+v\sqrt{2}+r\frac{1+\sqrt{5}}{2}+s\frac{\sqrt{2}+\sqrt{10}}{2}$ for integers u,v,r,s, and so $1, \sqrt{2}, \frac{1+\sqrt{5}}{2}, \frac{\sqrt{2}+\sqrt{10}}{2}$ is an integral basis for the ring of integers, as claimed.

- Example: Show that the ring of integers of $K = \mathbb{Q}(\sqrt{5},\sqrt{13})$ is $\mathbb{Z}[\frac{1+\sqrt{5}}{2}, \frac{1+\sqrt{13}}{2}]$, with integral basis $\{1, \frac{1+\sqrt{5}}{2}, \frac{1+\sqrt{13}}{2}, \frac{(1+\sqrt{5})(1+\sqrt{13})}{4}\}$.
  - Note that K has the three quadratic subfields $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{13})$, $\mathbb{Q}(\sqrt{65})$ with respective rings of integers $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$, $\mathbb{Z}[\frac{1+\sqrt{13}}{2}]$, $\mathbb{Z}[\frac{1+\sqrt{65}}{2}]$.
  - The Galois group of $K/\mathbb{Q}$ is isomorphic to the Klein 4-group, now with generators σ, τ such that $\sigma(\sqrt{5},\sqrt{13}) = (-\sqrt{5},\sqrt{13})$ and $\tau(\sqrt{5},\sqrt{13}) = (\sqrt{5},-\sqrt{13})$ and $\sigma\tau(\sqrt{5},\sqrt{13}) = (-\sqrt{5},-\sqrt{13})$.
  - Now suppose that $\alpha = a+b\sqrt{5}+c\sqrt{13}+d\sqrt{65}$ is an algebraic integer, for $a,b,c,d \in \mathbb{Q}$.
  - Then $\mathrm{tr}_{K/\mathbb{Q}(\sqrt{2})}(\alpha) = \alpha+\tau(\alpha) = 2a+2b\sqrt{5}$ must be in $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$, so $4a$ and $4b$ are integers of the same parity.
  - Also, $\mathrm{tr}_{K/\mathbb{Q}(\sqrt{13})}(\alpha) = \alpha+\sigma(\alpha) = 2a+2c\sqrt{13}$ must be in $\mathbb{Z}[\frac{1+\sqrt{13}}{2}]$, so $4a$ and $4c$ must be integers of the same parity.
  - Also, $\mathrm{tr}_{K/\mathbb{Q}(\sqrt{65})}(\alpha) = \alpha+\sigma\tau(\alpha) = 2a+2c\sqrt{65}$ must be in $\mathbb{Z}[\frac{1+\sqrt{65}}{2}]$, so $4a$ and $4d$ must be integers of the same parity.
  - Hence we must have $\alpha = \frac{p+q\sqrt{5}+r\sqrt{13}+s\sqrt{65}}{4}$ for integers p,q,r,s all of the same parity. By subtracting $\frac{(1+\sqrt{5})(1+\sqrt{65})}{4} = \frac{1+\sqrt{5}+5\sqrt{13}+\sqrt{65}}{4}$ if all of p,q,r,s are odd, we can make all of p,q,r,s even, in which case $\alpha = \frac{p'+q'\sqrt{5}+r'\sqrt{13}+s'\sqrt{65}}{2} + x\frac{(1+\sqrt{5})(1+\sqrt{65})}{4}$ for $x = 0$ or 1.
  - Then $\alpha - q'\frac{1+\sqrt{5}}{2} - r'\frac{1+\sqrt{13}}{2} - s'\frac{1+\sqrt{65}}{2} = \frac{p'-q'-r'-s'}{2}$ must be an (actual) integer u, meaning that $\alpha = u+q'\frac{1+\sqrt{5}}{2}+r'\frac{1+\sqrt{13}}{2}+s'\frac{1+\sqrt{65}}{2}+x\frac{(1+\sqrt{5})(1+\sqrt{13})}{4}$ for integers u,q',r',s',x.
  - Finally we note that $\frac{1+\sqrt{65}}{2} = 3+2\frac{(1+\sqrt{5})(1+\sqrt{65})}{4} - \frac{1+\sqrt{5}}{2} - 5\frac{1+\sqrt{13}}{2}$, so the extra element $\frac{1+\sqrt{65}}{2}$ can be written in terms of the other four.
  - We conclude that $\{1, \frac{1+\sqrt{5}}{2}, \frac{1+\sqrt{13}}{2}, \frac{(1+\sqrt{5})(1+\sqrt{13})}{4}\}$ is an integral basis for the ring of integers, as claimed.

- Exercise: Show that the ring of integers of $\mathbb{Q}(\sqrt{3},\sqrt{7})$ has integral basis $\{1, \sqrt{3}, \frac{\sqrt{3}+\sqrt{7}}{2}, \frac{1+\sqrt{21}}{2}\}$.
- Exercise: Compute an integral basis for the ring of integers of $\mathbb{Q}(\sqrt{2},\sqrt{3})$. [Hint: It's bigger than $\mathbb{Z}[\sqrt{2},\sqrt{3}]$.]

0.8 (Sep 19) The Ring of Integers in $\mathbb{Q}(\zeta_n)$

- Our other major source of examples where we can make explicit calculations is the cyclotomic fields $\mathbb{Q}(\zeta_n)$. We will now build up to our main result in this case, which is that the ring of integers of $\mathbb{Q}(\zeta_n)$ is in fact just $\mathbb{Z}[\zeta_n]$.

- For completeness, we may as well build up our stockpile of information about $\mathbb{Q}(\zeta_n)$ from the beginning.
- We recall that an nth root of unity is a complex number z with $z^n = 1$. For $d|n$, any dth root of unity is also an nth root of unity, and the primitive nth roots of unity are those nth roots of unity that are not dth roots of unity for any proper divisor d of n.

- Proposition (Cyclotomic Fields): Let $n \geq 2$ and let $\zeta_n = e^{2\pi i/n}$ be a primitive nth root of unity. The following hold:

1. There are n distinct nth roots of unity, forming a cyclic group of order n under multiplication denoted μ_n. The primitive nth roots of unity are the generators of this cyclic group, of the form ζ_n^a for $\gcd(a, n) = 1$.
   - Proof: Suppose $z \in \mathbb{C}$ has $z^n = 1$. Then $|z| = 1$ and so $z = e^{i\theta}$ for some θ; then $z^n = 1$ is equivalent to $e^{in\theta} = 1$ whence $\theta = 2k\pi/n$ for some integer k, which is to say, $z = \zeta_n^k$.
   - So these ζ_n^k are the nth roots of unity, and since the group homomorphism $\varphi : \mathbb{Z} \to \mu_n$ with $\varphi(k) = \zeta_n^k$ is clearly onto and has kernel $n\mathbb{Z}$, the group μ_n is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.
   - Then the primitive nth roots of unity are the ones which have order exactly n (rather than some proper divisor), so they correspond to the $\varphi(n)$ elements of $(\mathbb{Z}/n\mathbb{Z})^\times$ under the isomorphism: in other words, they are the powers ζ_n^a for a relatively prime to n.
2. Let $\Phi_n(x) = \prod_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} (x - \zeta_n^a)$ be the nth cyclotomic polynomial, whose roots are the primitive nth roots of unity. Then $\Phi_n(x)$ has integer coefficients.
   - Exercise: Show that $x^n - 1 = \prod_{d|n} \Phi_d(x)$. [Hint: Group together the roots of unity of each order $d|n$.]
   - Exercise: Show that $\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}$ where $\mu(n)$ denotes the Möbius μ-function $\mu(n) = \begin{cases} 0 & \text{if } n \text{ is not squarefree} \\ (-1)^k & \text{if } n = p_1 \cdots p_k \text{ for distinct primes } p_i \end{cases}$. Use this recurrence relation to calculate $\Phi_6(x)$ and $\Phi_{20}(x)$.
   - Proof: Using the recursion provided by the exercises above, we can see by induction on n that $\Phi_n(x)$ will always have integer coefficients. The base case $n = 1$ is trivial.
   - For the inductive step, observe that $\prod_{d|n, d<n} \Phi_d(x)$ is monic, has integer coefficients, and divides $x^n - 1$ in $\mathbb{Q}(\zeta_n)[x]$: hence it divides $x^n - 1$ in $\mathbb{Q}[x]$ since both polynomials have coefficients in $\mathbb{Q}$. Then by Gauss's lemma, $\prod_{d|n, d<n} \Phi_d(x)$ divides $x^n - 1$ in $\mathbb{Z}[x]$, so the quotient $\Phi_n(x)$ has integer coefficients.
3. The polynomial $\Phi_n(x)$ is irreducible and is therefore the minimal polynomial of ζ_n over $\mathbb{Q}$.
   - Exercise: For a prime p, show directly that $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible. [Hint: Use Eisenstein's criterion on $\Phi_p(x+1) = \dfrac{(x+1)^p - 1}{x}$.]
   - Proof: Suppose that we have an irreducible monic factor of $\Phi_n(x)$ in $\mathbb{Q}[x]$. By Gauss's lemma, this yields a factorization $\Phi_n(x) = f(x)g(x)$ where $f(x), g(x) \in \mathbb{Z}[x]$ are monic and $f(x)$ is irreducible.
   - Let ω be a primitive nth root of unity that is a root of f, and let p be any prime not dividing n. Since f is irreducible, this means f is the minimal polynomial of ω.
   - By properties of order, we see that ω^p is also a primitive nth root of unity, hence is a root of either f or of g.
   - Suppose ω^p is a root of g, so that $g(\omega^p) = 0$. This means ω is a root of $g(x^p)$, and so since f is the minimal polynomial of ω, it must divide $g(x^p)$: say $f(x)h(x) = g(x^p)$ for some $h(x) \in \mathbb{Z}[x]$.
   - Reducing modulo p, we see $\overline{f}(x)\overline{h}(x) = \overline{g}(x^p) = \overline{g}(x)^p$ in $\mathbb{F}_p[x]$, so by unique factorization we see $\overline{f}(x)$ and $\overline{g}(x)$ have a nontrivial common factor in $\mathbb{F}_p[x]$.
   - Then since $\Phi_n(x) = f(x)g(x)$, reducing modulo p yields $\overline{\Phi_n}(x) = \overline{f}(x)\overline{g}(x)$ and so $\overline{\Phi_n}(x)$ would have a repeated factor, hence so would $x^n - 1$. But this is a contradiction because since $x^n - 1$ is separable in $\mathbb{F}_p[x]$ (its derivative is nx^{n-1}, which is relatively prime to $x^n - 1$ because p does not divide n).
   - Hence we conclude that ω^p is not a root of g, so it must be a root of f. Since this holds for every root ω of f, we see that for any $a = p_1 p_2 \cdots p_k$ that is relatively prime to n, then $\omega^a = ((\omega^{p_1})^{p_2})^{\cdots p_n}$ is a root of f.
   - But this means every primitive nth root of unity is a root of f, and so $\Phi_n = f$ is irreducible as claimed.

4. Both $\Phi_n(x)$ and $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ have degree $\varphi(n)$, and $\Phi_n(x)$ is the minimal polynomial of ζ_n over $\mathbb{Q}$.
   - Proof: By definition $\Phi_n(x)$ has degree $\varphi(n)$. Since Φ_n is irreducible by (3), $\Phi_n(x)$ is then the minimal polynomial of ζ_n hence $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \deg(\Phi_n) = \varphi(n)$.
5. The extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois with Galois group isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$. Explicitly, the elements of the Galois group are the automorphisms σ_a for $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ acting via $\sigma_a(\zeta_n) = \zeta_n^a$.
   - Proof: Since $K = \mathbb{Q}(\zeta_n)$ is the splitting field of $x^n - 1$ (or $\Phi_n(x)$) over $\mathbb{Q}$ it is Galois, and $\#\mathrm{Gal}(K/\mathbb{Q}) = [K:\mathbb{Q}] = \varphi(n)$.
   - Furthermore, any automorphism σ must map ζ_n to one of its Galois conjugates over $\mathbb{Q}$, which are the roots of $\Phi_n(x)$ by (4): explicitly, these are the $\varphi(n)$ values ζ_n^a for a relatively prime to n.
   - Since there are in fact $\varphi(n)$ possible automorphisms, each of these choices must extend to an automorphism of $K/\mathbb{Q}$. Hence the elements of the Galois group are the maps σ_a as claimed.
   - Since $\sigma_a(\sigma_b(\zeta_n)) = \sigma_a(\zeta_n^b) = \zeta_n^{ab}$, the composition of automorphisms is the same as multiplication of the indices in $(\mathbb{Z}/n\mathbb{Z})^\times$, and since this association is a bijection, the Galois group is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$.

- Let us now prove our main result about the ring of integers in $\mathbb{Q}(\zeta_n)$:

- Theorem (Cyclotomic Ring of Integers): Let $n \geq 2$, let $\zeta_n = e^{2\pi i/n}$ be a primitive nth root of unity (so ζ_n is a root of $x^n - 1$). The following hold:

1. For any prime power $p^d > 2$ we have $N_{\mathbb{Q}(\zeta_{p^d})/\mathbb{Q}}(\zeta_{p^d}) = 1$ and $N_{\mathbb{Q}(\zeta_{p^d})/\mathbb{Q}}(1 - \zeta_{p^d}) = p$.
   - Exercise: For any prime power p^d, show that $\Phi_{p^d}(x) = \Phi_p(x^{p^{d-1}})$. [Hint: Show both sides equal $\prod_{i=1}^{p-1}(x^{p^{d-1}} - \zeta_p^i)$.]
   - Proof: By the exercise above, we know that the minimal polynomial of ζ_{p^d} is $\Phi_{p^d}(x) = \Phi_p(x^{p^{d-1}}) = x^{(p-1)p^{d-1}} + x^{(p-2)p^{d-1}} + \cdots + x^{p^{d-1}} + 1$, and we also have the factorization $\Phi_{p^d}(x) = \prod_{a \in (\mathbb{Z}/p^d\mathbb{Z})^\times}(x - \zeta_{p^d}^a)$.
   - Thus, $x^{(p-1)p^{d-1}} + x^{(p-2)p^{d-1}} + \cdots + x^{p^{d-1}} + 1 = \prod_{a \in (\mathbb{Z}/p^d\mathbb{Z})^\times}(x - \zeta_{p^d}^a)$.
   - Now, setting $x = 0$ yields $1 = \prod_{a \in (\mathbb{Z}/p^d\mathbb{Z})^\times}(-\zeta_{p^d}^a) = (-1)^{\varphi(p^d)} N(\zeta_{p^d}) = N(\zeta_{p^d})$ since $\varphi(p^d)$ is even.
   - Also, setting $x = 1$ yields $p = \prod_{a \in (\mathbb{Z}/p^d\mathbb{Z})^\times}(1 - \zeta_{p^d}^a) = N(1 - \zeta_{p^d})$.
2. For any odd prime p with $K = \mathbb{Q}(\zeta_p)$ and $S = \mathbb{Z}[\zeta_p]$, we have $\mathrm{disc}_{K/\mathbb{Q}}(S) = (-1)^{p(p-1)/2} p^{p-2}$.
   - Proof: For brevity, all norms and discriminants are from $\mathbb{Q}(\zeta_p)$ to $\mathbb{Q}$.
   - By our results on discriminants we know that $\mathrm{disc}(S) = (-1)^{p(p-1)/2} N[m'(\zeta_p)]$ where $m(x) = \Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ is the minimal polynomial of ζ_p.
   - A direct evaluation of $m'(\zeta_p)$ using the expansion above is rather unpleasant. Instead, note that $(x-1)m(x) = x^p - 1$: then differentiating and setting $x = \zeta_p$ yields $m(\zeta_p) + (\zeta_p - 1)m'(\zeta_p) = p\zeta_p^{p-1} = p/\zeta_p$, whence $m'(\zeta_p) = \dfrac{-p}{\zeta_p(1-\zeta_p)}$ since of course $m(\zeta_p) = 0$.
   - Then using (1) yields $\mathrm{disc}(S) = (-1)^{p(p-1)/2} N[m'(\zeta_p)] = (-1)^{p(p-1)/2} \dfrac{N(-p)}{N(\zeta_p)N(1-\zeta_p)} = (-1)^{p(p-1)/2} p^{p-2}$.
   - Exercise: Let p be an odd prime. Show that $\mathbb{Q}(\zeta_p)$ contains a unique quadratic subfield and that it is $\mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})$. [Hint: Use Galois theory for uniqueness, and discriminants to get the field itself.]
   - Exercise: Show that every quadratic field is a subfield of some cyclotomic field $\mathbb{Q}(\zeta_n)$. [Hint: Take a composite of $\mathbb{Q}(\zeta_8)$ and the $\mathbb{Q}(\zeta_p)$ for various p.] This is a special case of the Kronecker-Weber theorem: every number field K with abelian Galois group over $\mathbb{Q}$ is a subfield of some cyclotomic field.
3. For any $n \geq 2$ and $S = \mathbb{Z}[\zeta_n]$, the discriminant $\mathrm{disc}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(S)$ divides $n^{\varphi(n)}$.
   - Proof: For $g(x) = \prod_{d|n, d<n}(x - \zeta_n^d)$, we have $x^n - 1 = \Phi_n(x)g(x)$. Differentiating and then setting $x = \zeta_n$ yields $n\zeta_n^{-1} = \Phi_n'(\zeta_n)g(\zeta_n) + \Phi_n(\zeta_n)g'(\zeta_n) = \Phi_n'(\zeta_n)g(\zeta_n)$.

- Taking norms from $\mathbb{Q}(\zeta_n)$ to $\mathbb{Q}$ (noting that $N(\zeta_n^{-1}) = \pm 1$ since it is a unit) then yields $\pm n^{\varphi(n)} = N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}[\Phi_n'(\zeta_n)] \cdot N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}[g(\zeta_n)]$, and so $N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}[\Phi_n'(\zeta_n)]$ divides $n^{\varphi(n)}$.
- The desired result then follows immediately from $\text{disc}(S) = (-1)^{n(n-1)/2} N[\Phi_n'(\zeta_n)]$.

4. For any prime power p^d, the ring of integers of $K = \mathbb{Q}(\zeta_{p^d})$ is $\mathbb{Z}[\zeta_{p^d}]$.
   - Proof: For brevity write $\zeta = \zeta_{p^d}$. First, since $\mathbb{Z}[\zeta] = \mathbb{Z}[1-\zeta] = \mathbb{Z} \oplus \mathbb{Z}(1-\zeta) \oplus \cdots \oplus \mathbb{Z}(1-\zeta)^{\varphi(p^d)}$ since the minimal polynomial for ζ (hence $1-\zeta$) has degree $\varphi(p^d)$, by (3) we know that $\text{disc}(1-\zeta)$ divides $p^{d\varphi(p^d)}$, which is a power of p.
   - Then from our earlier results on discriminants, we know that any element of $\mathcal{O}_K$ can be written in the form $\dfrac{c_0 + c_1(1-\zeta) + \cdots + c_{\varphi(p^d)}(1-\zeta)^{\varphi(p^d)}}{p^k}$ for some integer k.
   - If $\mathcal{O}_K \neq \mathbb{Z}[\zeta_{p^d}]$, then by scaling the expression above by an appropriate power of p, we may suppose there is an element in $\mathcal{O}_K$ of the form $\alpha = \dfrac{c_0 + c_1(1-\zeta) + \cdots + c_{\varphi(p^d)}(1-\zeta)^{\varphi(p^d)}}{p}$ where not all of the c_i are divisible by p.
   - As calculated in (1) we have $N(1-\zeta_{p^d}) = p$, which explicitly says $(1-\zeta)\cdots(1-\zeta^{p^d-1}) = p$. Since each of the $\varphi(p^d)$ terms on the left-hand side is divisible by $1-\zeta$ in $\mathbb{Z}[\zeta]$, we see that $(1-\zeta)^{\varphi(p^d)}$ divides p in $\mathbb{Z}[\zeta]$.
   - Thus, we see $p/(1-\zeta)^{\varphi(p^d)}$ is an algebraic integer, hence for each $1 \leq i \leq \varphi(p^d)$ so is $\dfrac{p\beta}{(1-\zeta)^i} = c_0(1-\zeta)^{-i} + c_1(1-\zeta)^{1-i} + \cdots + c_i + c_{i+1}(1-\zeta) + \cdots + c_{\varphi(p^d)}(1-\zeta)^{\varphi(p^d)-i}$. Since the terms from c_i onward are clearly algebraic integers, subtracting them yields that $c_0(1-\zeta)^{-i} + c_1(1-\zeta)^{1-i} + \cdots + c_{i-1}(1-\zeta)^{-1}$ is an algebraic integer for each i, and then by an easy induction, this implies $c_{i-1}/(1-\zeta)$ is an algebraic integer for each $1 \leq i \leq \varphi(p^d)$.
   - But now taking norms yields that $N(1-\zeta) = p$ divides $N(c_{i-1}) = c_{i-1}^{\varphi(p^d)}$, hence each c_{i-1} is divisible by p. This is a contradiction, and so we must in fact have $\mathcal{O}_K \neq \mathbb{Z}[\zeta_{p^d}]$.
   - Exercise: For a prime p, show that $p = u(1-\zeta_{p^d})^{\varphi(p^d)}$ where u is a unit in $\mathbb{Z}[\zeta_{p^d}]$.

5. Suppose K and L are number fields such that $\text{disc}(K)$ and $\text{disc}(L)$ are relatively prime and such that $[KL:\mathbb{Q}] = [K:\mathbb{Q}][L:\mathbb{Q}]$. Then $\mathcal{O}_{KL} = \mathcal{O}_K \cdot \mathcal{O}_L$.
   - Proof: Suppose $\mathcal{O}_K$ has an integral basis $\alpha_1, \ldots, \alpha_n$ and $\mathcal{O}_L$ has an integral basis $\beta_1, \ldots, \beta_m$, where we note $[K:\mathbb{Q}] = n$ and $[L:\mathbb{Q}] = m$.
   - Then since $[KL:K] = [L:\mathbb{Q}]$ the set $\alpha_1, \ldots, \alpha_n$ is a basis for the field extension KL/K, and so the set of mn pairwise products $\alpha_1\beta_1, \ldots, \alpha_n\beta_m$ is a basis for the extension $KL/\mathbb{Q}$, so in particular, it is linearly independent.
   - Since each product $\alpha_i\beta_j$ is an algebraic integer and there are $mn = [KL:\mathbb{Q}]$ of them in total, we see that these products generate an order in the ring of integers $\mathcal{O}_{KL}$: we now show this order equals the full ring of integers $\mathcal{O}_{KL}$.
   - So let $\gamma \in \mathcal{O}_{KL}$: since the $\alpha_i\beta_j$ are a $\mathbb{Q}$-basis for KL, taking out common denominators allows us to write $\gamma = \sum_{i=1}^n \sum_{j=1}^n \dfrac{c_{i,j}}{d}\alpha_i\beta_j$ for some integers $c_{i,j}$ and some positive integer d, where $\gcd(d, c_{1,1}, \ldots, c_{n,m}) = 1$.
   - It suffices to show that d divides $\text{disc}(K)$, since then by symmetry it also divides $\text{disc}(L)$ hence must be 1 since $\text{disc}(K)$ and $\text{disc}(L)$ are relatively prime.
   - Let σ be any complex embedding of K. Since $[KL:K] = [L:\mathbb{Q}]$ there are exactly $[L:\mathbb{Q}]$ complex embeddings of KL that extend σ: say they are $\tau_1, \ldots, \tau_m$. If $\tau_i|_L = \tau_j|_L$ then $\tau_i^{-1}\tau_j$ would fix both K and L hence all of KL, hence must be the identity. Thus, the restrictions of the τ_i to L are all distinct, but since there are only $[L:\mathbb{Q}] = m$ possible embeddings, all m complex embeddings of L must occur exactly once.
   - So now consider the complex embedding of KL that restricts to σ on K and to the identity on L, which (by mild abuse of terminology) we also call σ.
   - Then $\sigma(\alpha) = \sum_{i=1}^n \sum_{j=1}^n \dfrac{c_{i,j}}{d}\sigma(\alpha_i)\beta_j = \sum_{i=1}^n \sigma(\alpha_i)x_i$ where $x_i = \sum_{j=1}^m \dfrac{c_{i,j}}{d}\beta_j$. Running over all of the complex embeddings of K yields n linear equations in the n variables $x_1, \ldots, x_n$.

- Solving the system using Cramer's rule yields $x_i = \dfrac{\det(M_i)}{\det(M)} = \dfrac{\det(M_i)\det(M)}{\operatorname{disc}(K)}$ where M is the $n \times n$ matrix with (i,k)-entry equal to $\sigma_k(\alpha_i)$ and M_i is the matrix obtained by replacing the ith column of M with $[\sigma_1(\alpha), \ldots, \sigma_n(\alpha)]^T$.
- Then $\operatorname{disc}(K)x_i = \sum_{j=1}^{m} \dfrac{c_{i,j}\operatorname{disc}(K)}{d}\beta_j$ is an algebraic integer for each i, but since the β_j are an integeral basis for $\mathcal{O}_L$, each of the coefficients $\dfrac{c_{i,j}\operatorname{disc}(K)}{d}$ must be an integer. But now since $\gcd(d, c_{1,1}, \ldots, c_{n,m}) = 1$, this implies d divides $\operatorname{disc}(K)$, as desired.

6. For any positive integer n, the ring of integers of $\mathbb{Q}(\zeta_n)$ is $\mathbb{Z}[\zeta_n]$.
   - Proof: By (4) we already know this result holds when n is a prime power.
   - Now suppose $n = p_1^{a_1} \cdots p_d^{a_d}$ for distinct primes p_i; we wish to apply (5) recursively.
   - Observe that $\mathbb{Q}(\zeta_n)$ is the compositum of the fields $\mathbb{Q}(\zeta_{p_i^{a_i}})$ for $1 \leq i \leq d$, and since $\varphi(n) = \varphi(p_1^{a_1}) \cdots \varphi(p_d^{a_d})$ the degree requirement from (5) is satisfied.
   - Additionally, from (3) we know that the discriminant of $\mathbb{Q}(\zeta_{p_i^{a_i}})$ is a power of p_i, so the discriminants of the fields are all pairwise relatively prime. Thus the discriminant requirement from (5) is also satisfied for each composition of fields.
   - We conclude that the ring of integers of $\mathbb{Q}(\zeta_n)$ is the product $\mathbb{Z}[\zeta_{p_1^{a_1}}] \cdots \mathbb{Z}[\zeta_{p_d^{a_d}}] = \mathbb{Z}[\zeta_n]$, as desired.
   - Exercise: If D and E are relatively prime squarefree integers congruent to 1 modulo 4, show that the ring of integers of $\mathbb{Q}(\sqrt{D}, \sqrt{E})$ is $\mathbb{Z}[\dfrac{1+\sqrt{D}}{2}, \dfrac{1+\sqrt{E}}{2}]$, and compute an integral basis for it.

Well, you're at the end of my handout. Hope it was helpful.