Contents

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.
  - 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.

[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 $\mathbb{Z}[x]$.

- $(d) \Rightarrow (a)$: 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 $\tilde{m}(x) = x^n + c_n dx^{n-1} + \cdots + c_1 d^{n-1}x + c_0 d^n$ 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 $\sigma_1, \dots \sigma_n$ 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 $p + q\sqrt{2} + ri + si\sqrt{2}$.

[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 $\varphi(n)$.

- 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 $1 \leq i \leq n$. 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 $\{\sigma_i\tau_j\}_{1 \leq i \leq n, 1 \leq j \leq m}$ 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.
  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 $1 \leq i \leq n$, 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.
  - 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 $\alpha_1, \ldots, \alpha_n$ 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 $\beta \in K$.

[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 $\left|p^2 - Dq^2\right| < 2\sqrt{D} + 1$. 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 $b > 0$.

- Consider the elements $\alpha_1', \ldots, \alpha_n' \in K$ giving the dual basis to $\alpha_1, \ldots, \alpha_n$: 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 $\alpha_1, \ldots, \alpha_n$ to zero except for α_i which is mapped to 1, is of the form $\varphi_{\alpha_i'}$ for some α_i'.)
- Since $\alpha_1', \ldots \alpha_n'$ are then clearly linearly independent, they are a $\mathbb{Q}$-basis for K.
- Now suppose β is some element of $\mathcal{O}_K$: since $\{\alpha_1', \ldots \alpha_n'\}$ 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 $\{1, \alpha, \ldots, \alpha^{n-1}\}$ 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 $\beta_1, \ldots, \beta_{n+1}$ 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 $\beta_1, \beta_2, \ldots, \beta_n \in \mathcal{O}_K$ 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 $\sigma_1, \ldots, \sigma_n : K \to \mathbb{C}$ be the complex embeddings of K fixing F. For an ordered n-tuple $(\alpha_1, \ldots, \alpha_n) \in K$, we define the discriminant

$\text{disc}_{K/F}(\alpha_1,\ldots,\alpha_n)$ of the tuple $(\alpha_1,\ldots,\alpha_n)$ to be $\text{disc}_{K/F}(\alpha_1,\ldots,\alpha_n) = \begin{vmatrix} \sigma_1(\alpha_i) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{vmatrix}^2$, 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 $\text{disc}_{K/\mathbb{Q}}(1,\sqrt{2}) = \begin{vmatrix} 1 & \sqrt{2} \\ 1 & -\sqrt{2} \end{vmatrix}^2 = 8$ and $\text{disc}_{K/\mathbb{Q}}(1+2\sqrt{2},3) = \begin{vmatrix} 1+2\sqrt{2} & 3 \\ 1-2\sqrt{2} & 3 \end{vmatrix}^2 = 288.$
- Example: For $K = \mathbb{Q}(\sqrt[3]{2})$ we have $\text{disc}_{K/\mathbb{Q}}(1,\sqrt[3]{2},\sqrt[3]{4}) = \begin{vmatrix} 1 & \sqrt[3]{2} & \sqrt[3]{4} \\ 1 & \zeta_3\sqrt[3]{2} & \zeta_3^2\sqrt[3]{4} \\ 1 & \zeta_3^2\sqrt[3]{2} & \zeta_3\sqrt[3]{4} \end{vmatrix}^2 = -108.$

- Here are some basic properties of the discriminant:
- Proposition (Properties of Discriminants): Let K/F be a degree-n extension of number fields.

1. $\text{disc}_{K/F}(\alpha_1,\ldots,\alpha_n)$ is equal to the determinant of the $n \times n$ matrix whose (i,j)-entry is $\text{tr}_{K/F}(\alpha_i\alpha_j)$. In particular, $\text{disc}_{K/F}(\alpha_1,\ldots,\alpha_n) \in F$.
   - Proof: Let M be the matrix whose (i,j)-entry is $\sigma_i(\alpha_j)$, so that $\text{disc}_{K/F}(\alpha_1,\ldots,\alpha_n) = \det(M)^2$.
   - Then the (i,j)-entry of the product M^TM is $\sum_{k=1}^n \sigma_k(\alpha_i)\sigma_k(\alpha_j) = \sum_{k=1}^n \sigma_k(\alpha_i\alpha_j) = \text{tr}_{K/F}(\alpha_i\alpha_j)$. 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 $\alpha_1,\ldots,\alpha_n \in \mathcal{O}_K$, then $\text{disc}_{K/F}(\alpha_1,\ldots,\alpha_n) \in \mathcal{O}_F$. In particular, $\text{disc}_{K/\mathbb{Q}}(\alpha_1,\ldots,\alpha_n)$ is always an integer.
   - Proof: From (1) we see that $\text{disc}_{K/F}(\alpha_1,\ldots,\alpha_n) \in F$. 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 $\text{disc}_{K/F}(\alpha_1,\ldots,\alpha_n) = 0$ 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 $\text{disc}_{K/F}(\alpha_1,\ldots,\alpha_n) = 0$: then the rows of the matrix $\{\text{tr}_{K/F}(\alpha_i\alpha_j)\}_{1\le i,j\le n}$ are F-linearly dependent, so there exist some $c_i \in F$, not all zero, with $c_1\text{tr}_{K/F}(\alpha_1\alpha_j) + \cdots + c_n\text{tr}_{K/F}(\alpha_n\alpha_j) = 0$ 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 $\text{tr}_{K/F}(\beta\alpha_j) = 0$ for each $1 \le j \le n$. However, this implies $\beta = 0$, since as we noted earlier, the linear map $\varphi_\beta : K \to F$ given by $\varphi_\beta(\alpha) = \text{Tr}_{K/F}(\beta\alpha)$ is nonzero for $\beta \ne 0$.
   - 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 $\alpha_1,\ldots,\alpha_n \in \mathcal{O}_K$ and $\text{disc}_{K/F}(\alpha_1,\ldots,\alpha_n) \ne 0$, 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 $\text{disc}_{K/F}(\alpha_1,\ldots,\alpha_n) \ne 0$ 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, $\mathrm{disc}_{K/\mathbb{Q}}(\beta_1, \ldots, \beta_n) = \det[\{\sigma_i(\beta_j)\}_{1 \le i,j \le n}]^2 = \det[A\{\sigma_i(\alpha_j)\}_{1 \le i,j \le n}]^2 = \det(A)^2 \mathrm{disc}_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)$, 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 $\mathrm{disc}(K) = \mathrm{disc}(1, \frac{1+\sqrt{D}}{2}) = \begin{vmatrix} 1 & (1+\sqrt{D})/2 \\ 1 & (1-\sqrt{D})/2 \end{vmatrix}^2 = D$.
- 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 $e_i = \dfrac{\det(M_i)}{\det(M)}$ 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 $e_i = \dfrac{\det(M)\det(M_i)}{d}$ 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 $\text{disc}_{K/\mathbb{Q}}(S) = \begin{vmatrix} \sigma_1(d_1\beta_1) & \cdots & \sigma_1(d_n\beta_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(d_1\beta_1) & \cdots & \sigma_n(d_n\beta_n) \end{vmatrix}^2 = (d_1 d_2 \cdots d_n)^2 \begin{vmatrix} \sigma_1(\beta_1) & \cdots & \sigma_1(\beta_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\beta_1) & \cdots & \sigma_n(\beta_n) \end{vmatrix}^2 =$ $[\mathcal{O}_K : S]^2 \text{disc}_{K/\mathbb{Q}}(\mathcal{O}_K)$, 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 $\mathrm{disc}_{K/\mathbb{Q}}(S) = (-1)^{n(n-1)/2} \prod_{i=1}^n \prod_{j \ne i} (\alpha_i - \alpha_j)$.
   - Factoring $m(x) = (x - \alpha_i) q_i(x)$ where $q_i(x) = \prod_{j \ne i} (x - \alpha_j)$, now differentiate to see $m'(x) = q_i(x) + (x - \alpha_i) q_i'(x)$: thus setting $x = \alpha_i$ yields $m'(\alpha_i) = q_i(\alpha_i) = \prod_{j \ne i} (\alpha_i - \alpha_j)$.
   - Therefore we see $\prod_{i=1}^n \prod_{j \ne i} (\alpha_i - \alpha_j) = \prod_{i=1}^n m'(\alpha_i) = N_{K/\mathbb{Q}}[m'(\alpha)]$, 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 $0 \leq k \leq n-1$, 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 $1 = d_0|d_1|d_2|\cdots|d_{n-1}|d = \text{disc}(K)$. 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 $\beta \in \text{span}_{\mathbb{Q}}(1, \alpha, \ldots, \alpha^k)$ 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 $d_k R_k \subseteq \mathbb{Z}[\alpha]$. 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 $d_k R_k \subseteq \mathbb{Z}[\alpha]$.
     - 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 $d_k R_k \subseteq \mathbb{Z}[\alpha]$.
  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 $\gamma = \frac{f_i(\alpha)}{d_i} \cdot \frac{f_j(\alpha)}{d_j}$ 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 $\frac{f_0(\alpha)}{d_0}, \ldots, \frac{f_{i+j}(\alpha)}{d_{i+j}}$; comparing coefficients of α^{i+j} then shows that $\frac{1}{d_i d_j}$ must be an integer multiple of $\frac{1}{d_{i+j}}$, 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 $\text{disc}(\alpha) = -23$.
  - 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 $\text{disc}(\alpha)$, 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 $\text{tr}(\beta) = c_0/2$ 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 $\beta = \dfrac{e_0 + e_1\alpha + e_2\alpha^2}{3}$ for some integers e_0, e_1, e_2.
  - Squaring yields $\beta^2 = \dfrac{(e_0^2 + 2e_1e_2) + (2e_0e_1 + 2e_2^2)\alpha + (e_1^2 + 2e_0e_2)\alpha^2}{9}$. In order for this quantity to be an algebraic integer, each of $e_0^2 + 2e_1e_2$, $e_0e_1 + e_2^2$, and $e_1^2 + 2e_0e_2$ must be divisible by 3 (this follows because $d_2 | 3$, so we cannot have denominators of 9). If any of e_0, e_1, e_2 is zero mod 3, all of them must be zero mod 3; otherwise, in the event all are nonzero, we see $e_0^2 \equiv e_1^2 \equiv e_2^2 \equiv 1 \pmod 3$, whence $e_1e_2 \equiv e_0e_2 \equiv -e_0e_1 \equiv 1 \pmod 3$. But this is a contradiction since the first two equalities require $e_0 \equiv e_1 \equiv e_2 \bmod 3$, which contradicts the third condition.
  - Therefore, all of e_0, e_1, e_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 $d_2|15$. Eliminate the possibility that d_2 is divisible by 5, then show that $d_2 = 3$ leads to an eventual contradiction modulo 3.]
- Exercise: Show that the ring of integers of $\mathbb{Q}(\sqrt[3]{10})$ has integral basis $\{1, \sqrt[3]{10}, \frac{1+\sqrt[3]{10}+\sqrt[3]{100}}{3}\}$. [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 $K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$ has integral basis $\{1, \sqrt{2}, \frac{1+\sqrt{5}}{2}, \frac{\sqrt{2}+\sqrt{10}}{2}\}$.
  - 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 $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$, $\mathbb{Z}[\sqrt{10}]$.
  - 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 $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$, 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 $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$, 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 $\alpha = \dfrac{p + q\sqrt{5} + r\sqrt{13} + s\sqrt{65}}{4}$ for integers p, q, r, s all of the same parity. By subtracting $\dfrac{(1+\sqrt{5})(1+\sqrt{65})}{4} = \dfrac{1 + \sqrt{5} + 5\sqrt{13} + \sqrt{65}}{4}$ if all of p, q, r, s are odd, we can make all of p, q, r, s even, in which case $\alpha = \dfrac{p' + q'\sqrt{5} + r'\sqrt{13} + s'\sqrt{65}}{2} + x\dfrac{(1+\sqrt{5})(1+\sqrt{65})}{4}$ for $x = 0$ or 1.
- Then $\alpha - q'\dfrac{1+\sqrt{5}}{2} - r'\dfrac{1+\sqrt{13}}{2} - s'\dfrac{1+\sqrt{65}}{2} = \dfrac{p' - q' - r' - s'}{2}$ must be an (actual) integer u, meaning that $\alpha = u + q'\dfrac{1+\sqrt{5}}{2} + r'\dfrac{1+\sqrt{13}}{2} + s'\dfrac{1+\sqrt{65}}{2} + x\dfrac{(1+\sqrt{5})(1+\sqrt{13})}{4}$ for integers u, q', r', s', x.
- Finally we note that $\dfrac{1+\sqrt{65}}{2} = 3 + 2\dfrac{(1+\sqrt{5})(1+\sqrt{65})}{4} - \dfrac{1+\sqrt{5}}{2} - 5\dfrac{1+\sqrt{13}}{2}$, so the extra element $\dfrac{1+\sqrt{65}}{2}$ can be written in terms of the other four.
- We conclude that $\{1, \dfrac{1+\sqrt{5}}{2}, \dfrac{1+\sqrt{13}}{2}, \dfrac{(1+\sqrt{5})(1+\sqrt{13})}{4}\}$ 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 $\{1, \sqrt{3}, \dfrac{\sqrt{3}+\sqrt{7}}{2}, \dfrac{1+\sqrt{21}}{2}\}$.
- 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 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 (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 $\mathrm{disc}(S) = (-1)^{n(n-1)/2} N[\Phi_n'(\zeta_n)]$.
  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 $\mathrm{disc}(1 - \zeta)$ 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 $\mathrm{disc}(K)$ and $\mathrm{disc}(L)$ 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 $\mathrm{disc}(K)$, since then by symmetry it also divides $\mathrm{disc}(L)$ hence must be 1 since $\mathrm{disc}(K)$ and $\mathrm{disc}(L)$ 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 $x_i = \dfrac{\det(M_i)}{\det(M)} = \dfrac{\det(M_i)\det(M)}{\mathrm{disc}(K)}$ 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 $\mathrm{disc}(K)x_i = \sum_{j=1}^m \dfrac{c_{i,j}\mathrm{disc}(K)}{d}\beta_j$ is an algebraic integer for each i, but since the β_j are an integral basis for $\mathcal{O}_L$, each of the coefficients $\dfrac{c_{i,j}\mathrm{disc}(K)}{d}$ must be an integer. But now since $\gcd(d, c_{1,1}, \ldots, c_{n,m}) = 1$, this implies d divides $\mathrm{disc}(K)$, as desired.
   - Remark: In the situation where $\Delta_K = \mathrm{disc}(K)$ and $\Delta_L = \mathrm{disc}(L)$ are not relatively prime, we do still obtain the weaker statement that $\mathcal{O}_K\mathcal{O}_L \subseteq \mathcal{O}_{KL} \subseteq \dfrac{1}{\gcd(\Delta_K, \Delta_L)}\mathcal{O}_K\mathcal{O}_L$.

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 $\mathbb{Z}[\frac{1+\sqrt{D}}{2}, \frac{1+\sqrt{E}}{2}]$, and compute an integral basis for it.

0.9 (Sep 23) Student Presentations of HW1 Problems

0.10 (Sep 25) Unique Factorization in $\mathcal{O}_K$

- Now that we have a moderately good idea of the additive structure of $\mathcal{O}_K$, we turn our attention now to the multiplicative structure of $\mathcal{O}_K$. A natural starting point is the question of when $\mathcal{O}_K$ has unique factorization of elements (more precisely, when $\mathcal{O}_K$ is a unique factorization domain).
  - We first observe that in $\mathcal{O}_K$, every nonzero nonunit can be written as a finite product of irreducible elements; this follows by an easy induction on the norm of the element (and indeed this essentially the same argument establishing existence of prime factorizations in $\mathbb{Z}$ itself).
  - Thus, the only manner in which $\mathcal{O}_K$ can fail to have unique factorization is if some elements have multiple inequivalent factorizations.
- In some situations, the ring $\mathcal{O}_K$ is a principal ideal domain and even Euclidean, such as for the field $K = \mathbb{Q}(i)$, with ring of integers the familiar Gaussian integers $\mathbb{Z}[i]$.
  - Explicitly, recall that in $\mathbb{Z}[i]$ we may obtain the quotient of $\alpha \in \mathbb{Z}[i]$ by a nonzero $\beta \in \mathbb{Z}[i]$ by computing $\alpha/\beta \in \mathbb{C}$ and then "rounding" to the nearest Gaussian integer q (simply round the real and imaginary parts of α/β to the nearest integer); the remainder is then the "leftover" $r = \alpha - q\beta$, and one then readily verifies that $N(r) \leq N(\beta)/2$.
  - A similar procedure can be used to show that $\mathcal{O}_{\sqrt{D}}$ is Euclidean for $D = -2, 2, 3$, and by instead rounding to the nearest element of $\mathcal{O}_{\sqrt{D}}$, the method can be adapted to show $\mathcal{O}_{\sqrt{D}}$ is Euclidean for $D = -3, -7, -11$ as well.
- In other situations, the ring $\mathcal{O}_K$ can fail to have unique factorization.
  - As we have already mentioned, $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$ is not a unique factorization domain:
  - Example: In $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})} = \mathbb{Z}[\sqrt{-5}]$, observe that we can write $6 = (1+\sqrt{-5})(1-\sqrt{-5}) = 2 \cdot 3$. Each of $1 \pm \sqrt{-5}$, 2, and 3 is irreducible in $\mathbb{Z}[\sqrt{-5}]$ since their norms are 6, 4, and 9 respectively and there are no elements in $\mathbb{Z}[\sqrt{-5}]$ of norm 2 or 3, and none of these elements are associate to one another. We therefore have two inequivalent irreducible factorizations of 6 in $\mathbb{Z}[\sqrt{-5}]$.
  - Indeed, many of the imaginary quadratic fields lack unique factorization:
  - Exercise: If $D > 4$ is squarefree and $-D \equiv 2, 3 \pmod 4$, show that $\mathcal{O}_{\sqrt{-D}} = \mathbb{Z}[\sqrt{-D}]$ is not a unique factorization domain. [Hint: If D is odd, use $2 \cdot (1+D)/2 = (1+\sqrt{-D})(1-\sqrt{-D})$, and if D is even use $2 \cdot (D/2) = \sqrt{-D} \cdot (-\sqrt{-D})$.]
  - The situation for real quadratic fields is more complicated, since the argument in the exercise above does not generally yield non-unique factorizations due to the presence of more elements of small norm.
  - Example: In $\mathbb{Z}[\sqrt{7}]$, we seemingly have a non-unique factorization $6 = (1+\sqrt{7})(-1+\sqrt{7}) = 2 \cdot 3$, but in fact none of $1 \pm \sqrt{7}$, 2, and 3 are irreducible: we have $2 = (3+\sqrt{7})(3-\sqrt{7})$, $1 \pm \sqrt{7} = (3 \pm \sqrt{7})(-2 \pm \sqrt{7})$, and $3 = (2+\sqrt{7})(-2+\sqrt{7})$, and so we can see that our factorizations of 6 both reduce to different arrangements of $6 = (3+\sqrt{7})(3-\sqrt{7})(2+\sqrt{7})(-2+\sqrt{7})$.
  - We can still find examples of non-unique factorizations in real quadratic fields, however.
  - Example: In $\mathbb{Z}[\sqrt{10}]$ we have $2 \cdot 3 = 6 = (2+\sqrt{10})(2-\sqrt{10})$, and in fact 2, 3, and $2 \pm \sqrt{10}$ are all irreducible since there are no elements in $\mathbb{Z}[\sqrt{10}]$ of norm ± 2 or ± 3 (as can be seen by reducing $a^2 - 10b^2 = \pm 2, \pm 3$ modulo 5).
  - The presence of additional units in real quadratic fields also adds some additional complications.

- Example: In $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$, we can observe that $4 = 2 \cdot 2 = (1+\sqrt{5})(-1+\sqrt{5})$ and that both 2 and $\pm 1 + \sqrt{5}$ are irreducible (as there are no elements of norm ± 2, similarly to in $\mathbb{Z}[\sqrt{10}]$). But in fact these factorizations are equivalent, since $1 + \sqrt{5} = 2 \cdot \dfrac{1+\sqrt{5}}{2}$ and $\dfrac{1+\sqrt{5}}{2} \in \mathcal{O}_{\sqrt{5}}$ is a unit (its norm is -1).

- Analyzing factorizations of higher-degree rings of integers is, if anything, even more difficult, since the norm functions even in the case of cubic fields are substantially more complicated.
  - For instance, in the ring of integers $\mathbb{Z}[\sqrt[3]{2}]$ of $\mathbb{Q}(\sqrt[3]{2})$, the norm is $N(a+b\sqrt[3]{2}+c\sqrt[3]{4}) = a^3+2b^3+4c^3-6abc$. We can certainly use the norm to identify some irreducible elements: for instance, $\sqrt[3]{2}$ and $1 + \sqrt[3]{2}$ are both irreducible since their norms are 2 and 3 respectively.
  - But it is much harder to try to decide (for instance) whether the elements 5 and 7 of respective norms 5^3 and 7^3 are irreducible. In fact, 5 is reducible (it factors as $5 = (1 + \sqrt[3]{4})(1 + 2 \cdot \sqrt[3]{2} - \sqrt[3]{4})$) but as it turns out, 7 is irreducible (though this is not so easy to prove!).

0.11 (Sep 26) Dedekind Domains

- It would appear that we are essentially at an impasse regarding factorization of elements. However, shifting our focus instead to ideals, we will be able to show that $\mathcal{O}_K$ does always possess unique prime factorization on the level of *ideals*, rather than elements.
  - In fact, this is where the name "ideal" originally arose: in Kummer's study of unique factorization, he constructed "ideal numbers" (essentially as sets of linear combinations of elements of $\mathcal{O}_K$) and proved that they did possess unique prime factorization. These "ideal numbers" were the prototype of the modern definition of an ideal.
  - To illustrate using an example from above, the element $6 \in \mathbb{Z}[\sqrt{-5}]$ has two different factorizations into irreducibles, which we can recast using ideals: $(6) = (2) \cdot (3) = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$.
  - However, as ideals, we can factor further: explicitly, one can verify that $(2) = (2, 1 + \sqrt{-5})^2$, that $(1 \pm \sqrt{-5}) = (2, 1 + \sqrt{-5}) \cdot (3, 1 \pm \sqrt{-5})$, and that $(3) = (3, 1 + \sqrt{-5}) \cdot (3, 1 - \sqrt{-5})$.
  - For an example of one of these calculations: we have $(2, 1 + \sqrt{-5}) \cdot (3, 1 + \sqrt{-5}) = (6, 2 + 2\sqrt{-5}, 3 + 3\sqrt{-5}, -4 + 2\sqrt{-5})$. We can reduce the generating set by observing that this ideal contains $(3+3\sqrt{-5}) - (2+2\sqrt{-5}) = 1+\sqrt{-5}$, and that each of the four generators of the product ideal is a multiple of $1+\sqrt{-5}$: thus, in fact, $(2, 1 + \sqrt{-5}) \cdot (3, 1 + \sqrt{-5}) = (1 + \sqrt{-5})$, as claimed. (The other calculations are similar.)
  - On the level of ideals, therefore, we see that these two factorizations are really "the same": both of them reduce to the factorization $(6) = (2, 1 + \sqrt{-5})^2 \cdot (3, 1 + \sqrt{-5}) \cdot (3, 1 - \sqrt{-5})$.
  - Furthermore, each of the ideals $(2, 1 + \sqrt{-5})$, $(3, 1 + \sqrt{-5})$, and $(3, 1 - \sqrt{-5})$ is prime (the quotient ring of $\mathbb{Z}[\sqrt{-5}]$ by each is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, and $\mathbb{Z}/3\mathbb{Z}$ respectively).

- Our goal is to show that the behavior in the example above holds in general: namely, that we can write any nonzero ideal in $\mathcal{O}_K$ as a product of prime ideals, and that this factorization is unique up to rearrangement.
  - For no additional cost, however, we can show the same results in the broader class of rings known as Dedekind domains (which were, historically, analyzed by Dedekind for precisely these reasons of understanding the class of rings possessing unique ideal factorization).
  - To motivate the definition of a Dedekind domain, we make some basic observations about the rings $\mathcal{O}_K$.

- Proposition (Ring Properties of $\mathcal{O}_K$): Let K be a number field of degree n over $\mathbb{Q}$ with ring of integers $\mathcal{O}_K$.

  1. Every ideal of $\mathcal{O}_K$ is finitely generated, which is to say, $\mathcal{O}_K$ is Noetherian.
     - Proof: We already showed this result earlier in our discussion of the additive structure of $\mathcal{O}_K$: any ideal is an additive subgroup of the free rank-n abelian group $\mathcal{O}_K$ hence is finitely generated as a group (thus also certainly as an ideal).
     - Exercise: If R is an integral domain, show that the following are equivalent:

       (a) Every ideal of R is finitely generated.

(b) Every ascending chain $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$ of ideals of R is eventually constant (i.e., there exists N such that $I_n = I_N$ for all $n \geq N$).

(c) Every nonempty collection S of ideals of R contains a maximal element (i.e., an ideal I such that if $J \in S$ has $I \subseteq J$ then $J = I$).

2. $\mathcal{O}_K$ has Krull dimension 1, which is to say, every nonzero prime ideal of $\mathcal{O}_K$ is maximal.
   - Recall that the Krull dimension of a ring is the maximum length of a chain of prime ideals, so saying that the Krull dimension is 1 is equivalent to saying that nonzero prime ideals are maximal and that the ring is not a field.
   - Exercise: Show that a finite integral domain is a field.
   - Proof 1: We show that if I is a nonzero ideal of $\mathcal{O}_K$, then $\mathcal{O}_K/I$ is finite.
   - Let $\alpha \in I$ be nonzero and let $m = N_{K/\mathbb{Q}}(\alpha)$; note m is a nonzero integer. Then m/α is an algebraic integer (being a product of Galois conjugates of α with one α excluded) and is in K, hence it is some $\beta \in \mathcal{O}_K$. Then $m = \alpha\beta \in I$.
   - Then since I is an ideal we have $m\mathcal{O}_K \subseteq I$, and so choosing an integral basis $\beta_1, \ldots, \beta_n$ for $\mathcal{O}_K$ we see that I contains the order $m\mathcal{O}_K$ with basis $m\beta_1, \ldots, m\beta_n$. Then $[\mathcal{O}_K : I]$ divides $[\mathcal{O}_K : m\mathcal{O}_K] = m^n$, which is finite, so $\mathcal{O}_K/I$ is finite (and indeed has cardinality dividing m^n).
   - To finish, if now P is a nonzero prime ideal, then $\mathcal{O}_K/P$ is a finite integral domain by the above, so by the exercise it is a field. This means P is maximal, as claimed.
   - Exercise: Suppose S is an integral ring extension of the commutative ring R with 1 (i.e., every element of S is the root of a monic polynomial in $R[x]$).
     (a) Show that if Q is a prime ideal of S, then $P = Q \cap R$ is a prime ideal of R.
     (b) Show that if S is a domain then R is a field if and only if S is a field. [Hint: Use the monic polynomial satisfied by a nonzero element to construct an inverse for it.]
     (c) Show that an ideal Q of S is maximal in S if and only if $P = Q \cap R$ is maximal in R. [Hint: Note S/Q is an integral extension of R/P.]
   - Proof 2: Essentially by definition, we see that $\mathcal{O}_K$ is an integral ring extension of $\mathbb{Z}$.
   - Then if Q is any prime ideal of $\mathcal{O}_K$, by the first part of the exercise we see that $\mathcal{O}_K \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$ which is necessarily of the form (p) for some prime p since $\mathcal{O}_K \cap \mathbb{Z}$ is nonzero.
   - But (p) is a maximal ideal of $\mathbb{Z}$, so by the third part of the exercise, that implies Q is a maximal ideal of $\mathcal{O}_K$, as desired.

3. The ring $\mathcal{O}_K$ is integrally closed in its field of fractions K.
   - We have previously noted (as an exercise) that the field of fractions of $\mathcal{O}_K$ is K. (It is quite obviously contained in K.)
   - Exercise: Suppose that R is a commutative ring with 1 and S is a ring containing R. Recall that the integral closure of R in S consists of the elements of S containing R, and R is integrally closed when its integral closure is just R itself.
     (a) Show that the integral closure of R in S is a subring of S containing R. [Hint: If s, t are integral over R, then $R[s]$ and $R[t]$ are finitely-generated R-modules, hence so is $R[s,t]$.]
     (b) Show that the integral closure of R in S is integrally closed in S. [Hint: Show that integrality is transitive.]
   - Proof 1: By definition, $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K. But by the second part of the exercise above, the integral closure is integrally closed.
   - We can also give a more explicit argument (which really is embedded in the general argument above):
   - Proof 2: Suppose α is in the integral closure of $\mathcal{O}_K$: then α is the root of some monic polynomial with coefficients in $\mathcal{O}_K$, say with $\alpha^d + \beta_{d-1}\alpha^{d-1} + \cdots + \beta_0 = 0$ for some $\beta_i \in \mathcal{O}_K$.
   - Then the ring $R = \mathbb{Z}[\beta_0, \ldots, \beta_{d-1}]$ is a finitely-generated $\mathbb{Z}$-module (since indeed it is contained in $\mathcal{O}_K$), and $\mathbb{Z}[\alpha]$ is a finitely-generated R-module (since is generated by $\{1, \alpha, \ldots, \alpha^{d-1}\}$).
   - We deduce that $\mathbb{Z}[\alpha, \beta_0, \ldots, \beta_{d-1}]$ and hence $\mathbb{Z}[\alpha]$ is therefore a finitely-generated $\mathbb{Z}$-module, and this implies α is an algebraic integer. So, α is an algebraic integer in K whence $\alpha \in \mathcal{O}_K$.

- In the proposition above, we have proved that the ring of integers $\mathcal{O}_K$ is a Noetherian, integrally closed domain in which nonzero prime ideals are maximal. We now consider this more general class of rings:

- Definition: A Dedekind domain is a Noetherian, integrally closed domain in which nonzero prime ideals are maximal.
    - Our proposition above shows that the ring of integers of a number field is a Dedekind domain.
    - Exercise: Show that principal ideal domains are Dedekind domains. [Hint: Use the general fact that UFDs are integrally closed.]
- Our goal now is to establish that in a Dedekind domain, every nonzero ideal can be written as a product of prime ideals (with the usual convention that the empty product represents the entire ring).
    - It is possible to give a more direct approach for this, but we will first develop some facts about fractional ideals, since the notion of a fractional ideal allows us to state some useful alternative characterizations of Dedekind domains.
- Definition: Let R be an integral domain with fraction field K. A fractional ideal of R is an R-submodule of K of the form $A = d^{-1}I$ for some nonzero $d \in R$ and some ideal I of R.
    - Equivalently, a fractional ideal is an R-submodule A of K such that $dA \subseteq R$ for some nonzero $d \in R$. (This definition is equivalent to the one above because dA is then an R-submodule of R, which is to say, an ideal I of R, and then $A = d^{-1}I$.)
    - Example: The fractional ideals of $\mathbb{Z}$ are the $\mathbb{Z}$-modules of the form $\frac{c}{d}\mathbb{Z}$ for integers c and d. More generally, if R is any PID, then the fractional ideals are the sets $\frac{c}{d}R$ where $c, d \in R$.
    - Any ideal of R is a fractional ideal of R, with $d = 1$. (For emphasis we can call them "integral ideals".)
    - We have a natural notion of the product IJ of two ideals I and J: namely, as the set IJ of all finite sums $r_1s_1 + \cdots + r_ks_k$ where each $r_i \in I$ and $s_i \in J$. This notion extends easily to fractional ideals by taking $(d^{-1}I)(e^{-1}J) = (de)^{-1}IJ$.
    - The ring $R = 1^{-1}R$ serves as a multiplicative identity under this product operation on fractional ideals, and since products are obviously associative and commutative, the set of fractional ideals forms a commutative semigroup under multiplication.
    - The invertible elements in this semigroup are the invertible fractional ideals: in other words, the fractional ideals A such that there exists another fractional ideal B with $AB = R$.
    - The utility of invertible fractional ideals is that they allow us to do cancellation when we have statements involving products of integral or fractional ideals, and (as such) arise very naturally in the proof of uniqueness of ideal factorizations.

0.12 (Sep 30) Ideal Factorization in Dedekind Domains

- We can establish some basic properties of fractional ideals:
- Proposition (Fractional Ideals): Let R be an integral domain with fraction field K, and let A be a fractional ideal of R.
    1. If A is invertible, then the inverse of A is unique.
        - Proof: If $AB = AC = R$, then $B = BR = B(AC) = (BA)C = (AB)C = RC = C$.
    2. For any nonzero $x \in R$, the principal fractional ideal xR is invertible with inverse $x^{-1}R$.
        - Proof: We have $(xR)(x^{-1}R) = (xx^{-1})RR = R$.
    3. If $A \neq 0$, then the set $A' = \{x \in K : xA \subseteq R\}$ is a fractional ideal of R, and $AA' \subseteq R$.
        - Proof: It is easy to see that A' is an R-submodule of K, since it contains 0 and is closed under subtraction and R-scaling.
        - Furthermore, for any nonzero $d \in A$ we see that $dA' \subseteq R$, so dA' is an R-submodule of R (i.e., an ideal I), and then $A' = d^{-1}I$, so A' is a fractional ideal.
        - Finally since $dA' \subseteq R$ for any $d \in A$ that means $AA' \subseteq R$.

4. With $A' = \{x \in K : xA \subseteq R\}$, A is invertible if and only if $AA' = R$, and in that case $A^{-1} = A'$.
   - Proof: If A is invertible with $AB = R$, then $B \subseteq A'$ by definition of A'; then $R = AB \subseteq AA' \subseteq R$ so we have equality everywhere hence $AA' = R$.
   - Conversely, if $AA' = R$ then by definition A is invertible with inverse $A^{-1} = A'$.
5. Invertible fractional ideals are finitely generated.
   - Proof: If A is invertible then by (4) we have $AA' = R$. Thus there exist some $a_1, \ldots, a_k \in A$ and $a_1', \ldots, a_k' \in A'$ with $a_1a_1' + \cdots + a_ka_k' = 1$.
   - Then for any $a \in A$ we have $a = (aa_1')a_1 + \cdots + (aa_k')a_k$ and each term $aa_i' \in R$ by definition of A'. Hence a is an R-linear combination of $a_1, \ldots, a_k$, meaning that $a_1, \ldots, a_k$ generates A.
6. The invertible fractional ideals of R form an abelian group under multiplication.
   - Proof: Obvious from the above discussion, (2), and the fact that $(AB)^{-1} = B^{-1}A^{-1}$.

- It is natural to ask: for which rings are *all* of the nonzero fractional ideals invertible? In fact, these are precisely the fields (rather trivially) and the Dedekind domains:
- Proposition (Invertible Fractional Ideals): Suppose R is an integral domain with fraction field $K \neq R$. If every nonzero fractional ideal of R is invertible, then R is a Dedekind domain.
  - Exercise: If R is a Noetherian integral domain, show that fractional ideals of R are the same as finitely-generated R-submodules of K. [Hint: Put things over a common denominator.]
  - Exercise: Suppose P is a prime ideal of an integral domain and $IJ \subseteq P$ for some ideals I and J. Show that $I \subseteq P$ or $J \subseteq P$. (Note that this property is the ideal analogue of the prime divisibility property $p|ab$ implies $p|a$ or $p|b$.)
  - Proof: Suppose that every nonzero fractional ideal of R is invertible. Then since invertible fractional ideals are finitely generated as we have already shown, in particular every integral ideal is finitely generated, so R is Noetherian.
  - To show R is integrally closed, suppose $\alpha \in K$ is integral over R. Consider the ring $R[\alpha]$: it is a finitely generated R-submodule of K because α is integral over R, so by the first exercise above, it is a fractional ideal of R, hence invertible by hypothesis.
  - But now observe that $R[\alpha]^2 = R[\alpha]$ because $R[\alpha]$ is a ring. Since $R[\alpha]$ is invertible, multiplying by its inverse then yields immediately that $R[\alpha] = R$, whence $\alpha \in R$ and so R is integrally closed.
  - Finally, suppose P is a nonzero prime ideal, and consider a maximal ideal M containing P.
  - Then by hypothesis M is invertible, in which case we see that $PM^{-1} \subseteq MM^{-1} = R$. Therefore PM^{-1} is some ideal of R, say I, and multiplying by M yields $P = MI$.
  - Then by the second exercise above, we see that $I \subseteq P$ or $M \subseteq P$. If $I \subseteq P$ multiply $PM^{-1} \subseteq P$ by P^{-1} to see $M^{-1} \subseteq R$ whence $R \subseteq RM = M$, which is impossible because M is maximal (hence not equal to R). We must therefore have $M \subseteq P$, and so $P = M$ is maximal.

- Our goal now is to analyze the factorization of ideals in Dedekind domains with the ultimate goal of showing that every nonzero ideal can be written uniquely as a product of prime ideals.
- Theorem (Ideal Factorizations): Let R be a Dedekind domain with fraction field $K \neq R$.
  1. If I is any nonzero proper ideal of R, then there exist prime ideals $P_1, \ldots, P_k$ of R such that $P_1 \cdots P_k \subseteq I \subseteq P_1 \cap \cdots \cap P_k$.
     - Proof: Suppose otherwise and let $\mathcal{F}$ be the set of all nonzero proper ideals of R that cannot be so written.
     - Then since R is Noetherian, $\mathcal{F}$ contains some maximal element I. Clearly I cannot be prime since otherwise we could take $I \subseteq I \subseteq I$.
     - Since I is not prime, there exist some $r, s \in R$ such that $rs \in I$ but $r, s \notin I$.
     - Now let $I_r = I + (r)$ and $I_s = I + (s)$, and observe that $I_rI_s = I + (rs) = I$ and $I \subseteq I_r \cap I_s$, so $I_rI_s \subseteq I \subseteq I_r \cap I_s$.

- Furthermore, I_r and I_s are clearly nonzero, and they are proper since if one of them were equal to R then their product would simply be the other, but neither I_r nor I_s is contained in I by the assumption that $r, s \notin I$.
- Therefore, I_r and I_s are nonzero proper ideals of R properly containing I so they are not in $\mathcal{F}$: therefore, there exist prime ideals $P_1, \ldots, P_k$ and $Q_1, \ldots, Q_l$ with $P_1 \cdots P_k \subseteq I_r \subseteq P_1 \cap \cdots \cap P_k$ and $Q_1 \cdots Q_l \subseteq I_s \subseteq Q_1 \cap \cdots \cap Q_s$.
- But then $P_1 \cdots P_k Q_1 \cdots Q_l \subseteq I \subseteq P_1 \cap \cdots \cap P_k \cap Q_1 \cap \cdots \cap Q_s$, so in fact I does have the desired property, contradiction. So all ideals have the claimed property.

2. Every nonzero prime ideal of R is invertible (as a fractional ideal).
   - Proof: Let P be a nonzero prime ideal of R. For any nonzero $a \in P$, by (1) there exist prime ideals $P_1, \ldots, P_k$ of R such that $P_1 \cdots P_k \subseteq aR$.
   - Observe that because $a \in P$ and P is prime, at least one of the P_i must contain P, but since nonzero primes are maximal, that means P_i equals P; without loss of generality take $P_1 = P$.
   - Now choose a in such a way that k is minimal. If $k = 1$ then we have $P \subseteq aR$ so since P is maximal and aR is proper we have $P = aR$ and thus P is invertible with inverse $a^{-1}R$ (as we have previously noted, principal ideals are invertible).
   - Now assume $k \geq 2$. We have $P(P_2 \cdots P_k) \subseteq aR$ and by minimality the product $P_2 \cdots P_k$ is not contained in aR, so let $b \in P_2 \cdots P_k \backslash aR$. Then $b \notin aR$ so that $ba^{-1} \notin R$.
   - Also, $Pb \subseteq PP_2 \cdots P_k \subseteq aR$ whence $(ba^{-1})P \subseteq R$. Recalling our definition $P' = \{x \in K : xP \subseteq R\}$, we therefore have $ba^{-1} \in P'$. Since $ba^{-1} \notin R$ and clearly R is contained in P' (since $RP = P$) this means P' is strictly larger than R.
   - But now consider PP': it is an ideal of R that contains P (since $1 \in P'$), so it is either P or R. If it were P, then $PP' = P$ would imply $P(P')^n = P$ for all $n \geq 1$ by a trivial induction.
   - Then for any nonzero $x \in P$ and $y \in P' \backslash R$ we would have $xy^n \in P \subseteq R$ for all n, which would imply $xR[y] \subseteq R$ and hence that $xR[y]$ is some ideal of R.
   - Then since R is Noetherian, this ideal is finitely generated (say by $a_1, \ldots, a_m$) and then the R-module $R[y]$ would also be finitely generated (by $x^{-1}a_1, \ldots, x^{-1}a_m$): but this says y is integral over R, so since R is integrally closed, we would have $y \in R$, contradiction.
   - Therefore we must have $PP' = R$ and so P is an invertible fractional ideal, as claimed.

3. Every nonzero proper ideal of R is a product of prime ideals.
   - Proof: By (1), for any nonzero proper ideal I there exist prime ideals $P_1, \ldots, P_k$ such that $P_1 \cdots P_k \subseteq I$. We show the result by induction on k.
   - The base case $k = 1$ is easy: if $P_1 \subseteq I$ then since P_1 is maximal and I is proper we have $P_1 = I$.
   - For the inductive step now suppose $k \geq 2$ and let M be a maximal ideal containing I. Then by the same argument as in (2) above, M must equal one of the P_i; without loss of generality take $M = P_1$.
   - By (2), M is invertible; multiplying by M^{-1} yields $P_2 \cdots P_k \subseteq M^{-1}I \subseteq M^{-1}M = R$.
   - Thus, $M^{-1}I$ is an ideal of R that contains the product $P_2 \cdots P_k$, so by the induction hypothesis it has some prime ideal factorization $M^{-1}I = Q_1 \cdots Q_l$. Then $I = MQ_1 \cdots Q_l$ is a prime ideal factorization of I.

4. Every nonzero fractional ideal of R is invertible.
   - Proof: From (2) and (3) we see every nonzero integral ideal is invertible.
   - Then for any fractional ideal $d^{-1}I$ we see that $(d^{-1}I)I^{-1}(dR) = R$, so $d^{-1}I$ has an inverse $I^{-1}(dR)$.
   - Remark: Earlier we showed that if every nonzero fractional ideal is invertible then R is a Dedekind domain. This result supplies the converse statement.

5. Every nonzero ideal of R can be written uniquely as a product of prime ideals, up to reordering.
   - Proof: Clearly (3) shows existence of such a factorization. So now suppose we have two factorizations of a nonzero ideal $I = P_1 \cdots P_k = Q_1 \cdots Q_l$; we show uniqueness by induction on k.
   - The base case $k = 0$ is trivial, since the empty product R cannot be written as a product of one or more prime ideals, since such a product is a proper ideal of R.
   - For the inductive step now suppose that products of $k-1$ prime ideals have unique factorization and suppose $I = P_1 \cdots P_k = Q_1 \cdots Q_l$. Then $Q_1 \cdots Q_l = P_1 \cdots P_k \subseteq P_k$ hence since P_k is prime, one of the Q_i is contained in P_k; by reordering suppose it is Q_l.

- But nonzero primes are maximal, so since P_k and Q_l are nonzero and prime, in fact we must have $P_k = Q_l$.
- By (2), P_k is invertible, so multiplying by P_k^{-1} yields $Q_1 \cdots Q_{l-1} = Q_l^{-1} I = P_k^{-1} I = P_1 \cdots P_{k-1}$, and now applying the inductive hypothesis to the ideal $J = P_1 \cdots P_{k-1} = Q_1 \cdots Q_{l-1}$ yields the result immediately.
- Exercise: If I is a nonzero ideal of a Dedekind domain R, show that I can be written uniquely in the form $I = \prod_{P_i \text{ prime}} P_i^{a_i}$ where the product is taken over all prime ideals of R and the a_i are nonnegative integers only finitely many of which are positive.
- Exercise: Show that the group of fractional ideals in a Dedekind domain is a free abelian group generated by the nonzero prime ideals.

6. For any ideal I of R, there exists some nonzero ideal J of R such that IJ is principal.
   - Proof: If $I = 0$ the result is trivial, so assume I is nonzero.
   - Then by (4), considered as a fractional ideal of R, I is invertible, say with some fractional ideal inverse $d^{-1}J$. Then $I(d^{-1}J) = R$, which is to say, $IJ = (d)$. (Note of course J is nonzero, since $I(d^{-1}0) = 0$.)
7. A Dedekind domain is a principal ideal domain if and only if it is a unique factorization domain.
   - Proof: Any PID is a UFD so the forward direction is immediate. (Alternatively, we could simply apply (5), since if R is a PID then ideal factorizations are the same as element factorizations, up to associates.)
   - Now suppose that R is a UFD. Since the zero ideal is principal and every nonzero ideal is a product of prime ideals by (3), it suffices to show that every prime ideal is principal.
   - So let P be a prime ideal; by (6) there exists some nonzero ideal J such that $PJ = (a)$ is principal.
   - Let a have unique factorization $a = p_1 \cdots p_k$ for some irreducible elements $p_1, \ldots, p_k \in R$. Then since irreducibles are prime in a UFD, each of the ideals (p_i) are prime, and so we have the equality $PJ = (p_1) \cdots (p_k)$.
   - Hence by uniqueness of prime ideal factorizations (5), we must have $P = (p_i)$ for some i, and so P is principal, as desired.

- We can see from the last item in the proposition above that every example of non-unique factorization of elements in a Dedekind domain, ultimately, arises from the presence of nonprincipal ideals.
  - This explains the behavior we observed in our earlier examples of non-unique factorization in the various rings of integers $\mathcal{O}_K$: the existence of nonprincipal ideals in these rings leads directly to the failure of unique factorization, and inversely.

0.13 (Oct 2) Ideal Divisibility in Dedekind Domains

- Now that we have established that Dedekind domains have the properties that every fractional ideal is invertible and every nonzero ideal has a unique prime ideal factorization, let us establish some other properties of ideals.
  - In keeping with our goal of establishing ideal analogues of properties of elements, we can easily develop the basic properties of ideal divisibility.

- Definition: If A and B are ideals of an integral domain R, we say that A divides B and write $A|B$ when there is some ideal C of R such that $B = CA$.

- Proposition (Ideal Divisibility): Suppose A and B are ideals of a Dedekind domain R.

1. We have $A|B$ if and only if $B \subseteq A$.
   - This property is often phrased as "To divide is to contain": A divides B precisely when A contains B.
   - Proof: If $A|B$ then $B = CA \subseteq A$.

- Conversely, if $B \subseteq A$ then since B is invertible, as fractional ideals we have $B^{-1}A \subseteq B^{-1}B = R$ and therefore $B^{-1}A = C$ is some ideal of R: then $A = CB$ so $A|B$.
- Exercise: If A is any ideal in a Dedekind domain R, show that there are only finitely many ideals of R that contain A.

2. We have $A|B$ and $B|A$ if and only if $A = B$.
   - Proof: Obvious from (1).
3. For ideals A and B we say that D is their ideal gcd if $D|A$ and $D|B$, and also for any other common ideal divisor D' with $D'|A$ and $D'|B$, we have $D'|D$. The ideal gcd exists and is unique, and it is equal to the ideal sum $A + B$.
   - Proof: By (1), D is an ideal gcd of A and B precisely when D contains both A and B, and for any other D' containing both A and B, we have $D \subseteq D'$.
   - But the sum ideal $A + B$ is the smallest ideal of R containing both A and B, so it satisfies the requirement of being a gcd.
   - Uniqueness follows from (2) since two gcds would divide each other.
4. For ideals A and B we say that L is their ideal lcm if $A|L$ and $B|L$, and also for any other common multiple L' with $A|L'$ and $B|L'$, we have $L|L'$. The ideal lcm exists and is unique, and it is equal to the ideal intersection $A \cap B$.
   - Proof: By (1), L is an ideal lcm precisely when L is contained in both A and B, and for any other L' contained in both A and B we have $L' \subseteq L$.
   - The intersection ideal $A \cap B$ clearly has this property, and uniqueness follows from (2) since two lcms would divide each other.
5. If A and B have prime ideal factorizations $A = P_1^{a_1} \cdots P_k^{a_k}$ and $B = P_1^{b_1} \cdots P_k^{b_k}$ where the P_i are distinct prime ideals, then $A|B$ if and only if $a_i \leq b_i$ for each i.
   - Proof: If $a_i \leq b_i$ for each i, then taking $C = P_1^{c_1} \cdots P_k^{c_k}$ with $c_i = b_i - a_i$ yields $B = CA$.
   - Conversely, if $B = CA$ then if C has prime ideal factorization $P_1^{c_1} \cdots P_k^{c_k}$ (we may assume the factorization has this form by adding additional prime ideals with exponent zero in the expressions for A and B if necessary), then by uniqueness of factorizations we necessarily have $c_i = b_i - a_i$ and so $a_i \leq b_i$ for each i.
6. If A and B have prime ideal factorizations $A = P_1^{a_1} \cdots P_k^{a_k}$ and $B = P_1^{b_1} \cdots P_k^{b_k}$ where the P_i are distinct prime ideals, then $\gcd(A, B) = P_1^{\min(a_1,b_1)} \cdots P_k^{\min(a_k,b_k)}$ and $\operatorname{lcm}(A, B) = P_1^{\max(a_1,b_1)} \cdots P_k^{\max(a_k,b_k)}$.
   - Proof: By (5) we see $P_1^{\min(a_1,b_1)} \cdots P_k^{\min(a_k,b_k)}$ is a common divisor of A and B.
   - If $D = P_1^{d_1} \cdots P_k^{d_k}$ is any other common divisor, then by (5) we see that $d_i \leq a_i$ and $d_i \leq b_i$ hence $d_i \leq \min(a_i, b_i)$, hence by (5) again that means D divides $P_1^{\min(a_1,b_1)} \cdots P_k^{\min(a_k,b_k)}$, so this ideal is in fact the gcd.
   - The lcm statement follows analogously.
   - Exercise: For any ideals A and B in a Dedekind domain, show that $AB = (A + B)(A \cap B)$.
7. We say ideals A and B are relatively prime when $\gcd(A, B) = R$. Two ideals are relatively prime if and only if they are comaximal (i.e., $A + B = R$) if and only if $AB = A \cap B$.
   - Exercise: If I and J are ideals in a commutative ring with 1, show that $IJ \subseteq I \cap J$, and also that if $I + J = R$ then $IJ = I \cap J$.
   - Proof: By (3) the statement $\gcd(A, B) = R$ is equivalent to $A + B = R$. The second equivalence follows immediately from the exercise above.

- Let us now examine the quotient structure of a Dedekind domain by its ideals.
- Proposition (Quotients of Dedekind Domains): Let R be a Dedekind domain and A be an ideal of R.

1. If A has prime ideal factorization $A = P_1^{a_1} \cdots P_k^{a_k}$, then $R/A \cong (R/P_1^{a_1}) \times \cdots \times (R/P_k^{a_k})$.

- Proof: This is simply an application of the Chinese remainder theorem for rings[4]. The statement follows immediately from the observation that the prime powers $P_i^{a_i}$ are pairwise relatively prime (per their factorizations) and are therefore pairwise comaximal.

2. For any pairwise relatively prime ideals $A_1, \ldots, A_d$ of R and any elements $r_1, \ldots, r_d$ of R, there exists a solution to the congruences $x \equiv r_i \pmod{A_i}$ and the solution is unique modulo $A_1, \ldots, A_d$.
   - Note as usual the statement $x \equiv r_i \pmod{A_i}$ means $x - r_i \in A_i$.
   - Proof: The result is immediate upon factoring each of the A_i into prime powers and then applying (1).
3. If A is nonzero, then every ideal in the quotient ring R/A is principal.
   - Proof: Equivalently, by the lattice isomorphism theorem, if B is any ideal containing A, then we need to show that $B = A + bR$ for some $b \in B$.
   - Now, if B is an ideal containing A, then $B|A$. Thus, if A has prime ideal factorization $A = P_1^{a_1} \cdots P_k^{a_k}$ then B must have a factorization $B = P_1^{b_1} \cdots P_k^{b_k}$ where each $b_i \leq a_i$.
   - Now choose any $r_i \in P_i^{b_i} \backslash P_i^{b_i+1}$ (such an element exists because $P_i^{b_i} = P_i^{b_i+1}$ would contradict unique factorization) and let b be a solution to the simultaneous congruences $b \equiv r_i \pmod{P_i^{b_i+1}}$ for each i, which exists by (2).
   - Then we see immediately that $P_i^{b_i}$ is the exact power of P_i dividing b, and so $\gcd(bR, A) = B$. But the ideal gcd is simply the sum, and so we have $B = A + bR$, as claimed.
4. If A is nonzero, then for any nonzero $a \in A$ there exists some $b \in A$ such that $A = aR + bR$. In particular, every ideal of R is generated (as an ideal, or equivalently as an R-module) by at most two elements.
   - Proof: The first statement follows immediately upon applying (3) to the ideals $A = aR$ and $B = R$.
   - The second statement is immediate since the zero ideal is principal and any nonzero ideal is of the form $A = aR + bR = (a, b)$ in the usual notation for ideals.

0.14 (Oct 3) Ideal Norms, Primes in Extensions

- We can also make some observations about the cardinality of the quotient ring of a Dedekind domain by an ideal I:
- Definition: For an nonzero ideal I of a Dedekind domain R, we define the ideal norm $N(I)$ to be the cardinality of the quotient ring R/I (equivalently, the index $[R : I]$). For completeness we also define the norm of the zero ideal to be 0.
  - In general, the ideal norm in arbitrary Dedekind domains can be infinite, such as for $R = F[t]$ and $I = (t)$ where F is any infinite field.
  - However, when R is the ring of integers in a number field, as we have shown previously, the quotient R/I is finite whenever I is a nonzero ideal.
- Proposition (Ideal Norms): Suppose R is a Dedekind domain.

1. If P is a nonzero prime ideal of R, then for any nonnegative d, the quotient ring P^d/P^{d+1} is isomorphic as an additive abelian group to R/P.
   - Exercise: Let R be an integral domain and let M be a maximal ideal of R. For any $d \geq 0$, show that M^d/M^{d+1} is an R/M-vector space.
   - Proof: Let $\alpha \in P^d \backslash P^{d+1}$ and consider the additive group homomorphism $\varphi : R \to P^d/P^{d+1}$ given by $\varphi(r) = \alpha r + P^{d+1}$.
   - Note (immediately from prime ideal factorizations) we have $\gcd(\alpha R, P^{d+1}) = P^d$, which is to say, $\alpha R + P^{d+1} = P^d$. This observation immediately implies that φ is onto, since for any $t \in P^d$ it says there exists some $s \in R$ such that $\alpha s + P^{d+1} = t + P^{d+1}$.

[4]The statement we use is as follows: let R be commutative with 1 and $I_1, I_2, \ldots, I_n$ be ideals of R. Then the map $\varphi : R \to (R/I_1) \times (R/I_2) \times \cdots \times (R/I_n)$ defined by $\varphi(r) = (r + I_1, r + I_2, \ldots, r + I_n)$ is a ring homomorphism with kernel $I_1 \cap I_2 \cap \cdots \cap I_n$. If all of the ideals $I_1, I_2, \ldots, I_n$ are pairwise comaximal, then φ is surjective and $I_1 \cap I_2 \cap \cdots \cap I_n = I_1 I_2 \cdots I_n$, and thus $R/(I_1 I_2 \cdots I_n) \cong (R/I_1) \times (R/I_2) \times \cdots \times (R/I_n)$.

- Additionally, for $r \in R$, since the largest power of P dividing (α) is P^d by construction, we see $r \in \ker\varphi \iff \alpha r \in P^{d+1} \iff P^{d+1}$ divides $(\alpha)(r) \iff P$ divides $(r) \iff r \in P$.
- Therefore, by the first isomorphism theorem, φ descends to an isomorphism from R/P to P^d/P^{d+1}, as desired.

2. For any nonzero prime ideal P, we have $[R : P^d] = [R : P]^d$.
   - Proof: By (1) each of the quotients R/P, P/P^2, ... , P^{d-1}/P^d is isomorphic as an additive group to R/P, so they all have the same cardinality as R/P.
   - Taking indices and using multiplicativity yields the result immediately.
3. The ideal norm is completely multiplicative: $N(IJ) = N(I)N(J)$ for all ideals I and J.
   - Proof: If I or J is zero the result is trivial.
   - Otherwise, by the Chinese remainder theorem, if $I = P_1^{a_1} \cdots P_k^{a_k}$ then $N(I) = N(P_1^{a_1}) \cdots N(P_k^{a_k})$, and by (2) we see $N(P_i^{a_i}) = N(P)^{a_i}$ for any P_i. The result then follows immediately upon multiplying the prime ideal factorizations of I and J and taking norms.
4. If $R = \mathcal{O}_K$ is the ring of integers of a number field K, then for any $\alpha \in \mathcal{O}_K$, for the ideal $I = (\alpha) = \alpha\mathcal{O}_K$ we have $N(I) = |N_{K/\mathbb{Q}}(\alpha)|$: thus, our use of the word "norm" here agrees with our earlier usage.
   - Proof: Let $\beta_1, \ldots, \beta_n$ be an integral basis of $\mathcal{O}_K$. Then $\alpha\beta_1, \ldots, \alpha\beta_n$ is an integral basis of I, so by our earlier results on discriminants we immediately have $\mathrm{disc}_{K/\mathbb{Q}}(\alpha\beta_1, \ldots, \alpha\beta_n) = N(I)^2 \mathrm{disc}_{K/\mathbb{Q}}(\beta_1, \ldots, \beta_n)$.
   - But $\mathrm{disc}_{K/\mathbb{Q}}(\alpha\beta_1, \ldots, \alpha\beta_n) = \begin{vmatrix} \sigma_1(\alpha\beta_1) & \cdots & \sigma_1(\alpha\beta_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha\beta_1) & \cdots & \sigma_n(\alpha\beta_n) \end{vmatrix}^2 = \begin{vmatrix} \sigma_1(\alpha)\sigma_1(\beta_1) & \cdots & \sigma_1(\alpha)\sigma_1(\beta_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha)\sigma_n(\beta_1) & \cdots & \sigma_n(\alpha)\sigma_n(\beta_n) \end{vmatrix}^2 =$
   $\sigma_1(\alpha)^2 \cdots \sigma_n(\alpha)^2 \begin{vmatrix} \sigma_1(\beta_1) & \cdots & \sigma_1(\beta_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\beta_1) & \cdots & \sigma_n(\beta_n) \end{vmatrix}^2 = N_{K/\mathbb{Q}}(\alpha)^2 \mathrm{disc}_{K/\mathbb{Q}}(\beta_1, \ldots, \beta_n)$.
   - Therefore, since $N(I)$ is nonnegative, we see $N(I) = |N_{K/\mathbb{Q}}(\alpha)|$ as claimed.

- Now that we have established many useful facts about the ideal structure in Dedekind domains, let us return back to use these tools to study the ideals in rings of integers of number fields.
  - So far we have established the existence of prime ideal factorizations, but we would like to be able to compute these factorizations explicitly.
  - Of course, even in $\mathbb{Z}$, actually computing prime factorizations efficiently is a difficult computational problem, so we should not expect to find any factorization procedures that operate more effectively than integer factorization.
  - Since the ring of integers $\mathcal{O}_K$ is an integral extension of $\mathbb{Z}$, its prime ideals all arise naturally from the prime ideals of $\mathbb{Z}$. For essentially the same effort, we can describe the behavior of primes for a general extension L/K rather than simply for $K/\mathbb{Q}$:

- Proposition (Primes in Extensions): Let L/K be an extension of number fields with respective rings of integers $\mathcal{O}_L$ and $\mathcal{O}_K$.

1. If Q is a prime ideal of $\mathcal{O}_L$, then $Q \cap \mathcal{O}_K = P$ is a prime ideal of $\mathcal{O}_K$, and the quotient $\mathcal{O}_K/P$ is a subring of $\mathcal{O}_L/Q$.
   - Proof: Consider the injection homomorphism $\varphi : \mathcal{O}_K \hookrightarrow \mathcal{O}_L$. Then $Q \cap \mathcal{O}_K = \varphi^{-1}(Q)$ is an ideal of $\mathcal{O}_K$ (inverse images of ideals are ideals), and φ therefore induces a homomorphism from $\mathcal{O}_K/\varphi^{-1}(Q)$ to $\mathcal{O}_L/Q$ which is clearly also injective.
   - Since Q is prime, $\mathcal{O}_L/Q$ has no zero divisors, and therefore the subring $\mathcal{O}_K/\varphi^{-1}(Q)$ also has no zero divisors, so $P = \varphi^{-1}(Q)$ is a prime ideal of $\mathcal{O}_K$.
2. If Q is a prime ideal of $\mathcal{O}_L$ and P is a prime ideal of $\mathcal{O}_K$, the following are equivalent (when they hold, we say Q lies over P and P lies under Q):
   (a) Q divides $P\mathcal{O}_L$ (b) Q contains $P\mathcal{O}_L$ (c) Q contains P (d) $Q \cap \mathcal{O}_K = P$ (e) $Q \cap K = P$
   - Proof: (a) and (b) are equivalent by the equivalence of divisibility and containment.

- (b) and (c) are equivalent since Q is an ideal of $\mathcal{O}_L$ and $P\mathcal{O}_L$ is the smallest ideal of $\mathcal{O}_L$ containing P.
- (d) obviously implies (c). For the converse note that if Q contains P then $Q \cap \mathcal{O}_K$ is an ideal of $\mathcal{O}_K$ containing P and it cannot be all of $\mathcal{O}_K$ (since this would imply $1 \in Q$), but since P is maximal this forces the intersection to be P.
- Finally, (d) and (e) are equivalent because $Q \cap K = Q \cap \mathcal{O}_K$ since Q only contains algebraic integers (explicitly, $Q \cap \mathcal{O}_K \subseteq Q \cap K = (Q \cap \mathcal{O}_L) \cap K = Q \cap \mathcal{O}_K$.)

3. Every nonzero prime ideal Q of $\mathcal{O}_L$ lies over a unique nonzero prime ideal P of $\mathcal{O}_K$, and indeed $P = Q \cap \mathcal{O}_K$.
   - Proof: This is immediate from (1) and (2) along with the observation that if $\alpha \in Q$ is nonzero, then $N_{L/\mathbb{Q}}(\alpha)$ is a nonzero integer in Q hence also in P, so P is nonzero also.
4. Every nonzero prime ideal P of $\mathcal{O}_K$ lies under at least one prime ideal Q of $\mathcal{O}_L$. There are finitely many primes Q lying over P, and they are the prime ideal factors in $\mathcal{O}_L$ of $P\mathcal{O}_L$.
   - Proof: All of this is immediate from the equivalences in (2) and the observation that $P\mathcal{O}_L$ has prime ideal factors since it is a proper ideal.
   - For this, suppose that $P\mathcal{O}_L = \mathcal{O}_L$ and consider the fractional ideal inverse P' of P in $\mathcal{O}_K$: it cannot be an integral ideal, so choose any $\alpha \in P'$ that is not in $\mathcal{O}_K$ hence not an algebraic integer. Then we would have $\alpha P\mathcal{O}_L \subseteq \alpha\mathcal{O}_L \subseteq \mathcal{O}_L$ which is impossible since α is not an algebraic integer.

- Applying (4) in the proposition above to the situation $K = \mathbb{Q}$, we see immediately that every nonzero prime ideal of $\mathcal{O}_L$ lies above a unique integer prime p, and these prime ideals of $\mathcal{O}_L$ are precisely the prime ideal factors of $p\mathcal{O}_L$.
  - We may therefore understand the prime ideals of $\mathcal{O}_L$ by studying how the ideal $p\mathcal{O}_L = (p)$ factors in $\mathcal{O}_L$. This is our next task.

- In some individual cases we can work out an essentially explicit description of the prime ideals in the ring of integers using *ad hoc* methods:

- Example: Characterize the prime ideals in $\mathbb{Z}[i]$.
  - Since $\mathbb{Z}[i]$ is Euclidean and therefore a PID, ideal factorizations are equivalent to element factorizations.
  - If p is an integer prime then either (p) is already a prime ideal or $p = rs$ has some nontrivial factorization. In the latter case, taking norms yields $p^2 = N(r)N(s)$ so since $N(r)$ and $N(s)$ must be greater than 1, we must have $N(r) = N(s) = p$, in which case the elements r and s are both irreducible (hence prime, hence generate prime ideals), so we get the factorization $(p) = (r)(s)$.
  - Explicitly, for $r = a + bi$ we see $p = a^2 + b^2$ is the sum of two squares, and conversely if $p = a^2 + b^2$ then certainly $p = (a + bi)(a - bi)$ so we get the ideal factorization $(p) = (a + bi)(a - bi)$.
  - It remains to characterize these primes that are the sum of two squares (which was first done historically by Girard and then followed later by Fermat): they are $p = 2$ and the primes congruent to 1 modulo 4.
  - Clearly $2 = 1^2 + 1^2$ is the sum of two squares, so we obtain the ideal factorization $(2) = (1 + i)(1 - i)$. Note here that because $1 + i$ and $1 - i$ are associates, in fact $(1 + i) = (1 - i)$, so as ideals we actually have $(2) = (1 + i)^2$.
  - For odd primes p, if $p = a^2 + b^2$ then reducing modulo p and rearranging yields $(a/b)^2 \equiv -1 \pmod{p}$ so -1 must be a quadratic residue modulo p. But by Euler's criterion we have the Legendre symbol evaluation $\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \pmod{p}$ which is only $+1$ when $p \equiv 1 \pmod{4}$, so we must have $p \equiv 1 \pmod{4}$.
  - In this situation, there exists an integer r with $r^2 \equiv -1 \pmod{p}$. Then clearly p divides neither $r + i$ nor $r - i$ in $\mathbb{Z}[i]$, yet it divides their product $(r + i)(r - i) = r^2 + 1$, so p is not a prime element, hence it must factor in $\mathbb{Z}[i]$ by the above.
  - We conclude that the prime ideals in $\mathbb{Z}[i]$ are as follows:
    1. The ideal $(1 + i)$, of norm 2, with $(2) = (1 + i)^2$.
    2. The prime ideals (p) of norm p^2 where p is a prime congruent to 3 mod 4.

3. The two ideals $(a+bi)$ and $(a-bi)$ of norm p where $a^2+b^2=p$ is a prime congruent to 1 mod 4.

- We mention also that the argument above gives an explicit way to compute the factorization of p in $\mathbb{Z}[i]$ when $p \equiv 1 \pmod 4$: namely, find a solution to $r^2 \equiv -1 \pmod p$, which can be done by taking $r = u^{(p-1)/4}$ for any quadratic nonresidue u, and then observe that as ideals we have $(p, r+i) = (a+bi)$, so we may find $a+bi$ using the Euclidean algorithm to compute $\gcd(p, r+i)$.

- Exercise: Show that the prime ideals of $\mathbb{Z}[\sqrt{-2}]$ are as follows: the ideal $(\sqrt{-2})$, the ideals (p) where p is a prime congruent to 5 or 7 modulo 8, and the two ideals $(a+b\sqrt{-2})$ and $(a-b\sqrt{-2})$ where $a^2+2b^2=p$ is a prime congruent to 1 or 3 mod 4.

0.15 (Oct 7) Ramification Index and Inertial Degree

- The methods we used to identify the prime ideals in $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{-2}]$ do not extend well to general rings of integers: one obvious difficulty is that we made substantial use of the fact that those rings are principal ideal domains, which many other rings of integers are not.

  - So let us pause for now our discussion of how to compute factorizations and return to the more abstract question of understanding how primes decompose in extensions.
  - Exercise: If P is a prime ideal of $\mathcal{O}_K$ that lies above the integer prime p, show that $N(P)$ is a power of p.
  - Exercise: We have previously observed that an element $\alpha \in \mathcal{O}_K$ of norm $\pm p$ for a prime p is irreducible. Show in fact that such an element is prime.

- Definition: Let L/K be an extension of number fields. If Q is a prime ideal of $\mathcal{O}_L$ lying above a prime ideal P of $\mathcal{O}_K$, the ramification index of Q over P, denoted[5] $e(Q|P)$, is the largest power of Q that divides $P\mathcal{O}_L$.

  - More explicitly, if $Q_1, \ldots, Q_k$ are the prime ideals of $\mathcal{O}_L$ lying over P, then we have a factorization $P\mathcal{O}_L = Q_1^{e_1} \cdots Q_k^{e_k}$: the ramification index $e(Q_i|P)$ is then simply the exponent e_i.
  - Since Q lies above P if and only if Q divides $P\mathcal{O}_L$, we see that $e(Q|P) \geq 1$. When $e(Q|P) > 1$ we say that Q is ramified over P, and when $e(Q|P) = 1$ we say that Q is unramified over P.
  - Example: In $\mathcal{O}_K = \mathbb{Z}[i]$, for the primes $P = 2\mathbb{Z}$ and $Q = (1+i)\mathcal{O}_K$ we have $e(Q|P) = 2$ since $(2) = (1+i)^2$ in $\mathbb{Z}[i]$. If $p \equiv 3 \pmod 4$ is a prime, then for $P = p\mathbb{Z}$ and $Q = p\mathcal{O}_K$ we have $e(Q|P) = 1$. If $p \equiv 1 \pmod 4$ is a prime with $p = a^2+b^2$, then for $P = p\mathbb{Z}$, $Q_1 = (a+bi)\mathcal{O}_K$, and $Q_2 = (a-bi)\mathcal{O}_K$ we have $e(Q_1|P) = e(Q_2|P) = 1$ since $P\mathcal{O}_K = Q_1Q_2$ and the two prime ideals Q_1 and Q_2 are not equal.
  - Example: In $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, as we have previously noted, each of the ideals $P_2 = (2, 1+\sqrt{-5})$, $P_3 = (3, 1+\sqrt{-5})$, $P_3' = (3, 1-\sqrt{-5})$, and $P_5 = (5, \sqrt{-5}) = (\sqrt{-5})$ is prime (the quotient has prime cardinality in each case). Since we also have $(2) = P_2^2$, $(3) = P_3P_3'$, and $(5) = P_5^2$, we see that $e(P_2|2) = 2$, $e(P_3|3) = e(P_3'|3) = 1$, and $e(P_5|5) = 2$.
  - Exercise: Let p be a prime. Show that $(1-\zeta_p)$ is a prime ideal of $\mathbb{Z}[\zeta_p]$ that lies above $p \in \mathbb{Z}$. [Hint: $\mathbb{Z}[\zeta_p]/(1-\zeta_p)$ is isomorphic to $\mathbb{Z}[x]/(1-x, \Phi_p(x))$.]
  - Example: In $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$, for $Q = (1-\zeta_p)\mathcal{O}_K$, noting that Q is a prime ideal lying above $P = p\mathbb{Z}$ by the exercise above, we have $e(Q|P) = p-1$ since $(p) = (1-\zeta_p)^{p-1}$ in $\mathbb{Z}[\zeta_p]$, as noted in an earlier exercise.

- Definition: Let K be a number field and P be a nonzero prime ideal of $\mathcal{O}_K$. The residue field associated to P is the quotient ring $\mathcal{O}_K/P$.

  - Note of course that the residue field is indeed a field because P is maximal, and in fact it is a finite field because the quotient ring by a nonzero ideal is finite (as we have shown previously).
  - Therefore, to understand the structure of the residue field (up to isomorphism), we really just need to determine its cardinality, since there is only one finite field of any given prime-power order (up to isomorphism).

[5] For notational convenience, when $P = (p) = p\mathbb{Z}$ is an ideal of $\mathbb{Z}$ we will simply write $e(Q|p)$.

- Example: In $\mathbb{Z}[i]$, the residue field for $(1+i)$ is $\mathbb{Z}[i]/(1+i)$ which is isomorphic to $\mathbb{F}_2$, the residue field for (p) for a prime $p \equiv 3 \pmod 4$ is $\mathbb{Z}[i]/(p)$ which is a field of cardinality p^2 hence is isomorphic to $\mathbb{F}_{p^2}$, and the residue field for $(a \pm bi)$ where $a^2+b^2 = p$ is a 1 mod 4 prime is $\mathbb{Z}[i]/(a+bi)$ which can be shown to have cardinality p, hence is isomorphic to $\mathbb{F}_p$.
- Example: In $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, again with $P_2 = (2, 1+\sqrt{-5})$, $P_3 = (3, 1+\sqrt{-5})$, $P_3' = (3, 1-\sqrt{-5})$, and $P_5 = (\sqrt{-5})$, the residue field for P_2 is isomorphic to $\mathbb{F}_2$, the residue fields for P_3 and P_3' are isomorphic to $\mathbb{F}_3$, and the residue field for P_5 is isomorphic to $\mathbb{F}_5$.
- Example: In $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$, with $Q = (1-\zeta_p)\mathcal{O}_K$, the residue field of Q has cardinality p hence is isomorphic to $\mathbb{F}_p$.
- Notice in all of the examples that the residue field of each prime ideal P was an extension of the field $\mathbb{F}_p$ where p is the prime of $\mathbb{Z}$ lying below P. In fact, a more general observation holds in any extension L/K of number fields.
- Explicitly, if Q is a prime of $\mathcal{O}_L$ lying over P in $\mathcal{O}_K$, then because $Q \cap \mathcal{O}_K = P$, if we compose the injection $\mathcal{O}_K \hookrightarrow \mathcal{O}_L$ with the projection $\mathcal{O}_L \to \mathcal{O}_L/Q$, the kernel of this composition is simply $\mathcal{O}_K \cap Q = P$, and therefore we have a natural injection of $\mathcal{O}_K/P$ into $\mathcal{O}_L/Q$.

- Definition: Let L/K be an extension of number fields. If Q is a prime ideal of $\mathcal{O}_L$ lying above a prime ideal P of $\mathcal{O}_K$, the inertial degree of Q over P, denoted $f(Q|P)$, is the field extension degree of $\mathcal{O}_L/Q$ over $\mathcal{O}_K/P$.
  - Example: In $\mathbb{Z}[i]$, for $P_2 = (1+i)$ we have $f(P_2|(2)) = 1$, for a prime $p \equiv 3 \pmod 4$ and $P = (p)$ we have $f(P|(p)) = 2$, and for the prime ideals $P = (a+bi)$ and $P' = (a-bi)$ where $a^2+b^2 = p$ is a 1 mod 4 prime we have $f(P|p) = f(P'|p) = 1$.
  - Example: In $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, again with $P_2 = (2, 1+\sqrt{-5})$, $P_3 = (3, 1+\sqrt{-5})$, $P_3' = (3, 1-\sqrt{-5})$, and $P_5 = (\sqrt{-5})$, we have $f(P_2|2) = 1$, $f(P_3|3) = f(P_3'|3) = 1$, and $f(P_5|5) = 1$.
  - Example: In $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$, with $Q = (1-\zeta_p)\mathcal{O}_K$, we have $f(Q|p) = 1$.

- Let us now establish some properties of the ramification index and inertial degree.
  - Exercise: Let $L/K/F$ be an extension tower of number fields with R a prime ideal of $\mathcal{O}_L$ lying over the prime ideal Q of $\mathcal{O}_K$ lying over the prime ideal P of $\mathcal{O}_F$.
    1. Show that the ramification index is multiplicative in towers: $e(R|P) = e(R|Q)e(Q|P)$.
    2. Show that the inertial degree is multiplicative in towers: $f(R|P) = f(R|Q)f(Q|P)$.

- Theorem (The ef-Theorem): Suppose L/K is an extension of number fields of degree m, where $K/\mathbb{Q}$ has degree n.
  1. Let P be a prime ideal of K lying over the integer prime p. Then $N(P) = p^{f(P|p)}$.
     - Proof: By definition of the inertial degree, $\mathcal{O}_K/P$ is a finite field of degree $f(P|p)$ over $\mathbb{Z}/p\mathbb{Z}$, so it has cardinality $p^{f(P|p)}$. Then by definition, $N(P) = [\mathcal{O}_K : P] = p^{f(P|p)}$.
     - Exercise: More generally show that if Q is a prime ideal of L lying over P, then $N_L(Q) = N_K(P)^{f(Q|P)}$.
  2. Let p be an integer prime and suppose (p) has prime ideal factors $P_1, \ldots, P_k$ in $\mathcal{O}_K$. Then $\sum_{i=1}^k e(P_i|p)f(P_i|p) = n = [K : \mathbb{Q}]$.
     - Proof: Suppose that p has prime ideal factorization $p\mathcal{O}_K = P_1^{e_1} \cdots P_k^{e_k}$ in $\mathcal{O}_K$, where by definition $e_i = e(P_i|p)$.
     - By (1), for $f_i = f(P_i|p)$ we have $N(P_i) = [\mathcal{O}_K : P_i] = p^{f_i}$, so since the ideal norm is completely multiplicative we see $N(p\mathcal{O}_K) = N(P_1)^{e_1} \cdots N(P_k)^{e_k} = p^{e_1 f_1} \cdots p^{e_k f_k}$.
     - But since $p\mathcal{O}_K = (p)$ is principal we also have $N(p\mathcal{O}_K) = p^n$, so $n = e_1 f_1 + \cdots + e_k f_k$ as claimed.
  3. For any prime ideal P of $\mathcal{O}_K$, we have $[\mathcal{O}_L : P\mathcal{O}_L] = [\mathcal{O}_K : P]^m$. Equivalently, $N_L(P\mathcal{O}_L) = N_K(P)^{[L:K]}$.
     - Proof: Note that $\mathcal{O}_L/P\mathcal{O}_L$ is a vector space over the finite field $\mathcal{O}_K/P$ (it is in fact a ring extension); the claimed result will then follow by showing the dimension of this vector space is equal to m.
     - First we show the dimension is at most m, so suppose that $\alpha_1, \ldots, \alpha_{m+1} \in \mathcal{O}_L$. Then since the dimension of L over K is m, there exist $\beta_1, \ldots, \beta_{m+1} \in K$ not all zero such that $\beta_1\alpha_1 + \cdots + \beta_{m+1}\alpha_{m+1} = 0$.

- By rescaling we may take all of the $\beta_i \in \mathcal{O}_K$. Now let B be the ideal of $\mathcal{O}_K$ spanned by the β_i, which is an invertible fractional ideal and therefore there exists some fractional ideal C with $BC = \mathcal{O}_K$.
- Choosing any $c \in C$ such that cB is not contained in P, multiplying by c yields $(c\beta_1)\alpha_1 + \cdots + (c\beta_{m+1})\alpha_{m+1} = 0$: now each of the coefficients is contained in $BC \subseteq \mathcal{O}_K$, and not all of them are in P, so the reduction modulo P of this equality yields a nontrivial R/P-linear dependence of the images $\overline{\alpha_1}, \ldots \overline{\alpha_{m+1}}$ in $\mathcal{O}_L/P\mathcal{O}_L$. Hence the dimension is at most n, as desired.
- For equality, suppose P lies over the integer prime p, and let $p\mathcal{O}_K$ have prime ideal factorization $p\mathcal{O}_K = P_1^{e_1} \cdots P_k^{e_k}$, where $e_i = e(P_i|p)$.
- We have shown above that $\dim_{\mathcal{O}_K/P_i}(\mathcal{O}_L/P_i\mathcal{O}_L) \leq m = [L:K]$, and therefore by taking norms we have $N_L(P_i\mathcal{O}_L) \leq N_K(P_i)^m = p^{mf_i}$ by (1), where $f_i = f(P_i|P)$.
- Then we have $p\mathcal{O}_L = (P_1\mathcal{O}_L)^{e_1} \cdots (P_k\mathcal{O}_L)^{e_i}$, and so taking ideal norms yields $p^{mn} = N_L(p\mathcal{O}_L) = N(P_1\mathcal{O}_L)^{e_1} \cdots N(P_k\mathcal{O}_L)^{e_k} \leq p^{m(e_1f_1+\cdots+e_kf_k)}$.
- But by (2) we have $\sum_{i=1}^k e_i f_i = n = [K:\mathbb{Q}]$, so we must have equality everywhere above. Hence in fact we have $\dim_{\mathcal{O}_K/P_i}(\mathcal{O}_L/P_i\mathcal{O}_L) = m$ for all prime ideals P_i above p, including P.

4. Let P be a prime ideal of $\mathcal{O}_K$ prime and suppose $P\mathcal{O}_L$ has prime ideal factors $Q_1, \ldots, Q_k$ in $\mathcal{O}_L$. Then $\sum_{i=1}^k e(Q_i|P)f(Q_i|P) = m = [L:K]$.
   - Proof: Taking norms of the prime ideal factorization $P\mathcal{O}_L = Q_1^{e_1} \cdots Q_k^{e_k}$ where as usual $e_i = e(Q_i|P)$ yields $N_L(P\mathcal{O}_L) = N_L(Q_1)^{e_1} \cdots N_L(Q_k)^{e_k}$.
   - By the exercise following (1) we have $N_L(Q_i) = N_K(P)^{f_i}$ for $f_i = f(Q_i|P)$, and by (3) we have $N_L(P\mathcal{O}_L) = N_K(P)^m$.
   - Putting these together we see $N_K(P)^m = N_K(P)^{e_1f_1} \cdots N_K(P)^{e_kf_k}$ whence $e_1f_1 + \cdots + e_kf_k = m$ as claimed.

- We can use the ef-theorem to classify the possible prime ideal factorization behaviors in extensions. The simplest situation is the case of a quadratic extension:
  - Suppose L/K is a quadratic extension of number fields. Then for any prime ideal P of $\mathcal{O}_K$, we have a prime ideal factorization of $P\mathcal{O}_L = Q_1^{e_1} \cdots Q_k^{e_k}$. For $f_i = e(Q_i|P)$, we then have $e_1f_1 + \cdots + e_kf_k = 2$, so since all of the e_i and f_i are positive integers, there are only three possibilities:
    1. $k = 1$, $e_1 = 2$, $f_1 = 1$. In this case we say P is ramified: its factorization in $\mathcal{O}_L$ is $P\mathcal{O}_L = Q^2$ for some prime ideal Q.
    2. $k = 1$, $e_1 = 1$, $f_1 = 2$. In this case we say P is inert: effectively, P remains prime as we extend from K to L, since its factorization is simply $P\mathcal{O}_L = P\mathcal{O}_L$.
    3. $k = 2$ and $e_1 = f_1 = e_2 = f_2 = 1$. In this case we say P is split: its factorization $P\mathcal{O}_L = Q_1Q_2$ splits apart into several distinct prime ideals.
  - Example: In $\mathbb{Z}[i]$, the prime 2 is ramified since $(2) = (1+i)^2$, the primes congruent to 3 modulo 4 are inert, and the primes congruent to 1 modulo 4 are split since they factor as $(p) = (a+bi)(a-bi)$ where the two ideal factors are not equal.
  - Example: In $\mathbb{Z}[\sqrt{-5}]$, the primes 2 and 5 are ramified since $(2) = (2, 1+\sqrt{-5})^2$ and $(5) = (\sqrt{-5})^2$ while the prime 3 is split since $(3) = (3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$ and the two ideal factors are not equal.

- In extensions of higher degree, we may obtain prime ideal factorizations that mix all of these various kinds of behaviors. Some extremal cases of note in an extension of degree n are as follows:
  1. We have $k = 1$, $e_1 = n$, $f_1 = 1$, in which case the prime ideal factorization is $P\mathcal{O}_L = Q^n$. In this situation we say P is totally ramified: it ramifies to the maximum extent possible.
  2. We have $k = 1$, $e_1 = 1$, $f_1 = n$, in which case the prime ideal P remains prime in $\mathcal{O}_L$. In this situation we say P is totally inert: its factorization does not change at all in the extension from K to L.
  3. We have $k = n$ and all $e_i = f_i = 1$, in which case the prime ideal factorization is $P\mathcal{O}_L = Q_1Q_2 \cdots Q_n$. In this situation we say P is totally split: its factorization splits apart into the maximum possible number of factors in the extension from K to L.

0.16 (Oct 9) Computing Prime Ideal Factorizations, I

- In order to give further examples, we need a more general procedure for computing ideal factorizations. Consider first the simpler case of an extension $K/\mathbb{Q}$ where $\mathcal{O}_K$ has a power basis: i.e., where $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some α.
    - If $m(x)$ is the minimal polynomial for α over $\mathbb{Q}$, then $\mathbb{Z}[\alpha]$ is ring-isomorphic to $\mathbb{Z}[x]/(m(x))$ via the association of α with x, since the evaluation homomorphism $\varphi_\alpha : \mathbb{Z}[x] \to \mathbb{Z}[\alpha]$ mapping x to α is clearly onto and has kernel $(m(x))$ hence it descends to an isomorphism $\varphi : \mathbb{Z}[x]/(m(x)) \to \mathbb{Z}[\alpha]$.
    - Suppose that P is a prime ideal of $\mathcal{O}_K = \mathbb{Z}[\alpha]$ that lies above the integer prime p. As we have shown previously, for any nonzero element a of an ideal I in a Dedekind domain, there exists some other b in that ideal with $(a, b) = I$. Applying this to $a = p$, we see that there exists some polynomial $b(\alpha) \in \mathbb{Z}[\alpha]$ such that $P = (p, b(\alpha))$.
    - Now using the isomorphism φ, we obtain an isomorphism of $\mathbb{Z}[\alpha]/(p)$ with $\mathbb{Z}[x]/(m(x), p)$. But by the third isomorphism theorem, $\mathbb{Z}[x]/(m(x), p)$ is isomorphic to $(\mathbb{Z}[x]/p)/[(m(x), p)/(p)] \cong \mathbb{F}_p[x]/(\tilde{m}(x))$ where $\tilde{m}(x)$ represents the reduction of $m(x)$ modulo p.
    - By the Chinese remainder theorem applied to the prime ideal factorization $(p) = P_1^{e_1} \cdots P_k^{e_k}$ in $\mathcal{O}_K$ we have $\mathbb{Z}[\alpha]/(p) \cong (\mathcal{O}_K/P_1^{e_1}) \times \cdots \times (\mathcal{O}_K/P_k^{e_k})$, while applying it to the irreducible factorization $\tilde{m}(x) = f_1(x)^{d_1} \cdots f_l(x)^{d_l}$ in $\mathbb{F}_p[x]$ yields $\mathbb{F}_p[x]/(\tilde{m}(x)) \cong (\mathbb{F}_p[x]/f_1^{d_1}) \times \cdots \times (\mathbb{F}_p[x]/f_l^{d_l})$.
    - The point now is that these two decompositions must be equivalent to one another, because the decomposition of this finite ring into indecomposable factors, as obtained from the Chinese remainder theorem, is unique. (More precisely, this follows from the structure theorem for modules over principal ideal domains.)
    - Therefore, after rearranging the factors if necessary, we see that we must have $k = l$, and that the isomorphisms must send $\mathbb{F}_p[x]/(f_i(x)^{d_i})$ to $\mathcal{O}_K/P_i^{e_i}$ for each i.
    - Following the various isomorphisms from $\mathbb{F}_p[x]/(\tilde{m}(x))$ back to $\mathbb{Z}[\alpha]/(p)$, we see that the polynomial $f_i(x) \in \mathbb{F}_p[x]$ generating the prime-power factor $f_i(x)^{d_i}$ in the factorization of $\tilde{m}(x)$ maps to the (prime) ideal $f_i(\alpha) + (p) = (p, f_i(\alpha))$ in $\mathbb{Z}[\alpha]/(p)$, and therefore we should take $P_i = (p, f_i(\alpha))$ and $e_i = d_i$ for each i.
    - In other words, to compute the factorization of (p) in $\mathcal{O}_K = \mathbb{Z}[\alpha]$, we factor the minimal polynomial $m(x)$ of α modulo p as $\tilde{m}(x) = f_1(x)^{e_1} \cdots f_k(x)^{e_k}$ for distinct irreducibles $f_i(x) \in \mathbb{F}_p[x]$: then for $P_i = (p, f_i(\alpha))$ we have $(p) = P_1^{e_1} \cdots P_k^{e_k}$.
    - We can also easily obtain the ramification index and inertial degree for each prime in these factorizations:
    - Exercise: Show that if $\mathcal{O}_K = \mathbb{Z}[\alpha]$ and the minimal polynomial $m(x)$ of α factors modulo p as $\tilde{m}(x) = f_1(x)^{e_1} \cdots f_k(x)^{e_k}$, then for $P_i = (p, f_i(\alpha))$ we have $e(P_i|p) = e_i$ and $f(P_i|p) = \deg(f_i)$.
- Let us illustrate how these calculations work in the situation of the Gaussian integers, where we already know the general answer:
- Example: For $K = \mathbb{Q}(i)$, find the prime ideal factorizations of (2), (3), and (5) in $\mathcal{O}_K = \mathbb{Z}[i]$.
    - The minimal polynomial of $\alpha = i$ over $\mathbb{Q}$ is $m(x) = x^2 + 1$, so we need to factor $x^2 + 1$ modulo 2, 3, and 5.
    - Modulo 2 clearly $x^2+1 = (x+1)^2$ so we obtain the ideal factorization $(2) = (2, 1+\alpha)^2$. For $P_2 = (2, 1+\alpha)$, since $1 + \alpha$ divides 2 we can see in fact that P_2 is principal and generated by $1 + \alpha$. Here, 2 is ramified, since $(2) = P_2^2$.
    - Modulo 3 the polynomial $x^2 + 1$ is irreducible, so $P_3 = (3)$ is already a prime ideal of $\mathcal{O}_K$: 3 is inert, with $e(P_3|3) = 1$ and $f(P_3|3) = 2$.
    - Modulo 5 we have $x^2+1 = (x+2)(x+3)$ so we obtain the ideal factorization $(5) = (5, \alpha+2)(5, \alpha+3)$. For $P_5 = (5, \alpha+2)$ since $\alpha+2$ divides 5 we see P_5 is principal and generated by $2+\alpha$. For $P_5' = (5, \alpha+3)$ it is not the case that $\alpha+3$ divides 5 (the quotient is in fact $(3-i)/2$), but another element $\alpha-2 = (\alpha+3)-5$ in the ideal does divide both generators, so $P_5' = (\alpha - 2)$ is also principal.
    - We see that 5 is split: for both ideals P_5 and P_5' we see that $e(P|5) = f(P|5) = 1$.

- Remark: Of course, we already have shown that $\mathbb{Z}[i]$ is a PID (since it is Euclidean); the point is that even when the prime ideals we obtain in our factorizations actually turn out to be principal, we may have to do some amount of work to find a generator.

- Example: For $K = \mathbb{Q}(\sqrt{-5})$, find the prime ideal factorizations of (2), (3), (5), (7), and (11) in $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$.
  - The minimal polynomial of $\alpha = \sqrt{-5}$ over $\mathbb{Q}$ is $m(x) = x^2 + 5$, so we need to factor $x^2 + 5$ modulo 2, 3, 5, 7, and 11.
  - Modulo 2 clearly $x^2 + 5 = (x + 1)^2$ so we obtain the ideal factorization $(2) = (2, 1 + \alpha)^2 = P_2^2$ for $P_2 = (2, 1 + \alpha) = (2, 1 + \sqrt{-5})$: this means 2 is ramified. Additionally, P_2 cannot be principal, since if $P_2 = (\beta)$ then we would have $N_{K/\mathbb{Q}}(\beta) = N_K(P_2) = 2$, but there are no elements of norm 2 in $\mathcal{O}_K$.
  - Modulo 3 we have $x^2+5 = (x-1)(x+1)$ so we obtain the ideal factorization $(3) = (3, 1+\alpha)(3, -1+\alpha) = P_3P_3'$ for $P_3 = (3, 1 + \alpha)$ and $P_3' = (3, -1 + \alpha) = (3, 1 - \alpha)$: this means 3 is split. We see neither P_3 nor P_3' can be principal, since $N_K(P_3) = N_K(P_3') = 3$ but there are no elements of norm 3 in $\mathcal{O}_K$.
  - Modulo 5 we have $x^2 + 5 = x^2$ so we obtain the ideal factorization $(5) = (5, \alpha)^2 = P_5^2$ for $P_5 = (5, \sqrt{-5})$, so 5 is ramified. Since $\sqrt{-5}$ divides 5 in fact $P_5 = (\sqrt{-5})$ is principal, as well.
  - Modulo 7 we have $x^2+5 = (x+3)(x-3)$ so we obtain the ideal factorization $(7) = (7, 3+\alpha)(7, -3+\alpha) = P_7P_7'$ for $P_7 = (7, 3 + \alpha)$ and $P_7' = (7, -3 + \alpha) = (7, 3 - \alpha)$: this means 7 is split. As above, neither P_7 nor P_7' is principal since there are no elements of norm 7 in $\mathcal{O}_K$.
  - Finally, modulo 11 the polynomial $x^2 + 5$ turns out to be irreducible, so (11) is itself prime, meaning 11 is inert in $\mathcal{O}_K$.

- Exercise: Compute the prime ideal factorizations of (2), (3), (5), (7), and (11) in $\mathcal{O}_K$ for $K = \mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$, and $\mathbb{Q}(\sqrt{5})$. Identify which primes ramify, split, and remain inert in each case.

- In higher-degree extensions, we can see additional kinds of behaviors:

- Example: For $K = \mathbb{Q}(\sqrt[3]{2})$, find the prime ideal factorizations of (2), (3), (5), (7), and (31) in $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$.
  - The minimal polynomial of $\alpha = \sqrt[3]{2}$ over $\mathbb{Q}$ is $m(x) = x^3 - 2$, so we need to factor $x^3 - 2$ modulo 2, 3, 5, and 7.
  - Modulo 2 clearly $x^3 - 2 = x^3$ so we obtain the ideal factorization $(2) = (2, \alpha)^3$. Here we can see that the prime ideal $P_2 = (2, \sqrt[3]{2})$ is principal and generated by $\sqrt[3]{2}$, and so we see that 2 is totally ramified in $\mathcal{O}_K$: $e(P_2|2) = 3$.
  - Modulo 3 we have $x^3 - 2 = (x + 1)^3$ so we obtain the ideal factorization $(3) = (3, 1+\alpha)^3$. In fact we can check that $3 = (1 + \alpha)(1 - \alpha + \alpha^2)$ and so the ideal $P_3 = (3, 1 + \alpha)$ is principal and generated by $1 + \alpha$. We see likewise that 3 is totally ramified in $\mathcal{O}_K$: $e(P_3|3) = 3$.
  - Modulo 5 we have $x^3 - 2 = (x+2)(x^2+3x+4)$ so we obtain the ideal factorization $(5) = (5, 2+\alpha)(5, 4+3\alpha+\alpha^2)$. For the ideal $P_5 = (5, 2 + \alpha)$ we have $e(P_5|5) = f(P_5|5) = 1$ whereas for $P_5' = (5, 4 + 3\alpha + \alpha^2)$ we have $e(P_5|5) = 1$ but $f(P_5|5) = 2$. Here we see that 5 splits partially, but not completely, in $\mathcal{O}_K$.
  - Modulo 7 we can verify that $x^3 - 2$ is irreducible, so $P_7 = (7)$ is already a prime ideal of $\mathcal{O}_K$. Here, 7 is totally inert: $f(P_7|7) = 3$.
  - Modulo 31 we can check that $x^3 - 2 = (x - 4)(x - 7)(x + 11)$ so we obtain the ideal factorization $(31) = (31, \alpha - 4), (31, \alpha - 7)(31, \alpha + 11)$. For the ideals $P_{31} = (31, \alpha - 4)$, $P_{31}' = (31, \alpha - 7)$, and $P_{31}'' = (31, \alpha + 11)$ we have $e(P_i|31) = f(P_i|31) = 1$ for each i. Here we see that 31 is totally split in $\mathcal{O}_K$.

- Example: For $K = \mathbb{Q}(\alpha)$ where $\alpha^3 + \alpha + 5 = 0$, compute the prime ideal factorizations of (2), (3), (5), (7), and (97).
  - The discriminant of $x^3 + x + 5$ is $-4 - 27 \cdot 5^2 = -7 \cdot 97$, so since the discriminant of α is squarefree by an earlier exercise we know that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.
  - So, to compute the desired prime ideal factorizations, we simply factor the minimal polynomial x^3+x+5 modulo 2, 3, 5, 7, and 97.
  - Modulo 2, the polynomial is irreducible, so 2 is totally inert and $P_2 = (2)$ is prime: $e(P_2|2) = 1$ and $f(P_2|2) = 3$.

- Modulo 3 we have $x^3+x+5 = (x+1)(x^2+2x+2)$ so we obtain the ideal factorization $(3) = (3, 1+\alpha)(3, 2+2\alpha+\alpha^2)$. We see that 3 splits in $\mathcal{O}_K$ but not completely: for $P_3 = (3, 1+\alpha)$ and $P_3' = (3, 2+2\alpha+\alpha^2)$ we have $e(P_3|3) = e(P_3'|3) = 1$ and $f(P_3|3) = 1$ while $f(P_3'|3) = 2$.
- To decide whether P_3 is principal we can first try dividing 3 by $1+\alpha$: using the Euclidean algorithm in $\mathbb{Q}[x]$ we can determine that $\frac{1}{3}(-2+x-x^2)(x+1) + \frac{1}{3}(5+x+x^3) = 1$ and thus substituting $x = \alpha$ we see $3/(1+\alpha) = -2+\alpha-\alpha^2$. Thus, $P_3 = (3, 1+\alpha) = (1+\alpha)$ is indeed principal, and then P_3' is also principal with generator $3/(1+\alpha) = -2+\alpha-\alpha^2$, which is indeed in P_3'.
- Modulo 5 we have $x^3+x+5 = x(x+2)(x+3)$ so we obtain the ideal factorization $(5) = (5, \alpha)(5, 2+\alpha)(5, 3+\alpha)$, so that 5 splits completely in $\mathcal{O}_K$. We can again attempt to determine whether the factors are principal by trying to find generators for each ideal; after some calculation we can find $5/\alpha = -1-\alpha^2$ so $P_5 = (5, \alpha) = (\alpha)$, and also $5/(2+\alpha) = 5-2\alpha+\alpha^2$ so $P_5' = (5, 2+\alpha) = (2+\alpha)$. But $5/(3+\alpha) = \frac{1}{5}(10-3\alpha+\alpha^2)$ so $3+\alpha$ is not a generator of the third ideal factor $P_5'' = (5, 3+\alpha)$. Instead, using the other two ideals' generators, we can instead compute $5/(\alpha(2+\alpha)) = -3+\alpha-\alpha^2$ and then check that indeed $P_5'' = (5, 3+\alpha) = (-3+\alpha-\alpha^2)$.
- Modulo 7 we have $x^3+x+5 = (x-1)(x-3)^2$ so we obtain the ideal factorization $(7) = (7, \alpha-1)(7, \alpha-3)^2$, so that 7 is partially ramified and partially split.
- For $P_7 = (7, \alpha-1)$ we can compute similarly that $7/(\alpha-1) = -2-\alpha-\alpha^2$ so $P_7 = (\alpha-1)$ is principal. However, to determine whether $P_7' = (7, \alpha-3)$ is principal is trickier, since $7/(\alpha-3) = \frac{1}{5}(-10-3\alpha-\alpha^2)$ so $\alpha-3$ is not a generator of this ideal. With some additional effort, however, one may verify that both 7 and $\alpha-3$ are divisible by α^2-2 and that $\alpha^2-2 \in P_7'$, so that $P_7' = (\alpha^2-2)$.
- Finally, for (97) we have $x^3+x+5 = (x+56)^2(x+82)$ so we obtain the ideal factorization $(97) = (97, 56+\alpha)^2(97, 82+\alpha)$. We can see that 97, like 7, is partially ramified and partially split in $\mathcal{O}_K$.

- Exercise: For $K = \mathbb{Q}(\sqrt[3]{5})$, compute the prime ideal factorizations of (2), (3), (5), (7), and (11) in $\mathcal{O}_K$. (Recall that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ as noted in an earlier exercise.)

- Exercise: For $K = \mathbb{Q}(\alpha)$ where $\alpha^3-\alpha+1 = 0$, compute the prime ideal factorizations of (2), (3), (5), (7), and (23) in $\mathcal{O}_K$. (Recall that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ as noted in an earlier exercise.)

- Example: For $K = \mathbb{Q}(\zeta_5)$, compute the prime ideal factorizations of (2), (3), (5), (7), (11) in $\mathcal{O}_K$.
  - Per our results we know $\mathcal{O}_K = \mathbb{Z}[\zeta_5]$ and that the minimal polynomial of ζ_5 is $\Phi_5(x) = x^4+x^3+x^2+x+1$.
  - Modulo 2, 3, and 7 the polynomial $\Phi_5(x)$ is irreducible, so (2), (3), and (7) are all inert.
  - Modulo 5 we have $\Phi_5(x) = (x-1)^4$ so for $P_5 = (5, -1+\zeta_5)$ we see $(5) = P_5^4$, so (5) is totally ramified. Indeed, since $\zeta_5 - 1$ divides 5, we see $P_5 = (1-\zeta_5)$ is actually principal.
  - Modulo 11 we have $\Phi_5(x) = (x+2)(x+6)(x+7)(x+8)$ so we see that (11) is totally split, with $(11) = (11, 2+\zeta_5)(11, 6+\zeta_5)(11, 7+\zeta_5)(11, 8+\zeta_5)$.
  - Some of these ideals we can readily verify are principal, since $N_{K/\mathbb{Q}}(2+\zeta_5) = \Phi_5(-2) = 11$, so $2+\zeta_5$ divides 11 and so $(11, 2+\zeta_5) = (2+\zeta_5)$. Indeed, from this calculation we can in fact conclude that *all* of the ideals are principal, since $11 = (2+\zeta_5)(2+\zeta_5^2)(2+\zeta_5^3)(2+\zeta_5^4)$ and so since each factor is an element of norm 11, each element generates a prime ideal. (Try to identify which factor corresponds to which of the four prime ideal factors of (11) given above!)
  - We can in fact determine the general features of the factorization of an arbitrary prime ideal (p), which requires determining how the polynomial $\Phi_5(x)$ splits modulo p.
  - Consider the field extension $\mathbb{F}_p(\zeta_5)/\mathbb{F}_p$, where ζ_5 represents a primitive fifth root of unity over $\mathbb{F}_p$. Since all finite fields are splitting fields, as soon as we adjoin one root, we get all the others, so all the irreducible factors of f must be the same degree, and this degree equals the degree d of the extension $\mathbb{F}_p(\zeta_5)/\mathbb{F}_p$.
  - Since then $\mathbb{F}_p(\zeta_5) = \mathbb{F}_{p^d}$, we need only determine the smallest power p^d such that $\mathbb{F}_{p^d}$ contains an element of multiplicative order 5. But since the multiplicative group of $\mathbb{F}_{p^d}$ is cyclic of order p^d-1, we are equivalently seeking the smallest d for which 5 divides p^d-1, which is simply the order of p as an element of $(\mathbb{Z}/5\mathbb{Z})^\times$.
  - That order is 1 when $p \equiv 1 \pmod 5$, 2 when $p \equiv 4 \pmod 5$, and 4 when $p \equiv 2, 3 \pmod 5$.

- We conclude that (p) splits completely as $(p) = P_1P_2P_3P_4$ with $e(P_i|p) = f(P_i|p) = 1$ when $p \equiv 1 \pmod 5$, that (p) splits as a product of two ideals $(p) = Q_1Q_2$ with $e(Q_i|p) = 1$ and $f(Q_i|p) = 2$ when $p \equiv 4 \pmod 5$, and (p) is inert with $(p) = R$ when $e(R|p) = 1$ and $f(R|p) = 4$ when $p \equiv 2, 3 \pmod 5$.

- Exercise: For $K = \mathbb{Q}(\zeta_7)$, compute the prime ideal factorizations of (2), (3), (5), (7), and (11) in $\mathcal{O}_K$. Determine also the general factorization behavior of (p) in terms of the residue class of p modulo 7.

0.17 (Oct 10) Student Presentations of HW2 Problems

0.18 (Oct 16) Computing Prime Ideal Factorizations, II

- Let us now generalize the prime factorization method we have been using so that it can apply to the general situation of a ring of integers in an arbitrary number field extension. Here is the main result:

- Theorem (Dedekind-Kummer Factorization): Suppose that L/K is an extension of number fields and $\alpha \in \mathcal{O}_L$ is nonzero with minimal polynomial $m(x)$ over K; note that the coefficients of $m(x)$ are algebraic integers hence in fact lie in $\mathcal{O}_K$. Further let P be any prime ideal of $\mathcal{O}_K$ lying over an integer prime p not dividing $[\mathcal{O}_L : \mathcal{O}_K[\alpha]]$, and suppose that $m(x)$ factors in the residue field $\mathcal{O}_K/P$ as $m(x) = f_1(x)^{e_1} \cdots f_k(x)^{e_k}$ for distinct monic irreducible polynomials $f_1, \ldots, f_k \in (\mathcal{O}_K/P)[x]$. Define the ideals $Q_i = (P, f_i(\alpha)) = P\mathcal{O}_L + f_i(\alpha)\mathcal{O}_L$.

  1. For each i either $Q_i = \mathcal{O}_L$ or $\mathcal{O}_L/Q_i$ is a field of degree $\deg(f_i)$ over $\mathcal{O}_K/P$.
     - Proof: Consider the quotient $(\mathcal{O}_K/P)[x]/(f_i(x))$, which is in fact a field of degree $\deg(f_i)$ over $\mathcal{O}_K/P$ since $f_i(x)$ is irreducible. This quotient is isomorphic to $\mathcal{O}_K[x]/(P, f_i(x))$ since it is obtained by taking the quotient of $\mathcal{O}_K[x]$ by P and then by $(f_i(x))$, and this is clearly equivalent to taking the quotient by the ideal generated by P and $f_i(x)$.
     - Now consider the ring homomorphism $\varphi : \mathcal{O}_K[x] \to \mathcal{O}_L/Q_i$ sending $x \mapsto \alpha + Q_i$. The kernel of this homomorphism is generated by $m(x)$ and Q_i hence it contains both $f_i(x)$ and P by hypothesis, and therefore also contains the ideal $(P, f_i(x))$ that they generate.
     - This means φ descends to a homomorphism of $\mathcal{O}_K[x]/(P, f_i(x)) \to \mathcal{O}_L/Q_i$. We claim this map is onto, which is to say that $\mathcal{O}_L = \mathcal{O}_K[\alpha] + Q_i$. For this note that $p \in Q_i$ since Q_i lies over P and P lies over p: and then the index of $\mathcal{O}_K[\alpha] + Q_i$ divides both the index $[\mathcal{O}_L : \mathcal{O}_K[\alpha]]$ and the index $[\mathcal{O}_L : p\mathcal{O}_L] = p^{[L:\mathbb{Q}]}$, but these are relatively prime by hypothesis.
     - Now, finally, because $\mathcal{O}_K[x]/(P, f_i(x))$ is a field, the first isomorphism theorem yields the desired result: either $\mathcal{O}_L/Q_i$ is the trivial ring (in which case $Q_i = \mathcal{O}_L$) or $\mathcal{O}_L/Q_i$ is isomorphic to the field $\mathcal{O}_K[x]/(P, f_i(x))$ of degree $\deg(f_i)$ over $\mathcal{O}_K/P$.
  2. The ideals $Q_1, \ldots, Q_k$ are pairwise comaximal: $Q_i + Q_j = \mathcal{O}_L$ for all $i \neq j$.
     - Proof: By the Euclidean algorithm in $(\mathcal{O}_K/P)[x]$, since $f_i(x)$ and $f_j(x)$ are relatively prime, there exist polynomials $h_i(x)$ and $h_j(x)$ such that $h_i(x)f_i(x) + h_J(x)f_j(x) \equiv 1 \pmod P$, which is to say, there exists $r \in P$ such that $h_i(x)f_i(x) + h_J(x)f_j(x) - r = 1$.
     - Now setting $x = \alpha$ yields $h_i(\alpha)f_i(\alpha) + h_j(\alpha)f_j(\alpha) - r = 1$, whence $1 \in (P, f_i(\alpha)) + (P, f_j(\alpha))$ as desired.
  3. The ideal $P\mathcal{O}_L$ divides $Q_1^{e_1} \cdots Q_k^{e_k}$.
     - Proof: First note that because $\prod_{i=1}^k f_i(x)^{e_i} = m(x)$ modulo P, setting $x = \alpha$ yields that $\prod_{i=1}^k f_i(\alpha)^{e_i} = m(\alpha) = 0$ modulo $P\mathcal{O}_L$.
     - Now since $Q_i = (P\mathcal{O}_L, f_i(\alpha))$ we see that $Q_1^{e_1} \cdots Q_k^{e_k}$ is contained in $(P\mathcal{O}_L, \prod_{i=1}^k f_i(\alpha)^{e_i}) = P\mathcal{O}_L$ by the observation above. Since divisibility is equivalent to containment, the result follows.
  4. The prime ideal factorization of $P\mathcal{O}_L$ is $P\mathcal{O}_L = Q_1^{e_1} \cdots Q_k^{e_k}$, and also $e(Q_i|P) = e_i$ and $f(Q_i|P) = \deg(f_i)$.
     - Proof: By (1), each of the ideals Q_i is either equal to $\mathcal{O}_L$ or a prime ideal of $\mathcal{O}_L$ that lies over p with $f(Q_i|P) = \deg(f_i)$. (In the former case, which as we will see does not actually occur, we can view $f(Q_i|P)$ as being zero.)
     - Additionally, by (2) we see that all of the prime ideals among $Q_1, \ldots, Q_k$ are distinct.

- Finally, by (3) we know that $P\mathcal{O}_L$ divides $Q_1^{e_1} \cdots Q_k^{e_k}$, and therefore the prime ideal factorization of $P\mathcal{O}_L$ must be of the form $Q_1^{d_1} \cdots Q_k^{d_k}$ for some integers $d_i \leq e_i$.
- By the ef-theorem, we then have $n = [L : K] = \sum_{i=1}^{k} d_i \cdot f(Q_i|P) \leq \sum_{i=1}^{k} e_i \deg(f_i) = \deg(m) = n$. But this forces us to have equality everywhere, so we must have $e(Q_i|P) = d_i = e_i$ for each i, and also $f(Q_i|P) = \deg(f_i)$ for each i.
- In particular, none of the Q_i can equal $\mathcal{O}_L$, so they are all prime ideals, and then so the prime ideal factorization of $P\mathcal{O}_L$ is $P\mathcal{O}_L = Q_1^{e_1} \cdots Q_k^{e_k}$.

- Aside from applying in general extensions and not just over $\mathbb{Q}$, the other main improvement in this theorem is that it does not require us to compute a basis for the ring of integers $\mathcal{O}_L$ over $\mathcal{O}_K$, which may not exist at all!
  - Of course, there is a tradeoff: we are free to choose any $\alpha \in \mathcal{O}_L$ that is not in $\mathcal{O}_K$ and compute with respect to α, but the method does not allow us to compute the factorization of any prime ideal above a prime p dividing the index $[\mathcal{O}_L : \mathcal{O}_K[\alpha]]$. Fortunately, there are only finitely many such primes, and we may certainly try to factor those remaining ideals by choosing another α whose index is different. (Unfortunately, this may not always succeed: there exist examples where every choice of α yields an index divisible by p.)
  - In the situation where $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ for some α, we of course have no difficulties, but there may not exist such an α for general extensions L/K.

- Example: For $K = \mathbb{Q}(\sqrt[3]{10})$, find the prime ideal factorizations of (2), (5), (7), (11), and (3) in $\mathcal{O}_K = \mathbb{Z}[1, \sqrt[3]{10}, \frac{1+\sqrt[3]{10}+\sqrt[3]{100}}{3}]$.
  - We first try using $\alpha = \sqrt[3]{10}$ with minimal polynomial $m(x) = x^3 - 10$.
  - Using the integral basis $\{1, \alpha, \frac{1}{3}(1+\alpha+\alpha^2)\}$ computed in an earlier exercise, we can calculate $\text{disc}(K) = -300$ and $\text{disc}_{K/\mathbb{Q}}(\alpha) = -2700$ so that $[\mathcal{O}_K : \mathbb{Z}[\alpha]] = 3$ (which agrees with the fact that $d_1 = 1$ and $d_2 = 3$ for this α).
  - Therefore, the Dedekind-Kummer method will apply with α to any prime $p \neq 3$.
  - For $p = 2$ we see $m(x) = x^3 \pmod 5$ so 2 is totally ramified with $(2) = P_2^3$ where $P_2 = (2, \alpha)$. One may check in fact that P_2 is principal and generated by $-2 + \alpha$, which has norm 2.
  - For $p = 5$ we see $m(x) = x^3 \pmod 5$ as well so 5 is also totally ramified with $(5) = P_5^3$ where $P_5 = (5, \alpha)$. One may check in fact that P_5 is principal and generated by $5 + 2\alpha + \alpha^2$, which has norm 5.
  - For $p = 7$ we see $m(x)$ is irreducible modulo 7, so 7 is totally inert.
  - For $p = 11$ we see $m(x) = (x + 1)(x^2 - x + 1) \pmod{11}$, so 11 is partially split with $(11) = P_{11}P'_{11}$ where $P_{11} = (11, 1 + \alpha)$ and $P'_{11} = (11, 1 - \alpha + \alpha^2)$. One may similarly check that $P_{11} = (1 + \alpha)$ and $P'_{11} = (1 - \alpha + \alpha^2)$ are both principal.
  - In order to factor the ideal $p = 3$, however, we cannot use the order $\mathbb{Z}[\alpha]$ since its index is divisible (in fact equal) to 3.
  - Looking around for another simple order, we can try using the order $\mathbb{Z}[\beta]$ where $\beta = \frac{1}{3}(1+\alpha+\alpha^2)$, which we have already shown is also an algebraic integer. In fact this will work, because after some calculation we can find $\text{disc}_{K/\mathbb{Q}}(\beta) = -300$ whence $[\mathcal{O}_K : \mathbb{Z}[\beta]] = 1$. (This means in fact we could have just used $\mathbb{Z}[\beta]$ for all our calculations.)
  - We can find the minimal polynomial for β by computing the characteristic polynomial of the multiplication-by-β map on K with respect to the field basis $\{1, \alpha, \alpha^2\}$; this yields the minimal polynomial $M(x) = x^3 - x^2 - 3x - 3$.
  - Then for $p = 3$ we see $M(x) = x^2(x - 1) \pmod 3$, so 3 is partially ramified and partially split with factorization $(3) = P_3^2 P'_3$ where $P_3 = (3, \beta)$ and $P'_3 = (3, -1 + \beta)$. One may then verify that $P_3 = (\beta)$ and $P'_3 = (\beta - \alpha)$ are both principal.
  - Remark: If we had attempted to use the factorization procedure to factor (3) using the order $\mathbb{Z}[\alpha]$, the resulting factorization would be incorrect, since $x^3 - 10 = (x - 1)^3 \pmod 3$, but in fact the ideal (3) is not totally ramified.

- Example: For $K = \mathbb{Q}(\sqrt{5}, \sqrt{13})$, find the prime ideal factorizations of (3), (5), (13), and (2) in $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{5}}{2}, \frac{1+\sqrt{13}}{2}]$. Compare these factorizations to the corresponding factorizations in $\mathcal{O}_F$ for $F = \mathbb{Q}(\sqrt{5})$.
  - Using the integral basis $\{1, \frac{1+\sqrt{5}}{2}, \frac{1+\sqrt{13}}{2}, \frac{(1+\sqrt{5})(1+\sqrt{13})}{4}\}$ we obtained earlier for $\mathcal{O}_K$, we can compute $\text{disc}(K) = 5^2 13^2$.
  - To compute factorizations we try using $\alpha = \frac{\sqrt{5}+\sqrt{13}}{2} \in \mathcal{O}_K$, which does have $K = \mathbb{Q}(\alpha)$ since the four Galois conjugates of α are $\alpha_i = \frac{\pm\sqrt{5}\pm\sqrt{13}}{2}$.
  - Then the minimal polynomial of α over $\mathbb{Q}$ is $m(x) = \prod_i (x - \alpha_i) = x^4 - 9x^2 + 4$ and $\text{disc}_{K/\mathbb{Q}}(\alpha) = \prod_{i<j}(\alpha_i - \alpha_j)^2 = 2^6 5^2 13^2$, and so $[\mathcal{O}_K : \mathbb{Z}[\alpha]] = 2^6$.
  - In $F = \mathbb{Q}(\sqrt{5})$ we have instead the minimal polynomial $M(x) = x^2 - x - 1$ for the generator $\beta = \frac{1+\sqrt{5}}{2}$.
  - For $p = 3$ we see $m(x) = (x^2 + x - 1)(x^2 - x - 1) \pmod 3$, so $3\mathcal{O}_K = Q_3 Q_3'$ where $Q_3 = (3, -1 + \alpha + \alpha^2)$ and $Q_3' = (3, -1 - \alpha + \alpha^2)$.
  - In $F = \mathbb{Q}(\sqrt{5})$ since the polynomial $M(x) = x^2 - x - 1$ is irreducible mod 3, we see that $3\mathcal{O}_F = P_3$ is a prime ideal of $\mathcal{O}_{\sqrt{-5}}$. Thus, in the extension tower $K/F/\mathbb{Q}$, the prime 3 is inert from $\mathbb{Q}$ to F, but splits from F to K.
  - For $p = 5$ we see $m(x) = (x^2 + 3)^2 \pmod 5$, so $5\mathcal{O}_K = Q_5^2$ where $Q_5 = (5, 3 + \alpha^2)$.
  - In F, since $x^2 - x - 1 = (x + 2)^2 \pmod 5$, we see that $5\mathcal{O}_F = P_5^2$ where $P_5 = (5, 2 + \alpha)$. Thus, in the extension tower $K/F/\mathbb{Q}$, the prime 5 ramifies from $\mathbb{Q}$ to F, but the ramified prime P_5 remains inert from F to K.
  - For $p = 13$ we see $m(x) = (x^2 + 2)^2 \pmod{13}$ we see that $13\mathcal{O}_K = Q_{13}^2$ where $Q_{13} = (13, 2 + \alpha^2)$.
  - In F, since $x^2 - x - 1$ is irreducible mod 13, we see $13\mathcal{O}_F = P_{13}$ is a prime ideal of $\mathcal{O}_{\sqrt{-15}}$. Thus, in the extension tower $K/F/\mathbb{Q}$, the prime 13 is inert from $\mathbb{Q}$ to F, but then ramifies from F to K.
  - To find the factorization of $p = 2$ we cannot directly use Dedekind-Kummer, but instead we can exploit the intermediate field F. Explicitly, in $\mathcal{O}_F$ since $M(x) = x^2 - x - 1$ is irreducible modulo 2, we see that $2\mathcal{O}_F = P_2$ is a prime ideal in $\mathcal{O}_F$.
  - Now since $\mathcal{O}_K = \mathcal{O}_F[\frac{1+\sqrt{13}}{2}]$, we may use Dedekind-Kummer to find the factorization of $2\mathcal{O}_K = P_2\mathcal{O}_K$ in the extension K/F. To do this we must factor the minimal polynomial $\tilde{m}(x) = x^2 - x - 3$ of $\gamma = \frac{1+\sqrt{13}}{2}$ in the residue field $\mathcal{O}_K/P_2 \cong \mathbb{F}_4$.
  - We can see that $\tilde{m}(x)$ does factor over $\mathbb{F}_4$ (since $\mathbb{F}_4$ is the degree-2 extension of $\mathbb{F}_2$, all quadratic polynomials split in $\mathbb{F}_4$): explicitly, with $\mathcal{O}_K/P_2 \cong \mathbb{Z}[\beta]/(2) \cong \mathbb{F}_2[y]/(y^2 - y - 1)$ where y corresponds to $\beta = \frac{1+\sqrt{5}}{2}$, we obtain the factorization $\tilde{m}(x) = (x + y)(x + y + 1)$ (note that all of the coefficients are still modulo 2).
  - Therefore, we see that $2\mathcal{O}_K = Q_2 Q_2'$ where $Q_2 = (2, \gamma + \beta)$ and $Q_2' = (2, \gamma + \beta + 1)$.
  - Exercise: For $K = \mathbb{Q}(\sqrt{5}, \sqrt{13})$, compare the prime ideal factorizations of (2), (3), (5), and (7) in K to those in the other two subfields $\mathbb{Q}(\sqrt{13})$ and $\mathbb{Q}(\sqrt{65})$.

- Exercise: For $K = \mathbb{Q}(\sqrt{3}, \sqrt{7})$, find the prime ideal factorizations of (2), (3), (5), and (7) in $\mathcal{O}_K = \mathbb{Z}[\frac{\sqrt{3}+\sqrt{7}}{2}]$. Compare these factorizations to the corresponding factorizations in $\mathcal{O}_F$ for $F = \mathbb{Q}(\sqrt{3})$.

0.19 (Oct 17) Factorizations and Ramification

- In fact, as originally shown by Dedekind, the only primes for which we may fail to obtain a factorization using the Dedekind-Kummer method are fairly small.

- Theorem (Dedekind): Suppose K is a number field and p is a prime integer. If $p\mathcal{O}_K$ has prime ideal factorization $P_1^{e_1} \cdots P_k^{e_k}$ in $\mathcal{O}_K$, then there exists some $\alpha \in \mathcal{O}_K$ with p not dividing the index $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ if and only if there exist distinct monic irreducible polynomials $g_1(x), \ldots, g_k(x) \in \mathbb{F}_p[x]$ such that $\deg(g_i) = f(P_i|p)$ for each $1 \leq i \leq k$. As a consequence, if there does not exist any such α, then $p < [K : \mathbb{Q}]$.

- If there exists such an α, then by the factorization theorem proven earlier, then the polynomials $g_1(x), \ldots, g_k(x)$ can simply be taken as the irreducible factors of $m(x)$, since as we noted in the proof of that theorem, we have $\deg(g_i) = f(P_i|p)$.
- We only sketch the proof of the converse: suppose we have distinct monic polynomials $g_1(x), \ldots, g_k(x) \in \mathbb{Z}[x]$ whose reductions are irreducible modulo p and where $\deg(g_i) = f(P_i|p)$. For each P_i let $I_i = \prod_{j \neq i} P_j^{e_j}$ so that $p\mathcal{O}_K = P_i^{e_i} I_i$.
- Now choose $a_i \in \mathcal{O}_K$ such that $g_i(a_i) \equiv 0 \pmod{P_i}$, $g_i(a_i) \not\equiv 0 \pmod{P_i^2}$, and $a_i \equiv 0 \pmod{I_i}$: such a choice is always possible because the field $\mathcal{O}_K/P_i$ is a finite field of degree $f(P_i|p) = \deg(g_i)$ over $\mathbb{F}_p$ which is the splitting field of all irreducible polynomials of that degree, so g_i has some root a_i mod P_i. If this root gives $g_i(a_i) \equiv 0 \pmod{P_i^2}$ then simply add any element of P_i not in P_i^2 to it: since g_i is irreducible it cannot have a repeated root modulo P_i, so the new choice must have $g_i(a_i) \not\equiv 0 \pmod{P_i^2}$. Finally, the third condition $a_i \equiv 0 \pmod{I_i}$ can be added via the Chinese remainder theorem.
- Finally, use the Chinese remainder theorem to construct an element $\alpha \equiv a_i \pmod{P_i^2}$ for each $1 \leq i \leq k$ that generates $K/\mathbb{Q}$ (this last condition can be included by the exercise below). With a somewhat tedious calculation, one may then show p does not divide $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$, so this element has the desired property.
- Exercise: Let K be a number field and let I be a nonzero ideal of $\mathcal{O}_K$ with $c \in \mathcal{O}_K$ arbitrary. Show that there are infinitely many elements $a \equiv c \pmod{I}$ such that $K = \mathbb{Q}(a)$. [Hint: Let $b \in \mathcal{O}_K$ generate $K/\mathbb{Q}$ and $N = N(I)$. Show that infinitely many $c_k = a + kNb$ for $k \in \mathbb{Z}$ are generators of $K/\mathbb{Q}$.]
- For the bound $p < [K : \mathbb{Q}]$ we first recall another fact:
- Exercise: Let p be a prime and let $f_p(n)$ be the number of monic irreducible polynomials of degree n in $\mathbb{F}_p[x]$. Show that $f_p(n) = \frac{1}{n} \sum_{d|n} \mu(d) p^{n/d}$ where μ denotes the Möbius μ-function.
- To prove the bound, suppose that $p \geq [K : \mathbb{Q}]$. Then for any $1 \leq m \leq [K : \mathbb{Q}]$, by the ef-theorem there can be at most $[K : \mathbb{Q}]/m \leq p/m$ prime ideals in the factorization of $p\mathcal{O}_K$ with inertial degree f equal to m.
- But by the exercise above, we have $f_p(m) > p^m/m \geq p/m$, and so there do exist at least as many monic irreducible polynomials in $\mathbb{F}_p[x]$ of degree m as prime ideal factors of $p\mathcal{O}_K$ having inertial degree m. The converse theorem above then immediately yields that there exists some $\alpha \in \mathcal{O}_K$ with p not dividing the index $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$, as required.
- Exercise: Suppose that $K/\mathbb{Q}$ is an extension of degree 3. Show that if p is an odd prime, then there exists some $\alpha \in \mathcal{O}_K$ such that $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ is not divisible by p. Show also that if 2 splits completely in K, then for any $\alpha \in \mathcal{O}_K$, the index $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ is divisible by 2.

- We will mention also that there is a way to extend the Dedekind-Kummer factorization method to handle the situations where p divides the index $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$, as shown by Ore in 1926:

- Theorem (Ore Factorization Theorem): Let $K = \mathbb{Q}(\alpha)$ where $\alpha \in \mathcal{O}_K$ has minimal polynomial $m(x)$ over $\mathbb{Q}$, let p be an integer prime lying below a prime ideal P of $\mathcal{O}_K$, and suppose that p^d is the exact power of p dividing the discriminant of α. If $m(x)$ has a factorization modulo p^{d+1} of the form $m(x) = g_1(x) \cdots g_r(x)$ for irreducible polynomials $g_1, \ldots, g_r$, then the prime ideal factorization of p in $\mathcal{O}_K$ is $p\mathcal{O}_K = P_1^{e_1} \cdots P_r^{e_r}$ where the P_i are distinct prime ideals and $e(P_i|p)f(P_i|p) = \deg(g_i)$.

  - This theorem also extends naturally to the situation of a relative extension L/K, which we will not bother with.
  - We will not prove this theorem, but the fundamental idea is to lift the isomorphism given by the Chinese remainder theorem that we described in the Dedekind-Kummer factorization procedure from $\mathbb{Z}/p\mathbb{Z}$ to the p-adic ring $\mathbb{Z}_p$.
  - More explicitly, the distinct components of the p-adic factorization of $m(x)$ will correspond to the distinct prime powers $P_i^{e_i}$, so there are the same number of each and then comparing the extension degrees of the corresponding local residue fields yields the second statement. Finally, one uses Hensel's lemma to show that the factorization of $m(x)$ modulo p^k for increasing k stabilizes for $k \geq d+1$, and therefore the factorization structure of $m(x)$ modulo p^{d+1} will be the same as the p-adic factorization structure of $m(x)$ obtained by taking an appropriate inverse limit of factorizations modulo p^k as $k \to \infty$.

- We will note that factoring polynomials over $\mathbb{Z}/p^d\mathbb{Z}$ is not as convenient as factoring them in $\mathbb{Z}/p\mathbb{Z}$, since factorizations are no longer unique (their structures, however, still are): for instance, the polynomial x^2-1 has four roots and four different factorizations over $\mathbb{Z}/8\mathbb{Z}$, namely as $(x-r)^2$ for $r=1,3,5,7$, but each individual factorization only has a single repeated factor.
- Example: For $K=\mathbb{Q}(\sqrt[3]{10})$ using $\alpha=\sqrt[3]{10}$, we may observe that $\text{disc}(\alpha)=-2^2 3^3 5^2$ so the exact power of 3 dividing the discriminant of α is 3^3. Factoring $m(x)=x^3-10$ modulo 3^4 we find a factorization $(x-13)(x^2+13x+7)$, and so by Ore's theorem we see that $3\mathcal{O}_K$ is the product of two prime powers, one of which has $ef=1$ and the other of which has $ef=2$. In fact, because 3 is ramified in K (as follows from results we will establish shortly), at least one factor must have ramification index greater than one; thus, we can conclude that $3\mathcal{O}_K$ factors as $P_1^2 P_2$ for some prime ideals P_1 and P_2 each of norm 3.

- Our goal now is to study the phenomenon of ramification. To motivate some of the constructions, let us first review the examples of ramified primes we have already found.
  - In $\mathbb{Q}(i)$, of discriminant 2, the only ramified prime is $(2)=(1+i)^2$.
  - In $\mathbb{Q}(\sqrt{-5})$, of discriminant -20, the primes $(2)=(2,1+\sqrt{-5})^2$ and $(5)=(\sqrt{-5})^2$ are ramified. The primes 3, 7, and 11 are unramified.
  - In $\mathbb{Q}(\sqrt[3]{2})$, of discriminant -108, the primes $(2)=(\sqrt[3]{2})^3$ and $(3)=(1+\sqrt[3]{2})^3$ are totally ramified, while the primes 5, 7, and 31 are unramified.
  - In $\mathbb{Q}(\zeta_5)$, of discriminant 625, the prime $(5)=(1-\zeta_5)^4$ is totally ramified, while the primes 2, 3, 7, and 11 are unramified.
  - In $\mathbb{Q}(\sqrt[3]{10})$, of discriminant -300, the primes $(2)=(-2+\sqrt[3]{10})^3$ and $(5)=(5+2\sqrt[3]{10}+\sqrt[3]{100})^3$ are totally ramified, while $(3)=P_3^2 P_3'$ was ramified (but not totally).
  - In $\mathbb{Q}(\sqrt{5},\sqrt{13})$, of discriminant $5^2 13^2$, the primes 5 and 13 ramify, but only partially: 5 ramifies from $\mathbb{Q}$ to $\mathbb{Q}(\sqrt{5})$ while 13 ramifies from $\mathbb{Q}(\sqrt{5})$ to $\mathbb{Q}(\sqrt{5},\sqrt{13})$.

- We can see quite clearly that in all of our examples, the ramified primes are precisely the ones dividing the discriminant of the field. In the situation where $\mathcal{O}_K=\mathbb{Z}[\alpha]$ we can show this quite directly:

- Exercise: Suppose $K=\mathbb{Q}(\alpha)$ where $\mathcal{O}_K=\mathbb{Z}[\alpha]$. Prove that an integer prime p is ramified in K if and only if p divides the discriminant $\text{disc}(K)$. [Hint: Note $\text{disc}(K)=\text{disc}(m(x))$ where $m(x)$ is the minimal polynomial of α over $\mathbb{Q}$, and apply Dedekind-Kummer.]

- In the general case, we have to expend a bit more effort. Let us prove half of the main result now:

- Proposition (Ramification and Discriminants): Suppose K is a number field and p is an integer prime. If p ramifies in K, then $p|\text{disc}(K)$.
  - Proof: Suppose P is a prime ideal of $\mathcal{O}_K$ lying above $p\in\mathbb{Z}$ with $e(P|p)>1$, and write $p\mathcal{O}_K=PI$ where by hypothesis I is a product that includes all of the ideals lying above p, hence is contained in all of these ideals.
  - Let α be an element of I not in $p\mathcal{O}_K$ (note I properly divides hence properly contains $\mathcal{O}_K$): then by hypothesis α is contained in all primes of $\mathcal{O}_K$ lying above p, but α is not an $\mathcal{O}_K$-multiple of p.
  - Let L be the Galois closure of $K/\mathbb{Q}$: then since α is contained in all primes of $\mathcal{O}_K$ lying above p, it is also contained in all primes of $\mathcal{O}_L$ lying above p.
  - For any $\sigma\in\text{Gal}(L/\mathbb{Q})$ and any prime ideal Q of $\mathcal{O}_L$ lying above p, we can see easily that $\sigma^{-1}(Q)$ is also a prime ideal lying above p, hence $\sigma^{-1}(Q)$ contains α, and so Q contains $\sigma(\alpha)$.
  - Now choose an integral basis $\beta_1,\ldots,\beta_n$ of $\mathcal{O}_K$: then $\alpha=a_1\beta_1+\cdots+a_n\beta_n$ for some $a_i\in\mathbb{Z}$, where not all of the a_i are divisible by p because $\alpha\notin p\mathcal{O}_K$. Suppose without loss of generality that p does not divide a_1.

- Then letting $\sigma_1, \dots, \sigma_n$ be the complex embeddings of K, we have $\begin{vmatrix} \sigma_1(\alpha) & \sigma_1(\beta_2) & \cdots & \sigma_1(\beta_n) \\ \sigma_2(\alpha) & \sigma_2(\beta_2) & \cdots & \sigma_2(\beta_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha) & \sigma_n(\beta_2) & \cdots\cdots & \sigma_n(\beta_n) \end{vmatrix} =$
$\begin{vmatrix} a_1\sigma_1(\beta_1)+\cdots+a_n\sigma_1(\beta_n) & \sigma_1(\beta_2) & \cdots & \sigma_1(\beta_n) \\ a_1\sigma_2(\beta_1)+\cdots+a_n\sigma_2(\beta_n) & \sigma_2(\beta_2) & \cdots & \sigma_2(\beta_n) \\ \vdots & \vdots & \ddots & \vdots \\ a_1\sigma_n(\beta_1)+\cdots+a_n\sigma_n(\beta_n) & \sigma_n(\beta_2) & \cdots\cdots & \sigma_n(\beta_n) \end{vmatrix} = a_1 \begin{vmatrix} \sigma_1(\beta_1) & \sigma_1(\beta_2) & \cdots & \sigma_1(\beta_n) \\ \sigma_2(\beta_1) & \sigma_2(\beta_2) & \cdots & \sigma_2(\beta_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\beta_1) & \sigma_n(\beta_2) & \cdots\cdots & \sigma_n(\beta_n) \end{vmatrix}$ and
so $\text{disc}(\alpha, \beta_2, \dots, \beta_n) = a_1^2 \text{disc}(\beta_1, \dots, \beta_n) = a_1^2 \text{disc}(K)$.
- Now by our calculations above, we know that $\sigma_i(\alpha) \in Q$ for every prime ideal Q of $\mathcal{O}_L$ lying over p, hence Q also contains $\text{disc}(\alpha, \beta_2, \dots, \beta_n)$. But since $\text{disc}(\alpha, \beta_2, \dots, \beta_n)$ is an integer, it is contained in $Q \cap \mathbb{Z} = p\mathbb{Z}$.
- Finally, since a_1 is not divisible by p, we conclude that $p | \text{disc}(K)$, as desired.

- We would like to establish the converse of this result, and extend it to relative extensions.
  - As motivation, note that for $K = \mathbb{Q}(\sqrt{5}, \sqrt{13})$, the primes 5 and 13 ramify in different ways: we can see that 5 ramifies in the subfield $\mathbb{Q}(\sqrt{5})$ and is unramified from $\mathbb{Q}(\sqrt{5})$, while 13 is unramified in the subfield $\mathbb{Q}(\sqrt{5})$ and then ramifies from $\mathbb{Q}(\sqrt{5})$ to K. (Additionally, the situation is entirely reversed in the subfield $\mathbb{Q}(\sqrt{13})$.)

0.20 (Oct 21) Ramification and Differents, I

- In order to study ramification in relative extensions, we will need to construct a discriminant associated to an extension L/K.
  - However, we cannot easily adapt the definition we used for the discriminant over $\mathbb{Q}$, since it ultimately relies on the existence of an integral basis of $\mathcal{O}_K$ over $\mathbb{Z}$, but a general extension $\mathcal{O}_L$ over $\mathcal{O}_K$ may not possess an integral basis.
  - We will take an approach involving the construction of a related object known as the different:

- Definition: Let L/K be an extension of number fields. For a fractional ideal A of L, we define its codifferent A^* to be the set $A^* = \{x \in L : \text{tr}_{L/K}(xA) \subseteq \mathcal{O}_K\}$ of all elements of L such that the trace of x times all elements of A lies in $\mathcal{O}_K$ (equivalently, is an algebraic integer).
  - We can see that when A is generated as an $\mathcal{O}_K$-module by $a_1, \dots, a_n$, then $A^* = \{x \in L : \text{tr}_{L/K}(xa_i) \in \mathcal{O}_K \text{ for } 1 \leq i \leq n\}$.
  - Example: For $L = \mathbb{Q}(i)$, $K = \mathbb{Q}$, and $A_1 = \mathbb{Z}[i]$, we see that A_1^* consists of all $x + iy \in \mathbb{Q}(i)$ such that $\text{tr}(x+iy) = 2x$ and $\text{tr}(i(x+iy)) = -2y$ are integral, so that $A_1^* = \frac{1}{2}\mathbb{Z}[i]$. For $A_2 = (1+i)\mathbb{Z}[i]$, we see that A_2^* consists of all $x+iy \in \mathbb{Q}(i)$ such that $\text{tr}((1+i)(x+iy)) = 2(x-y)$ and $\text{tr}((-1+i)(x+iy)) = -2(x+y)$ are integral, so that $A_2^* = \frac{1+i}{4}\mathbb{Z}[i]$.

- Let us establish some basic properties of the codifferent:

- Proposition (Properties of Codifferents): Let L/K be an extension of number fields and A be a nonzero fractional ideal of L/K.

1. The codifferent A^* is a nonzero fractional ideal of L/K.
   - Proof: Suppose $x_1, x_2 \in A^*$, $r \in \mathcal{O}_L$, and $a \in A$. Note then that $ra = b$ is also an element of A.
   - We have $\text{tr}_{L/K}((x_1 + rx_2)a) = \text{tr}_{L/K}(x_1 a) + \text{tr}_{L/K}(x_2 b) \in \mathcal{O}_K$ since both traces are in $\mathcal{O}_K$ by assumption. Therefore, $x_1 + rx_2 \in A^*$ as well, and so since trivially $0 \in A^*$ we see that A^* is an R-submodule of L.
   - To see it is a fractional ideal we must construct some nonzero $d \in \mathcal{O}_L$ with $dA^* \subseteq \mathcal{O}_L$.
   - For this, choose a field basis $\alpha_1, \dots, \alpha_n$ for L/K where each $\alpha_i \in \mathcal{O}_L$, and let b be a nonzero element of $A \cap \mathcal{O}_K$ (e.g., $N_{L/K}$ of a nonzero element in $A \cap \mathcal{O}_L$).

- We claim that the choice $d = b\text{disc}_{L/K}(\alpha_1, \ldots, \alpha_n) = \det[\{\text{tr}_{L/K}(\alpha_i\alpha_j)\}_{1\leq i,j\leq n}]$ works: it is nonzero since the α_i are linearly independent, and is in $\mathcal{O}_L$ since b and the α_i are.
- For any $x \in A^*$, since the α_i are a basis for L/K we may write $x = c_1\alpha_1 + \cdots + c_n\alpha_n$ for some $c_i \in K$. Observe that $b\alpha_i \in A$ for each i and thus $\text{tr}_{L/K}(xb\alpha_i) \in \mathcal{O}_K$ by assumption that $x \in A^*$.
- But now by linearity of the trace we have $\text{tr}_{L/K}(xb\alpha_i) = b\sum_{j=1}^n c_j \text{tr}_{L/K}(\omega_i\omega_j)$ for each i. Solving the resulting system for the c_i using Cramer's rule shows that $c_i = \dfrac{\det(M_i)}{\det(M)}$ where $M = \{\text{tr}_{L/K}(\alpha_i\alpha_j)\}_{1\leq i,j\leq n}$ and M_i is the matrix obtained by replacing the ith column by $\text{tr}_{L/K}(xb\alpha_i)/b$.
- Then $\det(M_i) \in b^{-1}\mathcal{O}_K$ and so $c_i d = c_i b \det(M) \in \mathcal{O}_K$ for each i. Hence $dx = (dc_1)\alpha_1 + \cdots + (dc_n)\alpha_n \in \mathcal{O}_L$, so the given choice of d does work, as claimed.
- Finally, if $A = e^{-1}I$, then $eA \subseteq \mathcal{O}_L$ whence $\text{tr}_{L/K}(eA) \subseteq \mathcal{O}_K$, so $e \in A^*$ yields a nonzero element of A^*.

2. The codifferent A^* satisfies $AA^* = \mathcal{O}_L^*$.
   - Proof: Observe $x \in A^* \iff \text{tr}_{L/K}(xA) \subseteq \mathcal{O}_K \iff \text{tr}_{L/K}(xA\mathcal{O}_L) \subseteq \mathcal{O}_K \iff xA \subseteq \mathcal{O}_L^* \iff x \in A^{-1}\mathcal{O}_L^*$.
   - Thus, $A^* = A^{-1}\mathcal{O}_L$ so $AA^* = \mathcal{O}_L^*$.
   - Exercise: If A is a nonzero fractional ideal of $\mathcal{O}_L$, show that $A^{**} = A$.
3. If I is any nonzero integral ideal of $\mathcal{O}_L$, then $(I^*)^{-1}$ is also an integral ideal of $\mathcal{O}_L$, and in fact it is contained in I.
   - Exercise: Suppose A is a nonzero fractional ideal of $\mathcal{O}_L$. Show that $A^{-1} \subseteq A^*$.
   - Exercise: Suppose A, B are nonzero fractional ideals of $\mathcal{O}_L$. Show that if $A \subseteq B$ then $B^{-1} \subseteq A^{-1}$ and $B^* \subseteq A^*$.
   - Proof: If $I \subseteq \mathcal{O}_L$ by the first exercise above we have $I^{-1} \subseteq I^*$. Then by the second exercise we see $(I^*)^{-1} \subseteq (I^{-1})^{-1} = I$, and so $(I^*)^{-1}$ is an integral ideal of $\mathcal{O}_L$ contained in I.
4. When $K = \mathbb{Q}$, if A has an integral basis $\alpha_1, \ldots, \alpha_n$ with dual basis $\alpha_1^*, \ldots, \alpha_n^*$ (so that $\text{tr}_{L/\mathbb{Q}}(\alpha_i\alpha_j^*) = 0$ for $i \neq j$ and 1 when $i = j$), then $\alpha_1^*, \ldots, \alpha_n^*$ is an integral basis for A^*.
   - As we have previously noted in our earlier discussion of discriminants, the dual basis always exists and can be computed by solving the associated linear system using Cramer's rule.
   - Proof: Let $x \in L$ and $y \in A$. Then there exist unique $x_i \in \mathbb{Q}$ with $x = x_1\alpha_1 + \cdots + x_n\alpha_n$ and unique $y_i \in \mathbb{Z}$ with $y = y_1\alpha_1^* + \cdots + y_n\alpha_n^*$.
   - Then $\text{tr}_{L/\mathbb{Q}}(x\alpha_j^*) = \text{tr}_{L/\mathbb{Q}}(\sum_{i=1}^n x_i\alpha_i\alpha_j^*) = \sum_{i=1}^n x_i \text{tr}_{L/\mathbb{Q}}(\alpha_i\alpha_j^*) = x_j$, so we see $x \in A^*$ if and only if each x_j is an integer.
   - Exercise: In $K = \mathbb{Q}(\sqrt{-5})$, compute a basis of A^* for $A = \mathcal{O}_K$ and for $A = (2, 1 + \sqrt{-5})\mathcal{O}_K$.

- By (1) in the proposition above, we can see there is a relationship between the codifferent A^* and the discriminant.
  - In particular, if we consider the codifferent $\mathcal{O}_L^*$, then since $1 \in \mathcal{O}_L$ we may take $b = 1$ in the argument in (1) to see that $\mathcal{O}_L^* \subseteq d^{-1}\mathcal{O}_L$ where $d = \text{disc}_{L/K}(\alpha_1, \ldots, \alpha_n)$ for any field basis $\alpha_1, \ldots, \alpha_n$ of L/K consisting of algebraic integers.
  - Taking inverses, we see that the inverse codifferent satisfies $(\mathcal{O}_L^*)^{-1} \supseteq (d^{-1}\mathcal{O}_L)^{-1} = d\mathcal{O}_L$.
  - We can see, then, that a somewhat natural candidate for an analogue to the discriminant for the extension L/K would be the ideal $(\mathcal{O}_L^*)^{-1}$, since it contains all of the discriminants $\text{disc}_{L/K}(\alpha_1, \ldots, \alpha_n)$ of n-tuples of algebraic integers in $\mathcal{O}_L$.

- Definition: Let L/K be an extension of number fields. For any nonzero ideal I of $\mathcal{O}_L$, we define the different of I, $D_{L/K}(I)$, to be the ideal $(I^*)^{-1}$, and we define the different of L/K, denoted $D_{L/K}$, to be the ideal $D_{L/K}(\mathcal{O}_L) = (\mathcal{O}_L^*)^{-1}$.
  - Exercise: Show that for any ideal I of $\mathcal{O}_L$, we have $D_{L/K}(I) = D_{L/K} \cdot I$: thus, we may view the notation $D_{L/K}(I)$ as representing a product or a function, interchangeably.
  - We will generally use the $D_{L/K}$ notation for differents instead of the star notation, since the star notation does not indicate the underlying field extension.

- Proposition (Properties of Differents): Let $L/K/F$ be an extension tower of number fields.

  1. The different $D_{L/F}$ equals the product $D_{L/K}D_{K/F}$.
     - Proof: Recall first that for any $\alpha \in L$ we have $\mathrm{tr}_{L/F}(\alpha) = \mathrm{tr}_{K/F}(\mathrm{tr}_{L/K}(\alpha))$.
     - Now let $a \in D_{K/F}^{-1}$ (so that $a \in K$ and $\mathrm{tr}_{K/F}(a\mathcal{O}_K) \subseteq \mathcal{O}_F$) and $b \in D_{L/K}^{-1}$ (so that $b \in L$ and $\mathrm{tr}_{L/K}(b\mathcal{O}_L) \subseteq \mathcal{O}_K$).
     - Then $\mathrm{tr}_{L/F}(ab) = \mathrm{tr}_{K/F}(\mathrm{tr}_{L/K}(ab)) = \mathrm{tr}_{K/F}(a\mathrm{tr}_{L/K}(b)) \in \mathrm{tr}_{K/F}(a\mathcal{O}_K) \subseteq \mathcal{O}_F$.
     - Thus, every element of $D_{L/K}^{-1}D_{K/F}^{-1}$ has trace in $\mathcal{O}_F$, so $D_{L/K}^{-1}D_{K/F}^{-1} \subseteq D_{L/F}^{-1}$ whence $D_{L/F} \subseteq D_{L/K}D_{K/F}$.
     - For the other containment, suppose $c \in D_{L/F}^{-1}$, so that $\mathrm{tr}_{L/F}(c\mathcal{O}_L) \subseteq \mathcal{O}_F$.
     - Then $\mathrm{tr}_{K/F}(\mathrm{tr}_{L/K}(c\mathcal{O}_L)) = \mathrm{tr}_{L/F}(c\mathcal{O}_L) \subseteq \mathcal{O}_F$, so by definition this means $\mathrm{tr}_{L/K}(c\mathcal{O}_L) \subseteq D_{K/F}^{-1}$ hence $D_{K/F}\mathrm{tr}_{L/K}(c\mathcal{O}_L) \subseteq \mathcal{O}_F$ hence $\mathrm{tr}_{L/K}(D_{K/F}c\mathcal{O}_L) \subseteq \mathcal{O}_F \subseteq \mathcal{O}_K$ hence $D_{K/F}c \subseteq D_{L/K}^{-1}$ hence $c \in D_{L/K}^{-1}D_{K/F}^{-1}$.
     - We conclude that $D_{L/F}^{-1} \subseteq D_{L/K}^{-1}D_{K/F}^{-1}$ whence $D_{L/K}D_{K/F} \subseteq D_{L/F}$, so we obtain equality.
  2. If L/K is Galois and $\sigma \in \mathrm{Gal}(L/K)$ is any Galois automorphism, then $\sigma(D_{L/K}) = D_{L/K}$.
     - Proof: For any $x \in \mathcal{O}_L^*$, observe that $\mathrm{tr}_{L/K}(\sigma(x)\mathcal{O}_L) = \mathrm{tr}_{L/K}(x\sigma^{-1}(\mathcal{O}_L)) = \mathrm{tr}_{L/K}(x\mathcal{O}_L) \subseteq \mathcal{O}_K$ and so $\sigma(x) \in \mathcal{O}_L^*$ also.
     - Thus, $\sigma(\mathcal{O}_L^*) \subseteq \mathcal{O}_L^*$. Similarly we see $\sigma^{-1}(\mathcal{O}_L^*) \subseteq \mathcal{O}_L^*$ hence applying σ we see $\mathcal{O}_L^* \subseteq \sigma(\mathcal{O}_L^*)$ so $\mathcal{O}_L^* = \sigma(\mathcal{O}_L^*)$.
     - Finally, since Galois automorphisms clearly commute with taking inverses of fractional ideals, we have $\sigma(D_{L/K}) = \sigma(\mathcal{O}_L^*)^{-1} = [\sigma(\mathcal{O}_L^*)]^{-1} = (\mathcal{O}_L^*)^{-1} = D_{L/K}$.
  3. For any ideals I of $\mathcal{O}_K$ and J of $\mathcal{O}_L$, we have $\mathrm{tr}_{L/K}(J) \subseteq I$ if and only if $J \subseteq D_{L/K}^{-1}I$.
     - Proof: Observe $\mathrm{tr}_{L/K}(J) \subseteq I \iff I^{-1}\mathrm{tr}_{L/K}(J) \subseteq \mathcal{O}_K \iff \mathrm{tr}_{L/K}(I^{-1}J) \subseteq \mathcal{O}_K \iff I^{-1}J \subseteq D_{L/K}^{-1} \iff J \subseteq D_{L/K}^{-1}I$.
  4. We have $N_{K/\mathbb{Q}}(D_{K/\mathbb{Q}}) = |\mathrm{disc}(K)|$.
     - Exercise: Suppose $\alpha_1, \ldots, \alpha_n$ is a basis of $K/\mathbb{Q}$ with dual basis $\alpha_1^*, \ldots, \alpha_n^*$. Show that $\mathrm{disc}(\alpha_1^*, \ldots, \alpha_n^*) = \mathrm{disc}(\alpha_1, \ldots, \alpha_n)^{-1}$. [Hint: Show that the product of the matrices $\{\sigma_i(\alpha_j)\}_{1\le i,j\le n}$ and the transpose of $\{\sigma_i(\alpha_j^*)\}_{1\le i,j\le n}$ is the identity matrix.]
     - Proof: Let $\alpha_1, \ldots, \alpha_n$ be an integral basis of $\mathcal{O}_K$ with dual basis $\alpha_1^*, \ldots, \alpha_n^*$, which by (4) of our previous proposition we know is an integral basis for $\mathcal{O}_K^* = D_{K/\mathbb{Q}}^{-1}$.
     - Let m be a positive integer such that $m\alpha_1^*, \ldots, m\alpha_n^*$ are all integers, and consider the ideal $I = mD_{K/\mathbb{Q}}^{-1}$ of $\mathcal{O}_K$; then $D_{K/\mathbb{Q}}^{-1} = m^{-1}I$.
     - By properties of ideal norms and the exercise above, we have $N_{K/\mathbb{Q}}(D_{K/\mathbb{Q}})^2 = \dfrac{N_{K/\mathbb{Q}}(m)^2}{N_{K/\mathbb{Q}}(I)^2} = \dfrac{|\mathrm{disc}(K)|\, m^{2n}}{\mathrm{disc}_{K/\mathbb{Q}}(m\alpha_1^*, \ldots, m\alpha_n^*)} = \dfrac{|\mathrm{disc}(K)|}{\mathrm{disc}_{K/\mathbb{Q}}(\alpha_1^*, \ldots, \alpha_n^*)} = \mathrm{disc}_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)\,|\mathrm{disc}(K)| = |\mathrm{disc}(K)|^2$.
     - Rearranging and taking the square root then yields $N_{K/\mathbb{Q}}(D_{K/\mathbb{Q}}) = |\mathrm{disc}(K)|$ immediately.
  5. For any extension L/K of number fields, $\mathrm{disc}(K)^{[L:K]}$ divides $\mathrm{disc}(L)$.
     - Proof: By (1) with $F = \mathbb{Q}$, we have $D_{L/\mathbb{Q}} = D_{L/K}D_{K/\mathbb{Q}}$. Taking norms yields $N_{L/\mathbb{Q}}(D_{L/\mathbb{Q}}) = N_{L/\mathbb{Q}}(D_{L/K})N_{L/\mathbb{Q}}(D_{K/\mathbb{Q}}) = N_{L/\mathbb{Q}}(D_{L/K})N_{K/\mathbb{Q}}(D_{K/\mathbb{Q}})^{[L:K]}$.
     - Now applying (4) yields $\mathrm{disc}\, L = \pm N_{L/\mathbb{Q}}(D_{L/K})(\mathrm{disc}\, K)^{[L:K]}$, so $\mathrm{disc}(K)^{[L:K]}$ divides $\mathrm{disc}(L)$.
  6. Suppose that $L = K(\alpha)$ for a generator $\alpha \in \mathcal{O}_L$ and let $m(x) \in \mathcal{O}_K[x]$ be the minimal polynomial of α over K. For the (fractional) ideal $A = \mathcal{O}_K[\alpha] = \mathcal{O}_K \oplus \mathcal{O}_K\alpha \oplus \cdots \oplus \mathcal{O}_K\alpha^{n-1}$ where $n = [L : K]$, we have $A^* = \dfrac{1}{m'(\alpha)}A$.
     - Proof: Let $r_1, \ldots, r_n$ be the various complex embeddings of α. Since $m(x) = \prod_{i=1}^n (x - r_i)$, differentiating and setting $x = r_i$ yields $m'(r_j) = \prod_{i\ne j}(r_j - r_i) = \dfrac{m(x)}{x - r_j}\Big|_{x=r_j}$.

- Thus, the polynomial $\frac{1}{m'(r_j)}\frac{m(x)}{x-r_j}$ evaluates to 1 when $x = r_j$ and (clearly) to 0 when x is equal to any other r_i.
- Multiplying by r_j^{k+1} and then summing over j then shows that the polynomial $\sum_{j=1}^n \frac{r_j^{k+1}}{m'(r_j)}\frac{m(x)}{x-r_j}$ evaluates to r_j^{k+1} for each $1 \leq j \leq n$. But the same is true for the polynomial x^{k+1} for $1 \leq k \leq n-2$, and therefore since each polynomial has degree at most $n-1$, they must be equal. For $k = n-1$ we can see that the same statement holds for $x^n - m(x)$ in place of x^n.
- We conclude that $\sum_{j=1}^n \frac{r_j^{k+1}}{m'(r_j)}\frac{m(x)}{x-r_j} = \begin{cases} x^{k+1} & \text{for } 0 \leq k \leq n-2 \\ x^n - m(x) & \text{for } k = n-1 \end{cases}$.
- Setting $x = 0$, we see $\mathrm{tr}_{L/K}(\frac{\alpha^k}{m'(\alpha)}) = \sum_{j=1}^n \frac{r_j^k}{m'(r_j)} = -\frac{1}{m(0)}\sum_{j=1}^n \frac{r_j^{k+1}}{m'(r_j)}\frac{m(0)}{-r_j} = \begin{cases} 0 & \text{for } 0 \leq k \leq n-2 \\ 1 & \text{for } k = n-1 \end{cases}$.
  Therefore, $\frac{\alpha^k}{m'(\alpha)} \in A^*$ for each $1 \leq k \leq n-1$. Hence $\frac{1}{m'(\alpha)}A \subseteq A^*$.
- Conversely, suppose $b \in A^*$, and suppose $m(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0$. Then for $p(x) = \sum_{i=1}^n b_i \frac{m(x)}{x-r_i}$ where b_i is the ith complex embedding of b, we see from the calculations above that $p(x) = \sum_{j=1}^n c_j \sum_{k=0}^{j-1} x^k \mathrm{tr}_{L/K}(b\alpha^{j-k-1})$.
- Since $b \in A^*$ each of the traces is in $\mathcal{O}_K$, so $p(x) \in \mathcal{O}_K[x]$. Then $bm'(\alpha) = p(\alpha) \in A$ so $b \in \frac{1}{m'(\alpha)}A$. This means $A^* \subseteq \frac{1}{m(\alpha)}A$, so we get equality as claimed.

7. Suppose that $L = K(\alpha)$ for a generator $\alpha \in \mathcal{O}_L$ with minimal polynomial $m(x)$. Then $m'(\alpha) \in D_{L/K}$.
   - Proof: Letting $A = \mathcal{O}_K[\alpha]$, since $A \subseteq \mathcal{O}_L$ we see $\mathcal{O}_L^* \subseteq A^*$, which is to say, $d_{L/K}^{-1} \subseteq A^*$.
   - By (6) we have $A^* = \frac{1}{m'(\alpha)}A$ hence $d_{L/K}^{-1} \subseteq \frac{1}{m'(\alpha)}A$ hence $m'(\alpha) \in d_{L/K}A \subseteq d_{L/K}$.

0.21 (Oct 23) Ramification and Differents, II

- We can see from (6) and (7) in the proposition above that there is an interesting connection between the different and derivatives.
  - In fact, differents are quite closely tied to the general notion of a derivation in a commutative ring, but giving a full discussion of this topic would take us somewhat far afield, so we will just give a brief summary.
- Definition: Let R be a commutative ring with 1 and M be an R-module. A derivation is a function $d : R \to M$ of additive groups such that $d(r+s) = d(r) + d(s)$ and $d(rs) = rd(s) + sd(r)$ for all $r, s \in R$.
  - In other words, a derivation is an additive function that also obeys the Leibniz formula for the product rule.
  - Example: For any commutative ring R, the usual derivative map $D : R[x] \to R[x]$ with $D(f(x)) = f'(x)$ is a derivation.
  - Exercise: Suppose R is a subring of S and $d : S \to M$ is a derivation such that $d(r) = 0$ for all $r \in R$. Prove the "chain rule" for polynomials: for any $p(x) \in R[x]$ and any $a \in S$, show that $d(p(a)) = p'(a)d(a)$ where p' is the usual formal derivative of p.
  - When S is also a ring, a derivation $d : R \to S$ is essential when the image $d(R)$ contains an element that is not a zero divisor of S.
- Theorem (Derivations and Differents): Let L/K be an extension of number fields. If I is an ideal of $\mathcal{O}_L$, then I divides the different $D_{L/K}$ if and only if there exists an essential derivation $d : S \to S/I$ vanishing on $\mathcal{O}_K$.
  - We will not prove this theorem, as the details are rather technical and not especially enlightening.

- Our main result is the close connection between the different and ramified primes:
- Theorem (Differents and Ramification): Let L/K be an extension of number fields, and let Q be a nonzero prime ideal of $\mathcal{O}_L$ lying over the prime ideal P of $\mathcal{O}_K$, lying over the integer prime p.

  1. The power $Q^{e(Q|P)-1}$ divides the different $D_{L/K}$.
     - Proof: Let $\hat{L}$ be the Galois closure of L/K and let $\sigma_1, \ldots, \sigma_n$ be the complex embeddings of L, viewed as elements of $\mathrm{Gal}(\hat{L}/L)$.
     - Also let $P\mathcal{O}_L = Q^{e(Q|P)}I$, where by definition Q does not divide I.
     - Let $x \in QI$ and take N such that p^N exceeds the ramification index of any prime ideal dividing $P\mathcal{O}_L$. Then we have $x^{p^N} \in (QI)^{p^N} \subseteq P$.
     - Applying σ_i yields $\sigma_i(x)^{p^N} \subseteq \sigma(P\mathcal{O}_K) = P$, and now summing over i shows $\mathrm{tr}_{L/K}(x^{p^N}) \in P$.
     - Then $\mathrm{tr}_{L/K}(x)^{p^N} = [\sum_{i=1}^n \sigma_i(x)]^{p^N} \equiv \sum_{i=1}^n \sigma_i(x^{p^n}) = \mathrm{tr}_{L/K}(x^{p^N}) \pmod{P\mathcal{O}_L}$ since the p^Nth power map is additive in characteristic p. But since both elements are in $\mathcal{O}_K$, the congruence also holds modulo P.
     - Thus, we see that $\mathrm{tr}_{L/K}(x)^{p^N} \in P$. But since P is a prime ideal, that means $\mathrm{tr}_{L/K}(x) \in P$.
     - This means $\mathrm{tr}_{L/K}(QI) \subseteq P$, so by properties of the different, that implies $QI \subseteq D_{L/K}^{-1}P$ hence $D_{L/K}QI \subseteq P$ hence $P = Q^{e(Q|P)}I$ divides $D_{L/K}QI$ hence $Q^{e(Q|P)-1}$ divides $D_{L/K}$, as claimed.
  2. If Q is tame (so that p does not divide $e(Q|P)$), then $Q^{e(Q|P)}$ does not divide the different $D_{L/K}$.
     - Exercise: Let Q be a nonzero prime ideal of $\mathcal{O}_L$. Show that the zero divisors in $\mathcal{O}_L/Q^e$ are the elements of Q/Q^e.
     - Proof: Suppose p does not divide $e = e(Q|P)$ and let $d : \mathcal{O}_L \to \mathcal{O}_L/Q^e$ be a derivation.
     - By the previous theorem, the claimed result is then equivalent to saying that $d(x)$ is a zero divisor (or zero) for all $x \in \mathcal{O}_L$.
     - Let $\pi \in P \backslash P^2$ and $\Pi \in Q \backslash Q^2$. Then the prime factorization of the fractional ideal $A = (\Pi^{-e}\pi)$ has no factors of Q, so $A = b^{-1}I$ for some $b \notin Q$ and some I not divisible by Q, and thus letting $a = b\Pi^{-e}\pi$ we see that $a, b \in \mathcal{O}_L \backslash Q$ and $\pi = \Pi^e a/b$.
     - Now we have $0 = \pi d(b) + bd(\pi) = d(\pi b) = d(\Pi^e a) = e\Pi^{e-1}d(\Pi)a$ modulo Q^e, so since none of e, Π^{e-1}, or a are zero modulo Q^e (here we use the fact that p does not divide e), that means $d(\Pi)$ is a zero divisor (or zero) in $\mathcal{O}_L/Q^e$.
     - Since the only zero divisors in $\mathcal{O}_L/Q^e$ are the elements of Q/Q^e that means $d(\Pi) \in Q/Q^e$.
     - Now if $x \in \mathcal{O}_L$ has $x \in Q$, then using a similar argument as for π above, there exist $r, s \in \mathcal{O}_L$ and s not in Q such that $x = \Pi r/s$: then $sd(x) + xd(s) = d(sx) = d(\Pi r) = rd(\Pi) + \Pi d(r) \in Q/Q^e$.
     - But since $xd(s) \in Q/Q^e$, this means $sd(x) \in Q/Q^e$ and hence since $s \notin Q$ that means $d(x) \in Q/Q^e$, so it is a zero divisor.
     - Finally, if $x \notin Q$, then by Lagrange's theorem in $\mathcal{O}_L/Q$ we know that $x^{N(Q)-1} \equiv 1 \pmod{Q}$, so $x^{N(Q)-1} = 1 + t$ for some $t \in Q$.
     - Then $d(t) = d(1+t) = d(x^{N(Q)-1}) = (N(Q)-1)x^{N(Q)-1}d(x)$ and since $N(Q)$ is divisible by p, neither $N(Q)-1$ nor $x^{N(Q)-1}$ is zero modulo Q, so we must have $d(x) \in Q/Q^e$ and so $d(x)$ is again a zero divisor.
  3. For any prime ideal Q of $\mathcal{O}_L$, the exact power of Q dividing the different $D_{L/K}$ is $\geq e(Q|P) - 1$, and equality holds if Q is tame (i.e., tamely ramified or unramified).
     - Proof: Immediate from (1) and (2), along with the observation that if Q is wildly ramified, then $e(Q|P)$ is divisible by p hence $e(Q|P) - 1 > 1$.
     - Remark: We will later be able to give a formula for the power of Q dividing the different when Q is wildly ramified as well.
  4. There are only finitely many prime ideals of $\mathcal{O}_L$ that are ramified in L/K, and they are precisely the prime ideal factors of the different $D_{L/K}$.
     - Proof: By (3), we see that Q divides the different if and only if $e(Q|P) > 1$, which is to say when Q is ramified. Since the different has only finitely many prime ideal factors, there are only finitely many ramified primes.

5. For an extension $K/\mathbb{Q}$, an integer prime p is ramified if and only if p divides $\text{disc}(K)$.
    - Proof: Immediate from (4) and the different norm formula $N_{K/\mathbb{Q}}(D_{K/\mathbb{Q}}) = |\text{disc}(K)|$.

- As an application of the different, we can show that there exist unramified field extensions (i.e., field extensions with no ramified primes).
    - Exercise: Show that L/K is unramified if and only if $\text{disc}(L) = \pm\text{disc}(K)^{[L:K]}$.
- Example: Show that the extension $\mathbb{Q}(\sqrt{5}, \sqrt{13})/\mathbb{Q}(\sqrt{65})$ is unramified.
    - Letting $L = \mathbb{Q}(\sqrt{5}, \sqrt{13})$ and $K = \mathbb{Q}(\sqrt{65})$, we see $L = K(\sqrt{5}) = K(\sqrt{13})$.
    - The different $D_{L/K}$, by our results, contains $m'(\alpha)$ for any $\alpha \in \mathcal{O}_L$ generating L/K.
    - Taking $\alpha = \frac{1+\sqrt{5}}{2}$ with minimal polynomial $x^2 - x - 1$ shows $\sqrt{5} \in D_{L/K}$ and taking $\alpha = \frac{1+\sqrt{13}}{2}$ with minimal polynomial $x^2 - x - 3$ shows that $2\alpha - 1 = \sqrt{13} \in D_{L/K}$.
    - But the ideal generated by $\sqrt{5}$ and $\sqrt{13}$ is all of $\mathcal{O}_L$ since it contains 5 and 13 hence also their integer gcd 1. Thus, $D_{L/K} = \mathcal{O}_L$, and so by our results above, that means no primes ramify in the extension L/K.
    - Alternatively, using the discriminant, we can compute that $\text{disc}(L) = 5^2 13^2$ using an integral basis to see that the only primes that ramify in $L/\mathbb{Q}$ are 5 and 13, so these are the only possible primes that could ramify in L/K.
    - But then we can just check directly using Dedekind-Kummer that neither 5 nor 13 ramifies in L/K, and so L/K is unramified.
    - Even if we did not have an integral basis for $\mathcal{O}_L$ already computed, we could just find the discriminant of an element of $\mathcal{O}_L$ generating $L/\mathbb{Q}$, which would at worst add finitely many extra primes to check.
- Exercise: Show that the extension $\mathbb{Q}(\sqrt{-3}, \sqrt{5})/\mathbb{Q}(\sqrt{-15})$ is unramified.
- Exercise: Let $\alpha^3 - \alpha - 1 = 0$. Show that the extension $\mathbb{Q}(\alpha, \sqrt{-23})/\mathbb{Q}(\sqrt{-23})$ is unramified.

0.22 (Oct 24) The Ideal Class Group

- Now that we have a better understanding of prime ideal factorizations and how to compute them, and about ramification, let us return to study the question of unique factorization once more.
    - As we have already discussed, a Dedekind domain is a unique factorization domain if and only if it is a principal ideal domain, and thus any examples of non-unique factorization of elements necessarily arise from nonprincipal ideals.
    - We would now like to quantify more precisely how "non-unique" the non-unique factorization of elements in a Dedekind domain can be.
    - As motivation let us again consider $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, which we have shown not to be a PID by constructing various nonprincipal ideals $I_2 = (2, 1+\sqrt{-5})$, $I_3 = (3, 1+\sqrt{-5})$, $I_3' = (3, 1-\sqrt{-5})$, $I_7 = (7, 3+\sqrt{-5})$, and $I_7' = (7, 3-\sqrt{-5})$.
    - If we compute the products of various pairs of these nonprincipal ideals, however, we will quickly discover that the products always end up being principal. Explicitly, here are various such calculations (note that to find potential generators for the ideal products, we can search for elements of the appropriate norm):
        * $I_2^2 = (2)$, $I_3 I_3' = (3)$, and $I_7 I_7' = (7)$ by Dedekind-Kummer.
        * $I_2 I_3 = (1+\sqrt{-5})$ since $I_2 I_3 = I_2 \cap I_3 \supseteq (1+\sqrt{-5})$ but $N(I_2 I_3) = 6 = N(1+\sqrt{-5})$.
        * $I_2 I_3' = (1-\sqrt{-5})$ by conjugating the calculation above.
        * $I_3^2 = (9, 3+3\sqrt{-5}, -4+2\sqrt{-5}) = (2-\sqrt{-5})$ since $2-\sqrt{-5}$ is in this ideal since $2-\sqrt{-5} = 9 - (3+3\sqrt{-5}) + (-4+2\sqrt{-5})$, and $N(I_3^2) = 9 = N(2-\sqrt{-5})$.
        * $(I_3')^2 = (2+\sqrt{-5})$ by conjugating the calculation above.
        * $I_2 I_7 = (14, 6+2\sqrt{-5}, 7+7\sqrt{-5}, -2+4\sqrt{-5}) = (3+\sqrt{-5})$ since $3+\sqrt{-5}$ is in this ideal since $3+\sqrt{-5} = 2(6+2\sqrt{-5}) - (7+7\sqrt{-5}) - (-2+4\sqrt{-5})$, and $N(I_2 I_7) = 14 = N(3+\sqrt{-5})$.

* $I_2 I_7' = (3 - \sqrt{-5})$ by conjugating the calculation above.
* $I_3 I_7 = (21, 9 + 3\sqrt{-5}, 7 + 7\sqrt{-5}, -1 + 4\sqrt{-5}) = (1 - 2\sqrt{-5})$ since $1 - 2\sqrt{-5} = 21 - 3(9 + 3\sqrt{-5}) + (7 + 7\sqrt{-5})$ and $N(I_3 I_7) = 21 = N(1 - 2\sqrt{-5})$.
* $I_3 I_7' = (21, 9 - 3\sqrt{-5}, 7 + 7\sqrt{-5}, 8 + 2\sqrt{-5}) = (4 + \sqrt{-5})$ since $4 + \sqrt{-5} = 21 + (7 + 7\sqrt{-5}) - 3(8 + 2\sqrt{-5})$ and $N(I_3 I_7') = 21 = N(4 + \sqrt{-5})$.
* $I_3' I_7 = (4 - \sqrt{-5})$ and $I_3' I_7' = (1 + 2\sqrt{-5})$ by conjugating the calculations above.

- These calculations suggest that there might actually be only one "class" of nonprincipal ideal in $\mathbb{Z}[\sqrt{-5}]$, up to an appropriate notion of equivalence of ideals.
- We would like to declare that two ideals are equivalent if they differ by a principal ideal factor. We can formulate an equivalence relation in this manner, but it is more natural to work instead with fractional ideals rather than integral ideals, since the invertible fractional ideals form a group, rather than merely a semigroup.

- Definition: Let R be a Dedekind domain and let J_R denote the multiplicative group of nonzero fractional ideals of R. A fractional ideal A of R is principal when it is of the form $A = d^{-1} I$ for a principal ideal I of R. It is easy to see that the nonzero principal fractional ideals form a subgroup P_R of the group of nonzero fractional ideals: we define the ideal class group $\mathrm{cl}(R)$ to be the quotient group J_R / P_R of invertible fractional ideals modulo principal fractional ideals.

  - We remark that the class group can be defined for any integral domain R in the same manner (namely, as the quotient group of invertible fractional ideals modulo principal fractional ideals), but for rings that are not Dedekind domains, there can exist non-invertible fractional ideals, whose behavior is then not accounted for by the class group.
  - Exercise: For a Dedekind domain R with fraction field K, show that the sequence of multiplicative groups $1 \to \mathcal{O}_K^* \hookrightarrow K^* \stackrel{a \mapsto aR}{\to} J_R \to \mathrm{cl}(R) \to 1$ is exact. (It is analogous to, and in fact generalizes, the exact sequence $1 \to k^* \hookrightarrow k(C)^* \stackrel{f \mapsto \mathrm{div}(f)}{\to} \mathrm{Div}^0(C) \to \mathrm{Pic}^0(C) \to 1$ for an algebraic curve C defined over an algebraically closed field k.)
  - For integral ideals I and J, we can see that (the images of) I and J are equivalent in the class group $\iff$ IJ^{-1} is a principal fractional ideal $\iff$ there exist nonzero $\alpha, \beta \in R$ such that $IJ^{-1} = \alpha^{-1}(\beta)$ $\iff$ there exist nonzero $\alpha, \beta \in R$ such that $(\alpha) I = (\beta) J$.
  - We therefore see that equivalence in the class group precisely captures our desired notion of equivalence of ideals up to principal factors.
  - Inversely, this equivalence relation on integral ideals does capture the full structure of the class group of fractional ideals as well (intuitively, we can just clear denominators when working with fractional ideals to convert statements to ones about integral ideals). Explicitly:
  - Exercise: For ideals I and J of a Dedekind domain R, write $I \sim J$ when there exist nonzero $\alpha, \beta \in R$ with $(\alpha) I = (\beta) J$.
    1. Show that $\sim$ is an equivalence relation on the ideals of R.
    2. Show that the multiplication operation $[I][J] = [IJ]$ on equivalence classes is well defined and gives the nonzero equivalence classes the structure of an abelian group G.
    3. Show that the map $\varphi : G \to \mathrm{cl}(R)$ given by $\varphi([I]) = \overline{I}$, where $\overline{I}$ denotes the image of I in the class group J_R / P_R, is well defined and an isomorphism.
  - Exercise: With the equivalence relation $\sim$ on ideals as given in the exercise above, show that $I \sim J$ if and only if I is isomorphic to J as an R-module. (Thus, the isomorphism classes of ideals are the same as the equivalence classes in the class group, yielding a third natural way to "discover" the class group.)
  - We can see that the trivial class in the class group consists of the principal (fractional) ideals, and therefore R is a principal ideal domain if and only if its class group is trivial.
  - Nontrivial classes in the class group correspond to inequivalent classes of nonprincipal ideals, and so we see that the class group gives a more precise way of measuring how badly R fails to have unique factorization of elements.

- For an arbitrary Dedekind domain, the class group can be infinite: in fact, it is a theorem of Claborn that for any abelian group G whatsoever, there exists a Dedekind domain whose class group is isomorphic to G.

- However, when $R = \mathcal{O}_K$ is the ring of integers of a number field K, the class group is always finite:

- Proposition (Finiteness of the Class Group): Suppose K is a number field of degree n over $\mathbb{Q}$ with complex embeddings $\sigma_1, \ldots, \sigma_n$. Let $\beta_1, \ldots, \beta_n$ be an integral basis of $\mathcal{O}_K$, and define the constant $c_K = \prod_{i=1}^{n} \left[\sum_{j=1}^{n} |\sigma_i(\beta_j)|\right]$.

  1. If I is a nonzero ideal of $\mathcal{O}_K$, then I contains a nonzero element α such that $|N(\alpha)| \leq c_K N(I)$.
     - Proof: Suppose K has degree n over $\mathbb{Q}$ and pick any integral basis $\beta_1, \ldots, \beta_n$ for $\mathcal{O}_K$. Also let $m = \lfloor N(I)^{1/n} \rfloor$, so that $m^n \leq N(I) < (m+1)^n$.
     - Then since the cardinality of R/I is $N(I) < (m+1)^n$, by the pigeonhole principle at least two of the $(m+1)^n$ elements $\{a_1\beta_1 + \cdots + a_n\beta_n : 0 \leq a, b \leq m\}$ in R must be congruent modulo I, so their difference is in I.
     - Thus, there exists a nonzero element $\alpha \in I$ of the form $\alpha = a_1\beta_1 + \cdots + a_n\beta_n$ where $-m \leq a_i \leq m$ for each i. By the triangle inequality we see $|N(\alpha)| = \prod_{i=1}^{n} |\sigma_i(\alpha)| \leq \prod_{i=1}^{n} \left[\sum_{j=1}^{n} |a_i| \cdot |\sigma_i(\beta_j)|\right] \leq m^n \cdot \prod_{i=1}^{n} \left[\sum_{j=1}^{n} |\sigma_i(\beta_j)|\right] \leq N(I) \cdot c_K$, as claimed.
  2. Every ideal class of $\mathcal{O}_K$ contains an ideal J such that $N(J) \leq c_K$.
     - Proof: Let $\mathcal{C}$ be an ideal class and let I be any ideal in the inverse class $\mathcal{C}^{-1}$.
     - By (1), there exists a nonzero element $\alpha \in I$ such that $N(\alpha) \leq c_K N(I)$. Because $\alpha \in I$, by the equivalence of divisibility and containment we see that I divides (α) and so $(\alpha) = IJ$ for some ideal J.
     - Taking norms yields $N(\alpha) = N(I)N(J)$, so $N(J) = \dfrac{N(\alpha)}{N(I)} \leq c_K$. Finally, taking ideal classes gives $[1] = [(\alpha)] = [I][J]$ so $J \in [I]^{-1} = (\mathcal{C}^{-1})^{-1} = \mathcal{C}$, as required.
  3. The ideal class group of $\mathcal{O}_K$ is finite.
     - Proof: By (2), every ideal class contains some ideal J with $N(J) \leq c_K$.
     - But there are only finitely many possible ideals J with $N(J) \leq c_K$: there are only finitely many possible prime ideals that could occur in the prime factorization of J (namely, the primes of norm at most c_K) and the power to which each such ideal can occur is bounded (since a prime power P^a has norm $N(P)^a$, we must have $a \leq \log_{N(P)} c_K \leq \log_p C_K$ for all such P lying over $p \in \mathbb{Z}$).
     - Thus, we have a finite list of ideals representing all ideal classes, so there are finitely many ideal classes.

- Exercise: Let L/K be an extension of number fields. Use the fact that the class group of $\mathcal{O}_K$ is finite to give another proof that $N_L(I\mathcal{O}_K) = N_K(I)^{[L:K]}$ for any ideal I of $\mathcal{O}_K$. [Hint: What can be said about $I^{h(K)}$?]

- This result is already enough to allow us to compute class groups in some cases.

  - When $K = \mathbb{Q}(\sqrt{D})$, when $D \equiv 2, 3 \pmod 4$ using the integral basis $\{1, \sqrt{D}\}$ we obtain $c_K = (1+\sqrt{D})^2$. In fact, we can do slightly better just by estimating $\left|N(a+b\sqrt{D})\right| = \left|a^2 - Db^2\right| \leq a^2 + Db^2 \leq m^2(1+D)$ to obtain $c_K = 1 + D$.

- Definition: If K is a number field, the class number of K is the order of the ideal class group of $\mathcal{O}_K$. The class number is often written as $h(K)$.

  - As we noted earlier, the class number of $\mathcal{O}_K$ is equal to 1 if and only if $\mathcal{O}_K$ is a principal ideal domain. A larger class number corresponds to having more inequivalent types of non-unique factorizations.
  - Our proof of (2) in the proposition above gives us an explicit way to calculate the ideal class group of $\mathcal{O}_K$: we need only compute all of the possible prime ideals having norm at most c_K, and then determine the resulting structure of these ideals under multiplication.

- Example: Show that the class group of $K = \mathbb{Q}(\sqrt{2})$ is trivial.

  - From the proposition, we know that any ideal class contains an ideal J of norm at most 3.

- Then the only possible prime divisors of the norm are 2 and 3, so the only possible prime ideal divisors of J are the primes lying above 2 and 3.
- Using the Dedekind-Kummer factorization theorem shows that in $\mathbb{Z}[\sqrt{2}]$ we have $(2) = (\sqrt{2})^2$ while the ideal (3) is inert and has norm 9, so the only possible ideals J are (1) of norm 1 and $(\sqrt{2})$ of norm 2.
- Since both of these ideals are principal, we conclude that every ideal of $\mathbb{Z}[\sqrt{2}]$ is principal and so the class group is trivial (so that $\mathbb{Z}[\sqrt{2}]$ is a principal ideal domain).

- Example: Show that the class group of $K = \mathbb{Q}(\sqrt{-5})$ has order 2.
  - From the proposition, we know that any ideal class contains an ideal J of norm at most 6.
  - Then the only possible prime divisors of the norm are 2, 3, and 5 so the only possible prime ideal divisors of J are the primes lying above 2, 3, and 5.
  - We have already computed the factorizations $(2) = (2, 1+\sqrt{-5})^2$, $(3) = (3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$, and $(5) = (\sqrt{-5})^2$.
  - Thus, the possible prime ideals dividing J are $I_2 = (2, 1+\sqrt{-5})$ of norm 2, $I_3 = (3, 1+\sqrt{-5})$ and $I_3' = (3, 1-\sqrt{-5})$ both of norm 3, and $I_5 = (\sqrt{-5})$ of norm 5.
  - As we have previously shown, the ideal I_2 is not principal, so since $I_2^2 = (2)$ we see that $[I_2]$ is an element of order 2 in the class group.
  - We have also previously shown that $I_2 I_3 = (1+\sqrt{-5})$, so $[I_3] = [I_2]^{-1} = [I_2]$, and then since $I_3 I_3' = (3)$ we see $[I_3'] = [I_2]$ as well.
  - Thus, since I_5 is principal, we see that all of the nonprincipal ideals lie in the same class (namely, the class $[I_2]$) and so the class group of $\mathbb{Z}[\sqrt{-5}]$ has order 2.

0.23 (Oct 28) Real and Complex Embeddings, Minkowski's Lattice Theorems

- Our ability to make effective class group calculations, like the ones above, requires being able to get a good estimate on the norm of the smallest nonzero element in a nonzero ideal I.
  - Saying that an element $\alpha \in I$ has small norm is the same as saying that the product of the absolute values of the various complex embeddings $\sigma_1, \ldots, \sigma_n$ of α is small.
  - So let us make some brief observations about the complex embeddings of K first.

- Definition: If K is a number field and $\sigma : K \to \mathbb{C}$ is an embedding of K, we say σ is a real embedding if the image of σ lies inside $\mathbb{R}$, and otherwise we say σ is an imaginary embedding (or nonreal embedding).
  - If τ is a nonreal embedding, then $\overline{\tau}$ is also a nonreal embedding distinct from τ, so the nonreal embeddings come in conjugate pairs.
  - Often the term "complex embedding" is used to refer specifically to the nonreal embeddings, though we have been using the term "complex embedding" to refer to any embedding, real or complex.

- Definition: If K is a number field with r real embeddings and $2s$ nonreal embeddings, the signature of K is the ordered pair (r, s). Note that if K has degree n over $\mathbb{Q}$, then $r + 2s = n$. A number field with $s = 0$ is totally real (all its embeddings are real) while a number field with $r = 0$ is totally complex (all its embeddings are nonreal).
  - Example: The real quadratic fields $\mathbb{Q}(\sqrt{D})$ for $D > 0$ are totally real and have signature $(2, 0)$, while the imaginary quadratic fields $\mathbb{Q}(\sqrt{D})$ for $D < 0$ are totally complex and have signature $(0, 1)$.
  - Example: The field $\mathbb{Q}(\sqrt[3]{n})$ for any cubefree integer n has signature $(1, 1)$ since the minimal polynomial $x^3 - n$ has one real root and two nonreal roots.
  - More generally, for $K = \mathbb{Q}(\alpha)$, if the minimal polynomial $m(x)$ of α has r real roots and $2s$ pairs of complex conjugate roots, then K has signature (r, s).
  - Exercise: Show that if $K/\mathbb{Q}$ is Galois, then K must be totally real or totally imaginary.

- Exercise: Show that if K has signature (r, s), then the sign of $\mathrm{disc}(K)$ is $(-1)^s$. [Hint: What does complex conjugation do to the discriminant matrix?]
- Now suppose K has r real embeddings $\sigma_1, \ldots, \sigma_r$ and $2s$ complex embeddings $\tau_1, \overline{\tau_1}, \ldots, \tau_s, \overline{\tau_s}$, where $r + 2s = n$.
- We would like to consider all of the complex embeddings of a given element $\alpha \in K$ together. To do this we only need the values of half of the complex embeddings, since the other half are their complex conjugates.
- This suggests we should use the natural map $\varphi : K \to \mathbb{R}^r \times \mathbb{C}^s$ via $\varphi(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_r(\alpha), \tau_1(\alpha), \ldots, \tau_s(\alpha))$, which is not only an additive group homomorphism but also a $\mathbb{Q}$-linear transformation.
- By decomposing the copies of $\mathbb{C}$ into real and imaginary parts we may equivalently view φ as a homomorphism $\varphi : K \to \mathbb{R}^n$, which in many cases will be more convenient for us:

- Definition: If K is a number field with r real embeddings and $2s$ nonreal embeddings, the Minkowski embedding is the $\mathbb{Q}$-linear map $\varphi : K \to \mathbb{R}^n$ defined by $\varphi(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_r(\alpha), \mathrm{Re}[\tau_1(\alpha)], \mathrm{Im}[\tau_1(\alpha)], \ldots, \mathrm{Re}[\tau_s(\alpha)], \mathrm{Im}[\tau_s(\alpha)])$.
  - Example: For $K = \mathbb{Q}(\sqrt{D})$ with $D > 0$, the Minkowski map is $\varphi(a + b\sqrt{D}) = (a + b\sqrt{D}, a - b\sqrt{D})$.
  - Example: For $K = \mathbb{Q}(\sqrt{D})$ with $D < 0$, the Minkowski map is $\varphi(a + b\sqrt{D}) = (a, b\sqrt{|D|})$.
  - Example: For $K = \mathbb{Q}(D^{1/3})$, the Minkowski map is $\varphi(a + bD^{1/3} + cD^{2/3}) = (a + bD^{1/3} + cD^{2/3}, a - \frac{1}{2}bD^{1/3} - \frac{1}{2}cD^{2/3}, \frac{\sqrt{3}}{2}bD^{1/3} - \frac{\sqrt{3}}{2}cD^{2/3})$.
  - Clearly $\ker \varphi = 0$ so φ is injective (thus justifying our use of the word "embedding").
  - Thus, if we choose any $\mathbb{Q}$-basis $\alpha_1, \ldots, \alpha_n$ of K, then by $\mathbb{Q}$-linearity the images $\varphi(\alpha_1), \ldots, \varphi(\alpha_n)$ are a basis for $\mathrm{im}(\varphi)$: thus, $\mathrm{im}(\varphi)$ is an n-dimensional $\mathbb{Q}$-vector space.
  - We want to understand the image of $\mathcal{O}_K$ under φ as an additive group. If we choose an integral basis $\alpha_1, \ldots, \alpha_n$ of $\mathcal{O}_K$, then again by linearity as above, we see that $\varphi(\alpha_1), \ldots, \varphi(\alpha_n)$ will be an integral basis for $\varphi(\mathcal{O}_K)$: the elements clearly span, and they are linearly independent because $\alpha_1, \ldots, \alpha_n$ are.
  - Thus, $\varphi(\mathcal{O}_K)$ is a rank-n additive subgroup of $\mathbb{R}^n$.
  - Exercise: Suppose G is an additive subgroup of $\mathbb{R}^n$. Show that the following are equivalent (in such a case we say G is discrete):
    1. G is nowhere dense in $\mathbb{R}^n$.
    2. Every compact subset of $\mathbb{R}^n$ contains finitely many points of G.
    3. Some open neighborhood of 0 contains finitely many points of G.
    4. The rank of G as an abelian group equals the dimension of $G \otimes_{\mathbb{Z}} \mathbb{R}$ as an $\mathbb{R}$-vector subspace of $\mathbb{R}^n$.
  - We claim that $\varphi(\mathcal{O}_K)$ is also discrete. To see this, consider the open neighborhood $S = \{(x_1, \ldots, x_n) : |x_i| < 1/2\}$ of the origin and suppose $\alpha \in \mathcal{O}_K$ has $\varphi(\alpha) \in S$.
  - Then $|\sigma_i(\alpha)| < 1/2$ for each embedding σ_i (real or complex), but this would imply $|N_{K/\mathbb{Q}}(\alpha)| = \prod_i |\sigma_i(\alpha)| < (1/2)^n < 1$ but since the norm is an integer, it would have to be zero, implying $\alpha = 0$.
  - This means the only point of S in $\varphi(\mathcal{O}_K)$ is the origin $\varphi(0)$, so by the exercise above, $\varphi(\mathcal{O}_K)$ is discrete.
  - Hence $\varphi(\mathcal{O}_K)$ is a discrete rank-n additive subgroup of $\mathbb{R}^n$, which is to say, a lattice in $\mathbb{R}^n$.
  - Exercise: Let K be a number field and $\varphi : K \to \mathbb{R}^n$ be the Minkowski map. Show that $\varphi(K)$ is dense in $\mathbb{R}^n$. [Hint: Replace integer coefficients with rational ones.]

- Definition: A lattice in $\mathbb{R}^n$ is an additive subgroup given by the $\mathbb{Z}$-span of an $\mathbb{R}$-basis for $\mathbb{R}^n$.
  - More explicitly, for any integral basis $\alpha_1, \ldots, \alpha_n$ of $\mathcal{O}_K$, $\varphi(\mathcal{O}_K)$ is the $\mathbb{Z}$-span of $\varphi(\alpha_1), \ldots, \varphi(\alpha_n)$.
  - A fundamental region for this lattice can be obtained by drawing all of the vectors $\varphi(\alpha_1), \ldots, \varphi(\alpha_n)$ outward from the origin, and then filling them in to create a "skew box". The points in this fundamental region give unique representatives for the quotient group $\mathbb{R}^n/\Lambda$, up to an appropriate choice of representatives on the boundary of the region. Since the fundamental region is simply a representative of $\mathbb{R}^n/\Lambda$, we call the n-measure[6] of the fundamental region the covolume of Λ.

[6] By n-measure we mean the Lebesgue measure on $\mathbb{R}^n$, like any sensible person would. (But we say "n-measure" because the only sets we consider are extremely nice, so we do not need to be concerned with of any of the interesting subtleties of measure theory.)

- Exercise: Suppose Λ is a lattice in $\mathbb{R}^n$ with an integral basis $v_1, \ldots, v_n$. Show that the covolume of Λ is equal to $|\det(v_1, \ldots, v_n)|$.

- By writing down a basis we can compute the volume of the fundamental region for $\varphi(\mathcal{O}_K)$ and then for $\varphi(I)$ for any nonzero ideal I:

- Proposition (Measures of Fundamental Regions): Let K be a number field of signature (r, s) and discriminant $\Delta = \text{disc}(K)$, and let $\varphi : K \to \mathbb{R}^n$ be the Minkowski map.

  1. The covolume of $\varphi(\mathcal{O}_K)$ is equal to $2^{-s}\sqrt{|\text{disc}(K)|}$.
     - Proof: Let $\alpha_1, \ldots, \alpha_n$ be an integral basis for $\mathcal{O}_K$. By the exercise above, we see that n-measure of the fundamental region for $\varphi(\mathcal{O}_K)$ is the (absolute value of the) determinant of the matrix whose columns are the vectors $\varphi(\alpha_1), \ldots, \varphi(\alpha_n)$.
     - This determinant is $\begin{vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_r(\alpha_1) & \cdots & \sigma_r(\alpha_n) \\ \text{Re}[\tau_1(\alpha_1)] & \cdots & \text{Re}[\tau_1(\alpha_n)] \\ \text{Im}[\tau_1(\alpha_1)] & \cdots & \text{Im}[\tau_1(\alpha_n)] \\ \vdots & \ddots & \vdots \\ \text{Re}[\tau_s(\alpha_1)] & \cdots & \text{Re}[\tau_s(\alpha_n)] \\ \text{Im}[\tau_s(\alpha_1)] & \cdots & \text{Im}[\tau_s(\alpha_n)] \end{vmatrix} = \frac{1}{(2i)^s} \begin{vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_r(\alpha_1) & \cdots & \sigma_r(\alpha_n) \\ \tau_1(\alpha_1) & \cdots & \tau_1(\alpha_n) \\ \overline{\tau_1(\alpha_1)} & \cdots & \overline{\tau_1(\alpha_n)} \\ \vdots & \ddots & \vdots \\ \tau_s(\alpha_1) & \cdots & \tau_s(\alpha_n) \\ \overline{\tau_s(\alpha_1)} & \cdots & \overline{\tau_s(\alpha_n)} \end{vmatrix} = \pm\frac{1}{(2i)^s}\sqrt{\text{disc}(K)}.$
     - By taking the absolute value above we see immediately that the covolume of $\varphi(\mathcal{O}_K)$ is $2^{-s}\sqrt{|\text{disc}(K)|}$.
  2. For any nonzero ideal I of $\mathcal{O}_K$, the covolume of $\varphi(I)$ is $N(I) \cdot 2^{-s}\sqrt{|\text{disc}(K)|}$.
     - Proof: Note that $\Lambda_I = \varphi(I)$ is a sublattice (i.e., an additive subgroup) of $\Lambda = \varphi(\mathcal{O}_K)$.
     - Since φ is an isomorphism of additive abelian groups that maps $\mathcal{O}_K$ to Λ and I to Λ_I, we see that $\Lambda/\Lambda_I \cong \mathcal{O}_K/I$. Taking cardinalities then yields $\#(\Lambda/\Lambda_I) = \#(\mathcal{O}_{\sqrt{D}}/I) = N(I)$.
     - Geometrically, this means that the fundamental domain for Λ_I consists of $N(I)$ copies of the fundamental domain for Λ, and then the desired result follows immediately from (1).

- Our goal now is to show that if a convex set in $\mathbb{R}^n$ is sufficiently nice and has a sufficiently large n-measure, it must contain a lattice point.

  - To obtain our bound, we will then apply these results to the region in $\mathbb{R}^n$ corresponding to the points of small norm, where "small" is chosen in such a way that we obtain a nonzero point lying in the lattice $\Lambda = \varphi(I)$, which will provide the desired nonzero element $\alpha \in I$ of small norm.

- Theorem (Minkowski Lattice Theorems): Let $n \geq 1$. Recall that a set B in $\mathbb{R}^n$ is convex when for any $x, y \in B$, all points on the line segment joining x and y are also in B, and a set is centrally symmetric when $x \in B$ implies $-x \in B$.

  1. (Blichfeldt's Principle) If S is a bounded measurable set in $\mathbb{R}^n$ whose n-measure is greater than 1, then there exist two points x and y in S such that $x - y$ has integer coordinates.
     - Proof: The idea is essentially to use the pigeonhole principle.
     - For each lattice point $a = (a_1, \cdots, a_n)$, let B_a be the "box" consisting of the points $(x_1, \cdots, x_n)$ whose coordinates satisfy $a_i \leq x_i < a_{i+1}$, and let $S_a = S \cap B_a$ be the intersection of S with B_a.
     - Since each point of S lies in exactly one box B_a, we have $\sum_{a \in \mathbb{Z}^n} \text{vol}(S_a) = \text{vol}(S)$.
     - Now let S_a^* be the set S_a translated by the vector $-a$: this translation preserves measure and moves B_a to B_0.
     - Then $\sum_{a \in \mathbb{Z}^n} \text{vol}(S_a^*) = \text{vol}(S) > 1$. But since all of the sets S_a^* lie inside B_0 which has volume 1, there must be some overlap.
     - If $S_{a_1}^* \cap S_{a_2}^*$ contains some point P, then $P + a_1 \in S$ and also $P + a_2 \in S$. Taking $x = P + a_1$ and $y = P + a_2$ we see that $x - y = a_1 - a_2$ has integer coordinates, as claimed.

- Remark: This proof can also be formulated analytically in terms of the characteristic function $\chi_B(x) = \begin{cases} 1 & \text{if } x \in B \\ 0 & \text{if } x \notin B \end{cases}$, which is integrable by the hypothesis that B is a measurable set. If we write $\psi(x) = \sum_{v \in \mathbb{Z}^n} \chi_B(x+v)$, then ψ is bounded because B is bounded so there are only finitely many nonzero terms for any $v \in \mathbb{Z}^n$. We may then integrate both sides and change the order of integration and summation (because the sum is a finite sum of nonnegative terms) and use the translation-invariance of the measure on $\mathbb{R}^n$ to see that $\int_{[0,1]^n} \psi(x)\,dx = \int_{[0,1]^n} \sum_{v \in \mathbb{Z}^n} \chi_B(x+v)\,dx = \sum_{v \in \mathbb{Z}^n} \int_{[0,1]^n} \chi_B(x+v)\,dx = \sum_{v \in \mathbb{Z}^n} \int_{[0,1]^n + v} \chi_B(x)\,dx = \int_{\mathbb{R}^n} \chi_B(x)\,dx$, and this last integral is simply the measure of B.

2. Let B be a convex open centrally-symmetric set in $\mathbb{R}^n$ whose n-measure is greater than 2^n. Then B contains a nonzero point of $\mathbb{Z}^n$.
   - We note here that the bound 2^n is sharp, since the open box $(-1,1)^n$ has measure 2^n and is convex, open, and centrally symmetric, but its only $\mathbb{Z}^n$-point is the origin.
   - Proof: Suppose B is a convex open set symmetric about 0 of measure $> 2^n$ and let $\frac{1}{2}B = \{\frac{1}{2}x : x \in B\}$.
   - Notice that since the measure of B is greater than, the measure of $\frac{1}{2}B$ is greater than 1. Now apply Blichfeldt's principle (1) to the set $\frac{1}{2}B$: we obtain distinct points $x, y \in \frac{1}{2}B$ such that $x - y$ has integer coordinates.
   - Then $2x \in B$ and $2y \in B$. Furthermore, since B is symmetric about the origin, $-2y \in B$.
   - Then because B is convex, the midpoint of the line segment joining $2x$ and $-2y$ lies in B.
   - This midpoint $x - y$ yields the desired nonzero point in B whose coordinates are integers.
3. Let Λ be a lattice in $\mathbb{R}^n$ whose fundamental domain has n-measure V. If B is a convex open centrally-symmetric set in $\mathbb{R}^n$ whose n-measure is greater than $2^n V$, then B contains a nonzero point of Λ.
   - Proof: Apply the linear transformation T sending the basis vectors of Λ to the standard basis of $\mathbb{R}^n$.
   - Linear transformations preserve open sets, convex sets, and central symmetry, so the image of B under this map is still open, convex, and centrally symmetric.
   - The volume of $T(B)$ is equal to $1/V$ times the volume of B by the geometric properties of determinants, so this new open convex centrally-symmetric set $T(B)$ has volume $> 2^n$.
   - Applying (2) to $T(B)$ yields that $T(B)$ contains a nonzero point all of whose coordinates are integers. This immediately implies that B contains a nonzero point of Λ, as required.
   - Exercise: Let Λ be a lattice in $\mathbb{R}^n$ whose fundamental domain has n-measure V. Show that if B is a convex closed centrally-symmetric set in $\mathbb{R}^n$ whose n-measure is greater than or equal to $2^n V$, then B contains a nonzero point of Λ.

0.24 (Oct 30) Student Presentations of HW3 Problems

0.25 (Oct 31) The Minkowski Bound

- We would now like to apply Minkowski's lattice theorem (3) to the lattice $\Lambda = \varphi(I)$ for a nonzero ideal I and an appropriate region in $\mathbb{R}^n$ consisting of points of small norm.
  - If K has signature (r,s), if we write $\varphi(\alpha) = (\sigma_1(\alpha), \dots, \sigma_r(\alpha), \mathrm{Re}[\tau_1(\alpha)], \mathrm{Im}[\tau_1(\alpha)], \dots, \mathrm{Re}[\tau_s(\alpha)], \mathrm{Im}[\tau_s(\alpha)]) = (x_1, \dots, x_r, y_1, z_1, \dots, y_s, z_s)$, then we can see that $N(\alpha) = \sigma_1(\alpha) \cdots \sigma_r(\alpha) \tau_1(\alpha) \overline{\tau_1(\alpha)} \cdots \tau_s(\alpha) \overline{\tau_s(\alpha)} = \sigma_1(\alpha) \cdots \sigma_r(\alpha) \left|\tau_1(\alpha)\right|^2 \cdots \left|\tau_s(\alpha)\right|^2 = x_1 \cdots x_r (y_1^2 + z_1^2) \cdots (y_s^2 + z_s^2)$.
  - Thus, the region consisting of points of "norm less than X" is the region $(x_1, \dots, x_r, y_1, z_1, \dots, y_s, z_s) \in \mathbb{R}^n$ with $\left|x_1 \cdots x_r (y_1^2 + z_1^2) \cdots (y_s^2 + z_s^2)\right| < X$.
  - This region is obviously centrally symmetric, and in some cases it is centrally symmetric and bounded: for instance, when $(r,s) = (0,1)$ it is the region $\left|y^2 + z^2\right| < X$ which is an open disc.
  - Unfortunately, this is not always the case: for instance, when $(r,s) = (2,0)$ it is the region $|x_1 x_2| < X$ which contains both coordinate axes, so it is neither convex nor bounded (since the convex hull of the coordinate axes is the entire plane).

- One way we can make the region convex is to take the set B defined by the inequalities $|x_i| \leq X$, $y_j^2 + z_j^2 \leq Y$ for positive reals X and Y, whose measure is $(2X)^r(\pi Y)^s$ and where the norm function is bounded by $X^r Y^s$. This region is obviously convex, open, and centrally symmetric.
- Then for any lattice Λ whose fundamental region has n-measure V, whenever $(2X)^r(\pi Y)^s > 2^n V$ we would get a nonzero point of Λ of norm at most $X^r Y^s$.
- So, taking $N = X^r Y^s$, for any $N > 2^n V 2^{-r}\pi^{-s} = \left(\frac{4}{\pi}\right)^s V$ we obtain a nonzero point of Λ of norm at most N.
- But in fact, we can get a better bound than this by intermingling all of the variables, as follows:

• Theorem (Minkowski Bound): Let K be a number field of degree n over $\mathbb{Q}$ with signature (r, s).

1. In $\mathbb{R}^n = (x_1, \ldots, x_r, y_1, z_1, \ldots, y_s, z_s)$, for any $t > 0$ the region B_t defined by $|x_1|+\cdots+|x_r|+2(\sqrt{y_1^2+z_1^2}+\cdots+\sqrt{y_s^2+z_s^2}) < t$ is open, convex, centrally symmetric, and has n-measure equal to $\frac{2^r}{n!}\left(\frac{\pi}{2}\right)^s t^n$.
   - Proof: Let $f(x_1, \ldots, y_s, z_s) = |x_1| + \cdots + |x_r| + 2(\sqrt{y_1^2+z_1^2} + \cdots + \sqrt{y_s^2+z_s^2})$.
   - Clearly B_t is open since it is the inverse image of an open set under the continuous function f, and equally clearly f is an even function, so B_t is centrally symmetric.
   - To see that B_t is convex we simply note that each component function of f is convex, so for $\mathbf{x}, \mathbf{y} \in B_t$ and $0 \leq u \leq 1$ we have $f(u\mathbf{x} + (1-u)\mathbf{y}) \leq uf(\mathbf{x}) + (1-u)f(\mathbf{y}) < t$, hence $u\mathbf{x} + (1-u)\mathbf{y} \in B_t$ also.
   - It remains to compute the measure of B_t. Since $f(\lambda\mathbf{x}) = \lambda f(\mathbf{x})$ for any positive λ, we see $B_t = tB_1$ and so it suffices to compute the n-measure of B_1.
   - Now let $M_{r,s}(t)$ be the n-measure of the set $|x_1| + \cdots + |x_r| + 2(\sqrt{y_1^2+z_1^2} + \cdots + \sqrt{y_s^2+z_s^2}) < t$; note that $M_{r,s}(t) = t^{r+2s}M_{r,s}(1)$.
   - First, by changing to polar coordinates we can see that $M_{0,s}(1) = \int_{\sqrt{y_1^2+z_1^2}+\cdots+\sqrt{y_s^2+z_s^2}<1/2} d\mu = \int_{r_1+\cdots+r_s<1/2} r_1 \cdots r_s \, dr_1 \cdots dr_s d\theta_1 \cdots d\theta_s = (\frac{\pi}{2})^s \int_{w_1+\cdots+w_s<1} w_1 \cdots w_s \, dw_1 \cdots dw_s = (\frac{\pi}{2})^s \frac{1}{(2s)!}$ as follows by a straightforward induction.
   - Then by integrating on the first variable, when $r > 0$ we have $M_{r,s}(1) = 2\int_0^1 M_{r-1,s}(1-x)\,dx = 2M_{r-1,s}(1) \cdot \int_0^1 (1-x)^{(r-1)+2s}\,dx = \frac{2}{r+2s}M_{r-1,s}(1)$.
   - By a trivial induction and the above, $M_{r,s}(t) = t^{r+2s}M_{r,s}(1) = \frac{2^r t^{r+2s}}{(r+2s)(r+2s-1)\cdots(1+2s)}M_{0,s}(1) = \frac{2^r(\pi/2)^s t^{r+2n}}{(r+2s)(r+2s-1)\cdots(1+2s)\cdot(2s)!} = \frac{2^r}{n!}\left(\frac{\pi}{2}\right)^s t^n$, as desired.
2. With the "norm" function $N(x_1, \ldots, x_r, y_1, z_1, \ldots, y_s, z_s) = x_1 \cdots x_r (y_1^2+z_1^2)\cdots(y_s^2+z_s^2)$ on $\mathbb{R}^n$, for any lattice of covolume V, there exists a nonzero point $\mathbf{x} \in \Lambda$ with $N(\mathbf{x}) \leq \frac{n!}{n^n}\left(\frac{8}{\pi}\right)^s V$.
   - Proof: Consider the region B_t from (1) defined by $|x_1|+\cdots+|x_r|+2(\sqrt{y_1^2+z_1^2}+\cdots+\sqrt{y_s^2+z_s^2}) < t$, which by (1) is convex, open, and centrally symmetric with n-measure equal to $\frac{2^r}{n!}\left(\frac{\pi}{2}\right)^s t^n$.
   - Therefore, by Minkowski's lattice theorem, if $\frac{2^r}{n!}\left(\frac{\pi}{2}\right)^s t^n > 2^n V$, which is to say, $t^n > n!\left(\frac{8}{\pi}\right)^s V$, then B_t will contain a nonzero point $\mathbf{x} \in \Lambda$.
   - Then for this $\mathbf{x} \in B_t$, by the arithmetic-geometric mean inequality applied to the list of n nonnegative real numbers $|x_1|, \ldots, |x_r|$, $\sqrt{y_1^2+z_1^2}$, $\sqrt{y_1^2+z_1^2}$, ... , $\sqrt{y_s^2+z_s^2}$, $\sqrt{y_s^2+z_s^2}$, we have

$$\begin{aligned} N(\mathbf{x})^{1/n} &= [x_1 \cdots x_r \sqrt{y_1^2+z_1^2}\sqrt{y_1^2+z_1^2}\cdots\sqrt{y_s^2+z_s^2}\sqrt{y_s^2+z_s^2}]^{1/n} \\ &\leq \frac{1}{n}\left[|x_1| + \cdots + |x_r| + 2(\sqrt{y_1^2+z_1^2} + \cdots + \sqrt{y_s^2+z_s^2})\right] < \frac{t}{n}. \end{aligned}$$

   - Thus, taking $t^n \to n!\left(\frac{8}{\pi}\right)^s V$ from above, we see $N(\mathbf{x}) \leq \frac{t^n}{n^n} = \frac{n!}{n^n}\left(\frac{8}{\pi}\right)^s V$, as claimed.

3. For any nonzero ideal I of $\mathcal{O}_K$, there exists a nonzero $\alpha \in I$ such that $\left|N_{K/\mathbb{Q}}(I)\right| \leq N(I) \cdot \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc} K|}$.
   - Proof: Apply (2) to the lattice $\Lambda = \varphi(I)$ whose covolume equals $V = N(I) \cdot 2^{-s}\sqrt{|\operatorname{disc}(K)|}$ as calculated earlier.
   - The estimate we obtain is $N(\alpha) = N(\varphi(\alpha)) = \frac{n!}{n^n}\left(\frac{8}{\pi}\right)^s N(I) \cdot 2^{-s}\sqrt{|\operatorname{disc}(K)|} = N(I) \cdot \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc} K|}$, as claimed.
4. (Minkowski Bound) Every ideal class of $\mathcal{O}_K$ contains an ideal J such that $N(J) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc} K|}$.
   - Proof: This follows by the same proof we gave earlier, but with the improved constant c_K provided by (4).

- Exercise: Show that if K is a number field of degree n over $\mathbb{Q}$ with signature (r, s), show that $|\operatorname{disc} K| \geq \left(\frac{\pi}{4}\right)^{2s}\left(\frac{n^n}{n!}\right)^2$. Show also that if $n > 1$ then $|\operatorname{disc} K| > 1$, and deduce that $\mathbb{Q}$ has no unramified extensions.
- Minkowski's bound is quite a lot better than the estimate we obtained earlier, since it is asymptotic to $\sqrt{|\operatorname{disc} K|}$ rather than to the discriminant itself, so the size of the computations we need to make to calculate class groups is much smaller.
   - Let us begin by investigating the class groups of quadratic fields.
- Example (again): Show that the class group of $K = \mathbb{Q}(\sqrt{-5})$ has order 2.
   - Here we have $n = 2$, $s = 1$, and $\operatorname{disc}(K) = -20$, so Minkowski's bound says that every ideal class of R contains an ideal of norm at most $\frac{2}{\pi}\sqrt{20} \approx 2.8471 < 3$, so the only nontrivial ideals we need to consider are ideals of norm 2.
   - Since (2) splits as $(2) = (2, 1 + \sqrt{-5})^2$, and we have previously shown that $(2, 1 + \sqrt{-5})$ is nonprincipal, we conclude that the class group is generated by the nonprincipal ideal $I_2 = (2, 1 + \sqrt{-5})$. Since I_2 has order 2 as $I_2^2 = (2)$, the class group has order 2 as claimed.
- Example: Show that the ring of integers of $K = \mathbb{Q}(\sqrt{-19})$ is a principal ideal domain.
   - Here we have $n = 2$, $s = 1$, and $\operatorname{disc}(K) = -19$, so Minkowski's bound says that every ideal class of R contains an ideal of norm at most $\frac{2}{\pi}\sqrt{19} \approx 2.7750 < 3$, so the only nontrivial ideals we need to consider are ideals of norm 2.
   - Since the minimal polynomial of the generator $m(x) = x^2 - x + 5$ is irreducible modulo 2, we see (2) is inert so there are no ideals of norm 2 in $\mathcal{O}_K$.
   - Therefore, the only ideal class is the trivial class, so the class group is trivial and $\mathcal{O}_{\sqrt{-19}}$ is a PID.
   - Remark: It can be shown that $\mathcal{O}_{\sqrt{-19}}$ is not Euclidean with respect to any norm, so this ring provides an example of a principal ideal domain that is not Euclidean.
- Example: Determine the class group of $K = \mathbb{Q}(\sqrt{5})$.
   - Here we have $n = 2$, $s = 0$, and $\operatorname{disc}(K) = 5$, so Minkowski's bound says that every ideal class of R contains an ideal of norm at most $\frac{1}{2}\sqrt{5} \approx 1.1180 < 2$, so there can be no nontrivial ideal classes.
   - Thus, the class group of $\mathbb{Z}[\sqrt{5}]$ is trivial.
- Example: Determine the class group of $K = \mathbb{Q}(\sqrt{10})$.
   - Here we have $n = 2$, $s = 0$, and $\operatorname{disc}(K) = 40$, so Minkowski's bound says that every ideal class of R contains an ideal of norm at most $\frac{1}{2}\sqrt{40} \approx 3.1623 < 4$, so the only nontrivial ideals we need to consider are ideals of norm 2 and norm 3.

- Applying Dedekind-Kummer to the minimal polynomial $m(x) = x^2 - 10$, we see that (2) is ramified and (3) splits: explicitly, $(2) = P_2^2$ for $P_2 = (2, \sqrt{10})$ and $(3) = P_3 P_3'$ for $P_3 = (3, 1 + \sqrt{10})$ and $P_3' = (3, 1 - \sqrt{10})$.
- Since $x^2 - 10y^2 = \pm 2, \pm 3$ has no solutions modulo 5, there are no elements of norm ± 2 or ± 3, so P_2, P_3, P_3' are non-principal.
- Thus, $[I_2]$ is an element of order 2 in the class group since I_2 is not principal but I_2^2 is.
- We can then compute $I_3^2 = (9, 3 + 3\sqrt{10}, 11 + 2\sqrt{10})$. To test for principality we can look for elements of norm 9, and looking at such elements (e.g., $1 \pm \sqrt{10}$) will reveal this ideal is in fact principal and generated by $(1 + \sqrt{10})$. Explicitly, $1 + \sqrt{10} = 9 + (3 + 3\sqrt{10}) - (11 + 2\sqrt{10}) \in I_3^2$ and each generator is divisible by $1 + \sqrt{10}$. Then $(I_3')^2 = (1 - \sqrt{10})$, so $[I_3]$ and $[I_3']$ are both ideal classes of order 2 and they are equal.
- It remains to determine the relationship between I_2 and I_3. Indeed, $I_2 I_3 = (6, 2 + 2\sqrt{10}, 3\sqrt{10}, 10 + \sqrt{10})$. To test for principality we can look for elements of norm 6, and looking at such elements (e.g., $4 \pm \sqrt{10}$) will reveal this ideal is in fact principal and generated by $(4 + \sqrt{10})$, since $4 + \sqrt{10} = (10 + \sqrt{10}) - 6$ and each generator is divisible by $4 + \sqrt{10}$. Thus since $[I_2][I_3] = (1) = [I_2]^2$, we see $[I_2] = [I_3]$.
- Thus, we conclude that there is one nonprincipal ideal class of order 2, so the class group is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

- Example: Determine the class group of $\mathbb{Q}(\sqrt{-31})$.
  - Here we have $n = 2$, $s = 1$, and $\text{disc}(K) = -31$, Minkowski's bound says that every ideal class of R contains an ideal of norm at most $\frac{2}{\pi}\sqrt{31} \approx 3.5445 < 4$, so the only nontrivial ideals we need to consider are ideals of norm 2 and 3.
  - Applying Dedekind-Kummer to the minimal polynomial $m(x) = x^2 - x + 8$ yields that 2 splits and 3 is inert, so we may ignore 3.
  - Explicitly we have $(2) = P_2 P_2'$ for $P_2 = (2, \frac{1+\sqrt{-31}}{2})$ and $P_2' = (2, \frac{1-\sqrt{-31}}{2})$.
  - We can check (by solving $a^2 + 31b^2 = 8, 16$) that there are no elements of norm 2 and the only elements of norm 4 are ± 2, so since $(2) = P_2 P_2'$ and $P_2 \neq P_2'$, we see that neither P_2 nor P_2^2 is principal.
  - On the other hand, P_2^3 has norm 8, and there are elements of norm 8, namely, $\alpha = \frac{1+\sqrt{-31}}{2}$. Indeed, we can see that $P_2^3 = (8, 4\alpha, 2\alpha^2, \alpha^3)$ so this ideal contains $8 + 8\alpha + \alpha^3 = \alpha$. Thus $P_2^3 = (\alpha)$ is principal, and so $[P_2]$ is an element of order 3 in the class group with inverse $[P_2'] = [P_2]^2$.
  - Therefore, the class group is generated by $[P_2]$ and is isomorphic to $\mathbb{Z}/3\mathbb{Z}$.

- Exercise: Show that for $D = -1, -2, -3, -7, -11, -19, -43, -67, -163$, the class group of $\mathbb{Q}(\sqrt{D})$ is trivial.
  - Heilbronn also showed that there were at most 10 imaginary quadratic fields of class number 1; since the 9 listed above were well known to have trivial class group, this meant there could exist at most one more. (Gauss had previously conjectured that there were only finitely many.)
  - The nonexistence of this 10th field was essentially proven by Heegner in 1952 using modular forms, but his proof had some minor gaps and it was not accepted[7] until Stark gave a full proof of the result in 1967. Baker also gave a proof, using an entirely different method (linear forms in logarithms), in 1966.

- Exercise: Show that for $D = 2, 3, 6, 11, 13, 15, 17, 19$, the class group of $\mathbb{Q}(\sqrt{D})$ is trivial.
  - Unlike in the situation of imaginary quadratic fields, Gauss conjectured there are infinitely many real quadratic fields of class number 1. As of 2024, this problem is still open.
  - Many small values of D do yield real quadratic fields of class number 1, such as the ones above.

- Exercise: Show that for $D = 101, 103, 107, 109$, the class group of $\mathbb{Q}(\sqrt{D})$ is trivial.

- Exercise: Show that $\mathbb{Q}(\sqrt{-10})$, $\mathbb{Q}(\sqrt{-13})$, and $\mathbb{Q}(\sqrt{-15})$ all have class number 2.

[7] Heegner was not a professional mathematician (he was in fact a radio engineer and high school teacher), which certainly contributed to the lack of belief in his claim to have settled a 150-year-old conjecture of Gauss by the broader mathematical community. Sadly, he died in 1965, before his results gained general acceptance.

- Exercise: Show that $\mathbb{Q}(\sqrt{7})$, $\mathbb{Q}(\sqrt{14})$, $\mathbb{Q}(\sqrt{23})$, and $\mathbb{Q}(\sqrt{29})$ all have class number 2.
- Exercise: Show that $\mathbb{Q}(\sqrt{-23})$, $\mathbb{Q}(\sqrt{-59})$, and $\mathbb{Q}(\sqrt{-83})$ all have class number 3.
- Exercise: Show that $\mathbb{Q}(\sqrt{79})$ has class number 4. Which group is its class group isomorphic to?
- Exercise: Show that $\mathbb{Q}(\sqrt{-17})$ and $\mathbb{Q}(\sqrt{-21})$ both have class number 4 but that their class groups are not isomorphic.
- Exercise: Show that $\mathbb{Q}(\sqrt{-103})$ has class number 5.
- Exercise: Show that $\mathbb{Q}(\sqrt{-29})$ has class number 6.
- Exercise: Show that $\mathbb{Q}(\sqrt{-71})$ has class number 7.
- We will mention that there are numerous other conjectures about various aspects of the class groups of real and imaginary quadratic fields.
    - One set of predictions are the Cohen-Lenstra heuristics, which posit, for odd primes p, the density with which any given abelian p-group will appear as the p-power torsion part of a class group (i.e., the Sylow p-subgroup) of a real or imaginary quadratic field.
    - For the prime $p = 2$, the structures of p-power torsion subgroups of class groups are fully understood, and are consequences of what is called genus theory, which is a name due to Gauss (as is the term "equivalence class", which first appeared in Gauss's treatment of quadratic forms) that has nothing to do with other uses of the word "genus", e.g., in topology.
    - Intuitively, the Cohen-Lenstra heuristics say that the probability, in an appropriate sense, that a given abelian p-group P will occur as the p-part of the class group of an imaginary quadratic field should be proportional to $1/\#\mathrm{Aut}(P)$. This may initially seem to be a rather unnatural weighting, but in fact it is quite sensible in the appropriate context: given a group acting on a set X, if we wish to select an orbit of the group uniformly at random, we should weight each of the elements of X by 1 over the size of its orbit and then pick an element of X at random with that weighting.
    - By summing $1/\#\mathrm{Aut}(P)$ over all finite abelian p-groups P, one obtains a constant μ_P, which can be computed (though not easily). Then the Cohen-Lenstra heuristics predict that the proportion of imaginary quadratic fields whose p-power torsion subgroup is isomorphic to P is equal to $\dfrac{1/\#\mathrm{Aut}(P)}{\mu_P}$.
    - Some various results for other primes: the probability that the class number is divisible by 3 (i.e., that the 3-part of the class group is not trivial) is approximately 43.99%, the probability that it is divisible by 5 is approximately 23.97%, and the probability that it is divisible by 7 is approximately 16.32%.
    - A similar heuristic holds for real quadratic fields, although the weighting is slightly different. For real quadratic fields, the probability that a prime p divides the class number is predicted to be $1 - \prod_{k \geq 2}(1 - p^{-k})$, which for $p = 3$ is approximately 15.98%, for $p = 5$ is approximately 4.96%, and for $p = 7$ is approximately 2.37%.
    - All of these results agree extremely well with the available numerical data.

0.26 (Nov 4) Computing More Class Groups

- Let us now compute some examples of class groups for higher-degree fields.
- Example: Show that the class group of $K = \mathbb{Q}(\sqrt[3]{2})$ is trivial.
    - We have $n = 3$, $s = 1$, and we have previously computed $\mathrm{disc}(K) = -108$, so Minkowski's bound says that every ideal class contains an ideal of norm at most $\dfrac{6}{27} \cdot \dfrac{4}{\pi}\sqrt{108} \approx 2.9404$, so we only need to consider 2.
    - Since $(2) = P_2^3$ for $P_2 = (2, \sqrt[3]{2}) = (\sqrt[3]{2})$ we see that the unique prime ideal of norm 2 is principal, so the class group of K is trivial.
- Example: Show that the class group of $K = \mathbb{Q}(\sqrt[3]{10})$ is trivial.

- We have $n = 3$, $s = 1$, and we have previously computed $\text{disc}(K) = -300$, so Minkowski's bound says that every ideal class contains an ideal of norm at most $\frac{6}{27} \cdot \frac{4}{\pi}\sqrt{300} \approx 4.9007$, so we only need to consider 2 and 3.
- With $\alpha = \sqrt[3]{10}$ and $\beta = \frac{1}{3}(1 + \sqrt[3]{10} + \sqrt[3]{100})$, we have previously computed that $(2) = P_2^3$ for $P_2 = (2, \alpha) = (2 - \alpha)$ and $(3) = P_3^2 P_3'$ for $P_3 = (3, \beta) = (\beta)$ and $P_3' = (3, -1 + \beta) = (\beta - \alpha)$.
- So since the prime ideals of norms 2 and 3 are all principal, the class group of K is trivial.

- Exercise: Show that the class group of $K = \mathbb{Q}(\sqrt[3]{5})$ is trivial.
- Exercise: Show that the class group of $K = \mathbb{Q}(\sqrt[3]{6})$ is trivial. (This can be done without computing an integral basis for the ring of integers, but it ends up being $\mathbb{Z}[\sqrt[3]{6}]$.)
- Exercise: For $K = \mathbb{Q}(\alpha)$ with $\alpha^3 - \alpha + 1 = 0$, show that the class group of K is trivial.
- Example: Find the class group of $K = \mathbb{Q}(\sqrt[3]{7})$.
  - By an argument similar to the one used for the other fields $\mathbb{Q}(\sqrt[3]{m})$, for $\alpha = \sqrt[3]{7}$ we can show that $\{1, \alpha, \alpha^2\}$ is an integral basis for $\mathcal{O}_K$.
  - Then we have $n = 3$, $s = 1$, and $\text{disc}(K) = N_{K/\mathbb{Q}}(3\alpha^2) = -3^3 7^2$, so Minkowski's bound says that every ideal class contains an ideal of norm at most $\frac{6}{27} \cdot \frac{4}{\pi}\sqrt{3^3 7^2} \approx 10.291$, so we need to consider 2, 3, 5, and 7.
  - Since we will need to compute element norms, we note also that $N_{K/\mathbb{Q}}(a + b\alpha + c\alpha^2) = a^3 + 7b^3 + 49c^3 - 21abc$ and in particular observe that the norm of any element is congruent to $a^3 \equiv 0, \pm 1 \pmod 7$.
  - Since $x^3 - 7 = (1+x)(1-x+x^2) \bmod 2$, we have $(2) = P_2 P_2'$ with $P_2 = (2, 1+\alpha)$ and $P_2' = (2, 1-\alpha+\alpha^2)$. Since there are no elements of norm ± 2 or ± 4 as noted above, both of these ideals are non-principal.
  - Next, since $x^3 - 7 = (2 + x)^3 \bmod 3$ we have $(3) = P_3^3$ with $P_3 = (3, 2 + \alpha)$. Since there are no elements of norm 3 as noted above, P_3 is non-principal, so since $[P_3]^3$ is the trivial class, that means $[P_3]$ is an element of order 3 in the class group.
  - Further, we have $x^3 - 7 = (2 + x)(-1 - 2x + x^2) \pmod 5$, so $(5) = P_5 P_5'$ with $P_5 = (5, 2 + \alpha)$ and $P_5' = (5, -1 - 2\alpha + \alpha^2)$. Again since there are no elements of norm ± 5 or ± 25, both P_5 and P_5' are nontrivial elements in the class group.
  - Finally, we obviously have $(7) = P_7^3$ with $P_7 = (7, \alpha) = (\alpha)$ so this ideal is principal.
  - It remains to characterize the relationships between P_2, P_3, P_5, since we obviously have $[P_2'] = [P_2]^{-1}$ and $[P_5'] = [P_5]^{-1}$.
  - To do this we want to construct products among P_2, P_3, P_5 that are principal (hence must have norm congruent to ± 1 mod 7). The smallest reasonable candidates are 6 and 15.
  - Searching briefly reveals $N_{K/\mathbb{Q}}(-1 + \alpha) = 6$, meaning that we must have $P_2 P_3 = (-1 + \alpha)$ since these are the only possible prime ideal factors that can produce a norm of 6. (Indeed we can see that $-1 + \alpha$ lies in both ideals, as it should.)
  - Similarly, we can see that $N_{K/\mathbb{Q}}(2 + \alpha) = 15$, so we must have $P_3 P_5 = (2 + \alpha)$ since again these are the only possible prime ideal factors that can produce a norm of 15. (Indeed we can see that $2 + \alpha$ lies in both ideals, as it should.)
  - So we see that $[P_2] = [P_3]^{-1}$ and $[P_5] = [P_3]^{-1}$, and so the ideal class group is generated by $[P_3]$. Since $[P_3]$ has order 3, that means the class group is isomorphic to $\mathbb{Z}/3\mathbb{Z}$.

- Example: Show that the class group of $\mathbb{Q}(\zeta_d)$ is trivial for $d = 3, 4, 5, 6, 7$.
  - Since $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\zeta_6) = \mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\zeta_4) = \mathbb{Q}(i)$ the values $d = 3, 4, 6$ follow from our earlier calculations. Recall also that we showed previously that $\text{disc}(\mathbb{Q}(\zeta_p)) = (-1)^{p(p-1)/2} p^{p-2}$.
  - For $d = 5$ we have $n = \varphi(d) = 4$, $s = 2$ and $\text{disc}(K) = 5^3$, so Minkowski's bound says that every ideal class contains an ideal of norm at most $\frac{4!}{4^4} \cdot (\frac{4}{\pi})^2\sqrt{125} \approx 1.6992$, so we need not make any further calculations to conclude the ideal class group is trivial.

- For $d = 7$ we have $n = \varphi(d) = 6$, $s = 3$ and $\text{disc}(K) = -7^5$, so Minkowski's bound says that every ideal class contains an ideal of norm at most $\frac{6!}{6^6} \cdot (\frac{4}{\pi})^3 \sqrt{7^5} \approx 4.1295$, so we only need to consider 2 and 3.
- Since 2 has order 3 modulo 7, by our earlier analysis of the factorization of cyclotomic polynomials modulo p we see that $\Phi_7(x)$ factors as a product of two cubics mod 2, and so we have $(2) = P_2 P_2'$ with P_2, P_2' each of norm 8. But these ideals' norms exceed the Minkowski bound, so we can ignore them. (Explicitly, $P_2 = (2, 1 + \zeta_7 + \zeta_7^3)$ and $P_2' = (2, 1 + \zeta_7^2 + \zeta_7^3)$.)
- Likewise, since 3 has order 6 modulo 7, $\Phi_7(x)$ is irreducible mod 3, so (3) is inert.
- It follows that there are no nonprincipal ideals of norm less than the Minkowski bound, and so the class group of $\mathbb{Q}(\zeta_7)$ is trivial.

- Exercise: Show that the class group of $\mathbb{Q}(\zeta_8)$ is trivial. [Hint: What is $N(1 - \zeta_8)$?]
- Exercise: Show that the class group of $\mathbb{Q}(\zeta_9)$ is trivial.
- Exercise: Show that the class group of $\mathbb{Q}(\zeta_{11})$ is trivial. [This isn't as bad as it might look, but there is one difficult prime. Try computing $N(1 + \zeta_{11} - \zeta_{11}^8)$.]
  - We will mention here that it was shown independently by Montgomery and Uchida in 1971 that for p prime, the class number of $\mathbb{Q}(\zeta_p)$ is equal to 1 if and only if $p \leq 19$. This was extended by Malsey to determine fully the fields $\mathbb{Q}(\zeta_n)$ of class number 1 (there turn out to be 30 distinct fields).
- Exercise: Show that the class group of $\mathbb{Q}(\zeta_{23})$ is not trivial. [Hint: Let P be a prime lying above 23 in $\mathbb{Q}(\sqrt{-23})$ and let Q lie above P in $\mathbb{Q}(\zeta_{23})$. Show that $N_{\mathbb{Q}(\zeta_{23})/\mathbb{Q}(\sqrt{-23})}(Q) = P$ and that P is nonprincipal; deduce Q is nonprincipal and in fact that $[Q]$ has order 3.]
- Example: Find the class group of $K = \mathbb{Q}(\sqrt{5}, \sqrt{13})$.
  - We have previously computed that $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{5}}{2}, \frac{1+\sqrt{13}}{2}]$ and that $\text{disc}(K) = 5^2 13^2$.
  - Since obviously all of the embeddings of K are real we have $r = 4$ and $s = 0$, so since $n = 4$, Minkowski's bound says that every ideal class contains an ideal of norm at most $\frac{4!}{4^4} \cdot \sqrt{5^2 13^2} = 6.09375$, so we must consider 2, 3, and 5.
  - Let $\alpha = \frac{\sqrt{5}+\sqrt{13}}{2}$, $\beta = \frac{1+\sqrt{5}}{2}$, and $\gamma = \frac{1+\sqrt{13}}{2}$, which are all in $\mathcal{O}_K$.
  - For $p = 3$, we previously computed $(3) = Q_3 Q_3'$ where $Q_3 = (3, -1 + \alpha + \alpha^2)$ and $Q_3' = (3, -1 - \alpha + \alpha^2)$. Each of these ideals has norm 9, which exceeds the Minkowski bound, so we may ignore them.
  - For $p = 5$ we also computed $(5) = Q_5^2$ where $Q_5 = (5, 3 + \alpha^2)$. This ideal has norm 25, which again exceeds the Minkowski bound, so we may ignore it.
  - For $p = 2$ we exploited the intermediate field $\mathbb{Q}(\sqrt{5})$ to see that $2\mathcal{O}_K = Q_2 Q_2'$ where $Q_2 = (2, \gamma - \beta)$ and $Q_2' = (2, \gamma - \beta - 1)$. (We can confirm that this form of factorization is correct using Ore's factorization theorem to see that (2) factors as the product of two prime powers each of which has $ef = 2$, but since 2 is unramified, there must be two prime ideals each with $f = 2$, meaning that they have norm 4.)
  - But we can also readily check that $\gamma - \beta = \frac{-\sqrt{5}+\sqrt{13}}{2}$ has norm 4, so it generates Q_2, and then $2/(\gamma - \beta) = \frac{\sqrt{5}+\sqrt{13}}{2}$ generates Q_2'. Both ideals are principal, so we conclude there are no nonprincipal ideal classes and that the class group is trivial.
- Exercise: Show that the class group of $K = \mathbb{Q}(\sqrt{2}, \sqrt{-3})$ is trivial but that the class group of $F = \mathbb{Q}(\sqrt{-6})$ has order 2. (Thus, class numbers can decrease when taking field extensions.)

0.27 (Nov 6) Dirichlet's Unit Theorem

- Our goal now is to study the multiplicative group of units in the ring of integers $\mathcal{O}_K$ for a number field K.
  - As we already showed quite a while ago, an element $\alpha \in \mathcal{O}_K$ is a unit if and only if $N_{K/\mathbb{Q}}(\alpha) = \pm 1$.

- Any torsion element in the unit group is (by definition) a root of unity. Furthermore, if $\zeta_d \in K$, then the cyclotomic field $\mathbb{Q}(\zeta_d)$ would be a subfield of K, and therefore by considering degrees we would necessarily have $\varphi(d) \leq [K : \mathbb{Q}]$.
- The roots of unity in K always include ± 1, and indeed if K has any real embeddings these are the only possible roots of unity. (Of course, if K is totally complex, then K can have other roots of unity.)
- Since there are only finitely many integers d with $\varphi(d)$ less than a fixed positive integer (as follows for instance from the easy estimate $\varphi(d) \geq \sqrt{d}$ for $d > 2$), we see that there are only finitely many roots of unity in K, and so since the composite of the fields $\mathbb{Q}(\zeta_a)$, $\mathbb{Q}(\zeta_b)$ is $\mathbb{Q}(\zeta_{\mathrm{lcm}(a,b)})$ we see that the torsion subgroup of the unit group is a finite cyclic group consisting of the roots of unity in K. Alternatively, we could appeal directly to the fact that a finite multiplicative subgroup of a field is cyclic:
- Exercise: Let F be a field and let G be a finite multiplicative subgroup of the multiplicative group $F^\times$. Show that G is cyclic. [Hint: Consider solving $x^{\#G} - 1 = 0$ in $F[x]$.]

- The remaining (more difficult) task is to understand the torsion-free part of the unit group.
  - Our goal is to use a similar strategy as the one we used to understand the additive structure of $\mathcal{O}_K$ in establishing the Minkowski bound: there, we constructed a group homomorphism $\varphi : K \to \mathbb{R}^n$ and exploited the fact that the image of $\mathcal{O}_K$ was a lattice.
  - So we would like to try a similar approach here: namely, constructing a group homomorphism $\psi : K^\times \to \mathbb{R}^n$ into Euclidean space, and then showing that the image of the unit group is a lattice.
  - For a real embedding σ, restricting to nonzero elements yields a homomorphism $\sigma : K^\times \to \mathbb{R}^\times$ of multiplicative groups, but to exploit lattice structures we need the image to be an additive group. There is an obvious way to achieve this: namely, by taking logarithms afterwards.
  - Since we clearly want to avoid having to deal with the logarithm of -1 we use the map $\alpha \mapsto \log|\sigma(\alpha)|$. This also works equally well for a complex embedding, since it allows us to avoid the issues of nonuniqueness of complex logarithms, but it does make the complex-conjugate embeddings redundant, since they have the same absolute values.
  - If K has real embeddings $\sigma_1, \ldots, \sigma_r$ and nonreal embeddings $\tau_1, \overline{\tau_1}, \ldots, \tau_s, \overline{\tau_s}$, we see that we can construct the desired map ψ as the composition of the Minkowski map $\varphi : K^\times \to \mathbb{R}^n\backslash\{0\}$ with the logarithmic map $\log : \mathbb{R}^n\backslash\{0\} \to \mathbb{R}^{r+s}$ via $\log(x_1, \ldots, x_r, y_1, z_1, \ldots, y_s, z_s) = (\log|x_1|, \ldots, \log|x_r|, \log(y_1^2+z_1^2), \ldots, \log(y_s^2+z_s^2))$.

- By exploiting the logarithmic map, we can characterize the structure of the unit group:

- Theorem (Dirichlet's Unit Theorem): Let K be a number field with signature (r, s), with real embeddings $\sigma_1, \ldots, \sigma_r$ and nonreal embeddings $\tau_1, \overline{\tau_1}, \ldots, \tau_s, \overline{\tau_s}$. Define the map $\psi : K^\times \to \mathbb{R}^{r+s}$ via $\psi(\alpha) = (\log|\sigma_1(\alpha)|, \ldots, \log|\sigma_r(\alpha)|, \log|\tau_1(\alpha)|^2, \ldots, \log|\tau_s(\alpha)|^2)$, let U_K be the unit group of $\mathcal{O}_K$, and let $N = N_{K/\mathbb{Q}}$ denote the norm.

  1. The map ψ is a group homomorphism: $\psi(\alpha\beta) = \psi(\alpha) + \psi(\beta)$ for all $\alpha, \beta \in K^\times$.
     - Proof: Clear, since $\log|\sigma(\alpha\beta)| = \log|\sigma(\alpha)\sigma(\beta)| = \log|\sigma(\alpha)| + \log|\sigma(\beta)|$ for each embedding σ, so the required property holds in each coordinate.
  2. The image $\psi(U_K)$ is contained in the hyperplane $H \subseteq \mathbb{R}^{r+s}$ given by $y_1 + y_2 + \cdots + y_{r+s} = 0$, and in fact $\psi(U_K) = H \cap \psi(\mathcal{O}_K\backslash\{0\})$.
     - Proof: Observe that $N(\alpha) = \sigma_1(\alpha)\cdots\sigma_r(\alpha)\tau_1(\alpha)\overline{\tau_1(\alpha)}\cdots\tau_s(\alpha)\overline{\tau_s(\alpha)}$ so taking absolute values yields $|N(\alpha)| = |\sigma_1(\alpha)|\cdots|\sigma_r(\alpha)|\cdot|\tau_1(\alpha)|^2\cdots|\tau_s(\alpha)|^2$.
     - Then for $\alpha \in U_K$ we have $|N(\alpha)| = 1$ so for $\psi(\alpha) = (y_1, \cdots, y_{r+s})$ we see $y_1 + \cdots + y_{r+s} = \log|\sigma_1(\alpha)| + \cdots + \log|\sigma_r(\alpha)| + \log|\tau_1(\alpha)|^2 + \log|\tau_s(\alpha)|^2 = \log 1 = 0$ as claimed.
     - Conversely, if $\alpha \in \mathcal{O}_K\backslash\{0\}$ has $\psi(\alpha) = (y_1, \cdots, y_{r+s})$ where $y_1 + \cdots + y_{r+s} = 0$ then by the same calculation we see $|N(\alpha)| = |\sigma_1(\alpha)|\cdots|\sigma_r(\alpha)|\cdot|\tau_1(\alpha)|^2\cdots|\tau_s(\alpha)|^2 = 1$ and so α is a unit.
  3. If B is any bounded subset of $\mathbb{R}^{r+s}$, then $\psi^{-1}(B) \cap \mathcal{O}_K$ is finite, hence $\psi^{-1}(B) \cap U_K$ is also finite.
     - Proof: As noted earlier, ψ is the composition of the Minkowski map $\varphi : K^\times \to \mathbb{R}^n\backslash\{0\}$ with the logarithmic map $\log : \mathbb{R}^n\backslash\{0\} \to \mathbb{R}^{r+s}$ via $\log(x_1, \ldots, x_r, y_1, z_1, \ldots, y_s, z_s) = (\log|x_1|, \ldots, \log|x_r|, \log(y_1^2+z_1^2), \ldots, \log(y_s^2+z_s^2))$.

- If B is bounded in $\mathbb{R}^{r+s}$ then the inverse image of B under the logarithmic map is obviously bounded in $\mathbb{R}^n$. Then because $\varphi(\mathcal{O}_K)$ is a lattice, we see that $\varphi(\mathcal{O}_K) \cap \log^{-1}(B)$ is finite, since any lattice has only finitely many elements in any bounded region.
- Finally, since φ is injective, taking the inverse image under φ shows that $\mathcal{O}_K \cap \psi^{-1}(B)$ is also finite, hence so is $U_K \cap \psi^{-1}(B)$ since U_K is a subset of $\mathcal{O}_K$.

4. The kernel $\ker(\psi)$ is finite and consists of the roots of unity in K.
   - Proof: The first part is immediate by taking $B = \{0\}$ in (3). Then because $\ker(\psi)$ is a finite subgroup of the unit group, all its elements must be roots of unity.
   - On the other hand, since $|\sigma(\zeta)| = 1$ for any complex embedding σ and any root of unity ζ, so $\ker(\psi)$ does contain all roots of unity in K, so $\ker(\psi)$ is precisely the roots of unity in K.
5. The image $\psi(U_K)$ is a lattice of rank at most $r + s - 1$.
   - Proof: By (3), $\psi(U_K)$ has the property that its intersection with any bounded subset of $\mathbb{R}^{r+s}$ is finite. Since it is an additive subgroup of $\mathbb{R}^{r+s}$ by (1), it is a lattice, and therefore its rank is at most $r + s$.
   - But by (2) we see that $\psi(U_K)$ is contained in a hyperplane hence its rank cannot be $r+s$ (since this is incompatible with being a subset of a codimension-1 subspace of $\mathbb{R}^{r+s}$), so the rank is at most $r + s - 1$.
6. The unit group U_K is a finitely generated abelian group of rank at most $r + s - 1$.
   - Proof: This is immediate from applying the first isomorphism theorem to (4) and (5).
7. For any fixed embedding σ of K (real or nonreal), there exists a positive constant C such that for any nonzero $\alpha \in \mathcal{O}_K$ there exists a nonzero $\beta \in \mathcal{O}_K$ with $|N(\beta)| \leq C$ and such that $\log|\sigma_i(\beta)| < \log|\sigma_i(\alpha)|$ for all embeddings $\sigma_i \neq \sigma$.
   - Proof: Suppose that $\psi(\alpha) = (a_1, \ldots, a_r, a_{r+1}, \ldots, a_{r+s})$.
   - Let B be the region in $\mathbb{R}^n$ defined by $|x_1| < c_1$, ... , $|x_r| < c_r$ and $y_1^2 + z_1^2 < c_{r+1}$, ... , $y_s^2 + z_s^2 < c_{r+s}$ where the c_i are chosen so that $0 < c_i < e^{a_i}$ for each a_i except the one corresponding to the special embedding σ, which is chosen (potentially to be very large) so that $c_1 c_2 \cdots c_{r+s} = (\frac{4}{\pi})^s \sqrt{|\operatorname{disc} K|}$.
   - Then B is an open convex centrally-symmetric region with n-measure equal to $(2c_1)\cdots(2c_r)(\pi c_{r+1})\cdots(\pi c_{r+s}) = 2^r \pi^s (\frac{4}{\pi})^s \sqrt{|\operatorname{disc} K|} = 2^{r+2s}\sqrt{|\operatorname{disc} K|} = 2^n \sqrt{|\operatorname{disc} K|}$, hence by Minkowski's lattice theorem it contains a nonzero element $\varphi(\beta)$ of the lattice $\Lambda = \varphi(\mathcal{O}_K)$ where φ is the Minkowski map. (Recall that as we have previously shown, the covolume of Λ is $\sqrt{|\operatorname{disc} K|}$.)
   - Then β has $|N(\beta)| \leq (\frac{4}{\pi})^s \sqrt{|\operatorname{disc} K|}$ and $\log|\sigma_i(\beta)| < \log c_i = a_i = \log|\sigma_i(\alpha)|$ for each $\sigma_i \neq \sigma$, so we may take $C = (\frac{4}{\pi})^s \sqrt{|\operatorname{disc} K|}$.
8. For any fixed embedding σ of K (real or nonreal), there exists a unit $u \in U_K$ such that $\log|\sigma_i(u)| < 0$ for all $\sigma_i \neq \sigma$, and with $\log|\sigma(u)| > 0$.
   - Proof: Let α_1 be an arbitrary element of $\mathcal{O}_K$ and apply (7) iteratively to obtain a sequence of nonzero elements $\alpha_1, \alpha_2, \ldots$ of elements of $\mathcal{O}_K$ such that $\log|\sigma_i(\alpha_{k+1})| < \log|\sigma_i(\alpha_k)|$ for each $\sigma_i \neq \sigma$, where the norms $|N(\alpha_k)|$ are uniformly bounded above by the constant C.
   - Then since there are only finitely many ideals with norm bounded by C, there are only finitely many possibilities for the principal ideals (α_k), and so by the pigeonhole principle, two of them must be equal.
   - If $(\alpha_a) = (\alpha_b)$ with $a < b$ then α_a and α_b are associates: then the unit $u = \alpha_a^{-1}\alpha_b$ has $\log|\sigma_i(u)| = \log|\sigma_i(\alpha_a)| - \log|\sigma_i(\alpha_b)| < 0$ for each $\sigma_i \neq \sigma$.
   - Finally, by (2), since the sum $\sum_i \log|\sigma_i(u)|$ is zero and all terms with $\sigma_i \neq \sigma$ are negative, the remaining term $\log|\sigma(u)|$ must be positive.
9. The unit group U_K is a finitely generated abelian group of rank equal to $r+s-1$ whose torsion subgroup consists of the roots of unity in K.
   - Exercise: Suppose that M is an $m \times m$ real matrix whose diagonal entries are positive, whose off-diagonal entries are negative, and whose row sums are all zero. Show that M has rank $m - 1$ and that any $m - 1$ columns are a basis for M. [Hint: Suppose there is a linear dependence involving $m - 1$ of the columns. Rescale to assume that the largest coefficient a_k of the dependence is 1 and the others are at most 1. Look at the kth row to obtain a contradiction.]

- Proof: Using (8), construct units $u_1, u_2, \ldots, u_{r+s}$ such that $\log|\sigma_i(u_j)|$ is negative when $i \neq j$ and positive when $i = j$. By the exercise above, the rank of the $(r+s) \times (r+s)$ matrix M whose (i,j)-entry is $\log|\sigma_i(u_j)|$ is equal to $r+s-1$. Thus, the logarithms of (any) of $r+s-1$ of these units are additively independent, hence the units themselves are multiplicatively independent.
- We conclude that the rank of U_K as an abelian group is at least $r+s-1$, so together with (6) we see its rank is exactly $r+s-1$. Finally, the statement about torsion was already shown earlier.

- From (9) we see that if we take $u_1, \ldots, u_{r+s-1}$ to be any set of generators for the torsion-free part of U_K, then the full set of units in K are those elements of the form $u = \zeta u_1^{a_1} \cdots u_{r+s-1}^{a_{r+s-1}}$ for some root of unity $\zeta \in K$ and any integers $a_1, \ldots, a_{r+s-1}$.

- Definition: For any number field K with signature (r,s), the unit rank of K is $r+s-1$. We say that units $u_1, \ldots, u_{r+s-1}$ form a fundamental system of units when all units of K can be written in the form $\zeta u_1^{a_1} \cdots u_{r+s-1}^{a_{r+s-1}}$ for some root of unity $\zeta \in K$ and some integers $a_1, \ldots, a_{r+s-1}$. Equivalently, $u_1, \ldots, u_{r+s-1}$ are a fundamental system of units when they generate the torsion-free part of the unit group U_K.

  - We can see immediately that $\mathbb{Q}$ of signature $(1,0)$ and the imaginary quadratic fields $\mathbb{Q}(\sqrt{D})$ for $D < 0$ with signature $(0,1)$ are the only fields with unit rank zero.
  - In general it can be quite difficult to construct a fundamental system of units. In principle, however, the argument used in the proof above (constructing units with most of their complex embeddings small, with only one that is large) can be converted into a computational algorithm.

- Before moving further, we will mention also that the matrix considered in the proof of (9), whose entries are the logarithms of the absolute values of the various complex embeddings of a set of generators of the unit group, turns out to carry important information as well.

- Definition: For a number field K and any units $w_1, \ldots, w_{r+s-1} \in \mathcal{O}_K$, we define their regulator $R(w_1, \ldots, w_{r+s-1})$ to be the absolute value of the determinant of the matrix $\{\log|\sigma_i(\omega_j)|\}_{1 \leq i,j \leq r+s-1}$ whose entries are the logarithms of the absolute values of the real and nonconjugate complex embeddings, with one embedding omitted. (We take the regulator of the empty set to be 1.)

  - Although the definition involves various choices (the ordering of the embeddings, which embedding is omitted) it is easy to see from the properties of determinants and the fact that $\sum_i \log|\sigma_i(u)| = 0$ for any unit u, that the choices do not affect the value of the regulator.
  - Additionally, we see that $R(w_1, \ldots, w_{r+s-1})$ is zero if and only if the units $w_1, \ldots, w_{r+s-1}$ are multiplicatively dependent, as follows immediately by writing $w_1, \ldots, w_{r+s-1}$ in terms of a fundamental system of units.
  - In the same way, by changing basis we see that $R(w_1, \ldots, w_{r+s-1}) = R(u_1, \ldots, u_{r+s-1})$ if $u_1, \ldots, u_{r+s-1}$ is another fundamental system of units, so the regulators of any fundamental system of units are the same: thus, we refer to this quantity as the regulator of K.

- The real quadratic fields $\mathbb{Q}(\sqrt{D})$ with $D > 0$ have signature $(2,0)$ hence have unit rank 1. Thus, their unit groups are of the form $U_K = \{\pm u^d : d \in \mathbb{Z}\}$ for a fundamental unit u.

  - For real quadratic fields, we can find the fundamental unit explicitly by finding the minimal solution to the Pell equation $a^2 - Db^2 = \pm 4$ in integers a, b; then the fundamental unit is $u = \frac{1}{2}(a + b\sqrt{D})$. (When $D \equiv 2, 3 \pmod 4$ we can instead just solve $a^2 - Db^2 = \pm 1$ and use $u = a + b\sqrt{D}$.)
  - Exercise: Suppose K is a real quadratic field. Show that there are four possible fundamental units, and if one of them is u then the others are $-u$, $\overline{u}$, and $-\overline{u}$. Conclude that there is a unique fundamental unit of the form $a + b\sqrt{D}$ where $a, b \in \mathbb{Q}$ are positive, and indeed that among all units of $\mathcal{O}_K$ with positive coefficients, the fundamental unit is the one with a and b minimal.
  - By the observations above, we can find the fundamental units for real quadratic fields $\mathbb{Q}(\sqrt{D})$ by finding the minimal positive solution to the corresponding Pell equation. Here are some examples for small D, which can be found by inspection or a brief search:

D	2	3	5	6	7	10	11	13
Fund. Unit	$1+\sqrt{2}$	$2+\sqrt{3}$	$(1+\sqrt{5})/2$	$5+2\sqrt{6}$	$8+3\sqrt{7}$	$3+\sqrt{10}$	$10+3\sqrt{11}$	$(3+\sqrt{13})/2$
Norm	-1	1	-1	1	1	-1	1	-1

- We mention also that the regulator of a real quadratic field $\mathbb{Q}(\sqrt{D})$ is the logarithm of its fundamental unit $a+b\sqrt{D}$ (where as above we choose the fundamental unit with a, b positive).
- Exercise: Suppose $K = \mathbb{Q}(\sqrt{D})$. Show that the fundamental unit of K is of the form $a+b\sqrt{D}$ with $a, b \in \mathbb{Z}$ whenever $D \not\equiv 5 \pmod 8$.

0.28 (Nov 7) Examples of Unit Groups

- For larger D, we require some deeper results from continued fractions and Pell's equation to compute the fundamental unit in an efficient manner.
  - We recall the notation $[a_0, a_1, \ldots, a_k] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\cdots + \cfrac{1}{a_k}}}$ for a finite continued fraction and $[a_0, a_1, \ldots] = \lim_{k\to\infty}[a_0, a_1, \ldots, a_k]$ for an infinite continued fraction. Any irrational number α has a unique continued fraction expansion with all $a_i \in \mathbb{Z}$ and $a_i > 0$ for $i > 0$, which may be computed recursively via $a_0 = \lfloor \alpha \rfloor$ and $[a_1, a_2, \ldots] = \dfrac{1}{\alpha - a_0}$.
  - A basic result in Diophantine approximation states that if α is irrational and $\dfrac{p}{q}$ is rational with $\left|\alpha - \dfrac{p}{q}\right| < \dfrac{1}{2q^2}$, then in fact $\dfrac{p}{q}$ is a continued fraction convergent to α.
  - It is then a straightforward inequality chase to deduce that if $r \in \mathbb{Z}$ has $r^2 + |r| < D$, then if x and y are positive integers with $x^2 - Dy^2 = r$ then $\dfrac{x}{y}$ is a continued fraction convergent to $\sqrt{D}$.
  - As noted above, to find the fundamental unit, we must solve the Pell's equation $x^2 - Dy^2 = \pm 1$ or ± 4 depending on D, so for $D > 20$, the fundamental unit is always obtained from a continued fraction convergent to $\sqrt{D}$.
  - By a somewhat tedious analysis, one may show that the continued fraction expansion of $\sqrt{D}$ is periodic and of the form $[a_0, \overline{a_1, a_2, \cdots, a_{k-1}, 2a_0}]$ with $a_0 = \lfloor \sqrt{D} \rfloor$, and this expansion may be tabulated efficiently using a method sometimes referred to as the "super magic box":
    - The rows in the table are the sequences A_n, C_n, a_n, p_n, q_n, and $p_n^2 - Dq_n^2 = (-1)^n C_{n+1}$.
    - We compute the sequences a_n, A_n, C_n via the recurrences $A_{n+1} = a_n C_n - A_n$, $C_{n+1} = (D - A_{n+1}^2)/C_n$, and $a_{n+1} = \lfloor (A_{n+1} + a_0)/C_{n+1} \rfloor$ with initial conditions $A_0 = 0$, $C_0 = 1$, and $a_0 = \lfloor \sqrt{D} \rfloor$. Once we reach a term with $C_k = 1$ (or when $D \equiv 1 \bmod 4$, the value $C_k = 4$) we stop, since we will have finished computing the necessary continued fraction expansion in the previous step.
    - We can then evaluate the convergents p_n/q_n using the recurrence relations $p_n = a_n p_{n-1} + p_{n-2}$ and $q_n = a_n q_{n-1} + q_{n-2}$ with initial conditions $p_{-1} = 1$, $p_0 = a_0$, $q_{-1} = 0$, $q_0 = 1$.
- Example: Find the fundamental unit of $\mathbb{Q}(\sqrt{14})$.
  - Here is the result of doing the super magic box calculation:

n	-1	0	1	2	3	4
$A_n = a_{n-1}C_{n-1} - A_{n-1}$		0	3	2	2	3
$C_n = (D - A_n^2)/C_{n-1}$		1	5	2	5	$\boxed{1}$
$a_n = \lfloor (A_n + a_0)/C_n \rfloor$		3	1	2	1	6
$p_n = a_n p_{n-1} + p_{n-2}$	1	3	4	11	15	101
$q_n = a_n q_{n-1} + q_{n-2}$	0	1	1	3	4	27
$p_n^2 - 14q_n^2$		-5	2	-5	1	-5

  - Since 14 is not 1 mod 4, we continue until obtaining $C_4 = 1$ and then compute the previous convergent $p_3/q_3 = 15/4$.
  - This tells us that the fundamental unit of $\mathbb{Z}[\sqrt{14}]$ is $15 + 4\sqrt{14}$, with norm $(-1)^4 C_4 = 1$.
- Example: Find the fundamental unit of $\mathbb{Q}(\sqrt{61})$.

- Here is the result of doing the super magic box calculation:

n	-1	0	1	2	3
$A_n = a_{n-1}C_{n-1} - A_{n-1}$		0	7	5	7
$C_n = (D - A_n^2)/C_{n-1}$		1	12	3	$\boxed{4}$
$a_n = \lfloor (A_n + a_0)/C_n \rfloor$		7	1	4	3
$p_n = a_n p_{n-1} + p_{n-2}$	1	7	8	39	125
$q_n = a_n q_{n-1} + q_{n-2}$	0	1	1	5	16
$p_n^2 - 14q_n^2$		-12	3	-4	9

- Since $61 \equiv 1 \pmod 4$ we stop once we obtain $C_3 = 4$, and then the previous convergent is $p_2/q_2 = 39/5$.
- This tells us that the fundamental unit of $\mathbb{Z}[\sqrt{14}]$ is $\frac{1}{2}(39 + 5\sqrt{61})$, with norm $(-1)^3 C_3/4 = -1$.

- Exercise: Find the fundamental units for the quadratic fields $\mathbb{Q}(\sqrt{D})$ for $D = 15, 17, 19, 21, 22, 23, 26$.

- Unfortunately, we do not have an analogous criterion like the one provided by the basic theory of Pell's equation that allows us to construct the fundamental unit for other classes of fields.
  - For certain classes of fields, however, we can make some basic estimates that will allow us at least to identify with certainty the fundamental unit in some examples.
  - For instance, the pure cubic fields $\mathbb{Q}(\sqrt[3]{D})$ also have signature $(1,1)$ so they likewise have unit rank 1, and their unit groups are also of the form $U_K = \{\pm u^d : d \in \mathbb{Z}\}$ for a fundamental unit u. If we can find a unit u that seems "small", if we can obtain a lower bound on the size of u, we can attempt to use the bound to show that u is actually the fundamental unit.
  - So suppose K is any cubic field with signature $(1,1)$ and discriminant D, and let u be a fundamental unit. Implicitly identifying u with its real embedding, then by negating or taking a reciprocal as necessary we may assume $u > 1$.
  - Then the three complex embeddings of u are u, re^{it}, re^{-it} for some $r > 0$ and $t \in (0, 2\pi)$, so $N(u) = ur^2$ hence $r = u^{-1/2}$ since ur^2 is positive and $N(u) = \pm 1$. Then

$$\begin{aligned} -\tfrac{1}{4}\text{disc}(u) &= -\tfrac{1}{4}(u - re^{it})^2(u - re^{-it})^2(re^{it} - re^{-it})^2 = [u^2 - 2ur\cos t + r^2]^2 \cdot (r^2 \sin t) \\ &= \sin^2 t \cdot (u^{3/2} - 2\cos t + u^{-3/2})^2 \\ &= (u^{3/2} + u^{-3/2})^2 - [(u^{3/2} + u^{-3/2})\cos t + 2\sin^2 t]^2 + 4\sin^2 t \\ &\le (u^{3/2} + u^{-3/2})^2 + 4 = u^3 + u^{-3} + 6 \end{aligned}$$

    which yields a quadratic inequality in u^3 that is easy enough to solve explicitly to get a lower bound on u in terms of $|\text{disc}(K)| \le |\text{disc}(u)|$.
  - A slightly weaker estimate that is often good enough is easily obtained by noting that because $u > 1$, we have $u^3 \ge \frac{1}{4}|D| - 6 - u^{-3} > \frac{1}{4}|D| - 7$.

- Example: Show that $1 + \sqrt[3]{2} + \sqrt[3]{4}$ is the fundamental unit of $\mathbb{Q}(\sqrt[3]{2})$.
  - Using the norm formula $N(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = a^3 + 2b^3 + 4c^3 - 6abc$ we see that this element does have norm -1 hence it is a unit, and it (obviously) is not a root of unity, so since it is greater than 1, it must be some positive power of the fundamental unit u.
  - Since $\text{disc}(K) = -108$, the (real embedding of the) fundamental unit u satisfies $u \ge (\frac{1}{4} \cdot 108 - 7)^{1/3} \approx 2.7144$ by our analysis above. (Alternatively, solving $u^3 + u^{-3} + 6 \ge 27$ directly yields $u \ge 2.7568$, so we see the weaker estimate is fairly close anyway.)
  - But now because $1 + \sqrt[3]{2} + \sqrt[3]{4} \approx 3.8473$, we can see that this element is less than u^2 (which must be greater than 7), so it must equal u itself.

- Exercise: For $\alpha^3 - \alpha + 1 = 0$, show that α is the fundamental unit of $\mathbb{Q}(\alpha)$.

- Exercise: Show that $4 + 2\sqrt[3]{7} + \sqrt[3]{49}$ is the fundamental unit of $\mathbb{Q}(\sqrt[3]{7})$.

- Exercise: Show that $\frac{1}{3}(23 + 11\sqrt[3]{10} + 5\sqrt[3]{100})$ is the fundamental unit of $\mathbb{Q}(\sqrt[3]{10})$.

- Finding units in other classes of fields is generally even more difficult, but we can still make some remarks about the cyclotomic fields.
  - The cyclotomic fields $\mathbb{Q}(\zeta_n)$ for $n > 2$ are totally complex hence have signature $(0, \frac{1}{2}\varphi(n))$, so in general they have unit rank $\frac{1}{2}\varphi(n) - 1$.
  - Since $\varphi(n)$ grows (generally) as n grows, we can only hope to construct systems of fundamental units explicitly when n is small.
- We can collect some basic results about units in cyclotomic fields. A full characterization of the units in general cyclotomic fields is quite difficult to come by, but we can at least construct some examples of units.
- Proposition (Some Units in Cyclotomic Fields): Let $n \geq 3$. Noting that $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{2n})$ when n is odd, assume further that $n \not\equiv 2 \pmod 4$.
  1. The roots of unity in $K = \mathbb{Q}(\zeta_n)$ are $\pm\zeta_n^d$ for integers d.
     - Proof: Clearly all of these elements are roots of unity in K. To show these are all of the roots of unity in K, suppose n has prime factorization $n = 2^{n_1} \cdots p_k^{n_k}$ and the order of u has prime factorization $\mathrm{ord}(u) = 2^{u_1} \cdots p_k^{u_k}$: we want to show that $\mathrm{ord}(u)$ divides $2n$ if n is odd, and otherwise divides n.
     - We can see that $u^{\mathrm{ord}(u)/p_i^{u_i}}$ is a primitive $p_i^{u_i}$th root of unity for each i, and conversely u can be written as a product of $p_i^{u_i}$th roots of unity by the Chinese Remainder Theorem, so saying $u \in K$ is equivalent to saying that $\mathbb{Q}(\zeta_{p_i^{u_i}})$ is a subfield of K for each prime power $p_i^{u_i}$.
     - But as we have previously noted, $\mathbb{Q}(\zeta_a) \cap \mathbb{Q}(\zeta_b) = \mathbb{Q}(\zeta_{\gcd(a,b)})$, so $\mathbb{Q}(\zeta_{p_i^{u_i}}) \cap \mathbb{Q}(\zeta_n)$ can only equal $\mathbb{Q}(\zeta_{p_i^{u_i}})$ when the field degrees $\varphi(p_i^{u_i})$ and $\varphi(\gcd(p_i^{u_i}, n)) = \varphi(p_i^{\min(u_i, n_i)})$ are equal. It is easy to see that this occurs if and only if $n_i \geq u_i$, or when $n_i = 0$, $u_i = 1$, and $p_i = 2$.
     - Equivalently, when $n_2 > 0$ (i.e., when n is odd) this means $n_i \geq u_i$ for all i whence $\mathrm{ord}(u)$ divides n, and when $n_2 = 0$ (i.e., when n is even) we have $n_i \geq u_i$ for all i except $i = 2$ where potentially $u_i = n_i + 1$: this means instead that $\mathrm{ord}(u)$ will divide $2n$.
  2. The field $K = \mathbb{Q}(\zeta_n)$ is totally complex, and its maximal real subfield $K_+ = K \cap \mathbb{R} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ is totally real, and K/K_+ is an extension of degree 2.
     - Proof: All of the complex embeddings ζ_n^k of ζ_n are nonreal, so K is totally complex, and so in particular $[K : K \cap \mathbb{R}] > 1$.
     - Additionally, clearly $\zeta_n + \zeta_n^{-1} = 2\cos(2\pi/n)$ is real, as are all of its Galois conjugates $\zeta_n^k + \zeta_n^{-k} = 2\cos(2\pi k/n)$ for $k \in \mathbb{Z}$, so the field K_+ is totally real and is contained in $K \cap \mathbb{R}$.
     - On the other hand, since ζ_n is a root of the quadratic polynomial $m(x) = x^2 - (\zeta_n + \zeta_n^{-1})x + 1$ in $K_+[x]$, we see that $[K : K_+] \leq 2$. But then $1 < [K : K \cap \mathbb{R}] \leq [K : K_+] \leq 2$, so in fact $K \cap \mathbb{R} = K_+$ and $[K : K_+] = 2$, as claimed.
     - Exercise: Show that the unit ranks of $K = \mathbb{Q}(\zeta_n)$ and $K_+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ are both equal to $\frac{1}{2}\varphi(n) - 1$.
     - The same phenomenon occurs (rather more trivially) with the imaginary quadratic fields and their proper subfield $\mathbb{Q}$, and in fact it turns out this is essentially the only situation where a field can have a proper subfield with the same unit rank:
     - Exercise: Suppose that L/K is an extension of number fields. Show that L and K have the same unit rank if and only if L is totally complex, K is totally real, and $[L : K] = 2$, in which case $K = L \cap \mathbb{R}$ is the maximal real subfield of L.
  3. Let p be an odd prime and $K = \mathbb{Q}(\zeta_p)$ with $K_+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$. Then any unit u in $\mathcal{O}_K$ can be written in the form $\zeta^b w$ where w is a unit of $\mathcal{O}_{K_+}$: in other words, u is a root of unity times a real unit.
     - Note that the exercise following (2) explains why this is plausible, because the unit ranks of $\mathcal{O}_K$ and $\mathcal{O}_{K_+}$ are the same, so the quotient group of the units of $\mathcal{O}_K$ modulo the units of $\mathcal{O}_{K_+}$ is finite. (We note that in general, the quotient need not just consist of the nonreal roots of unity in K, since the free part of the unit group of $\mathcal{O}_{K_+}$ could be a proper subgroup of the free part of the unit group of $\mathcal{O}_K$.)
     - Proof: Let $\alpha = u/\overline{u}$. Then α is an algebraic integer since $\overline{u}$ is a unit. Additionally, for any complex embedding σ, we see $|\sigma(\alpha)| = |\sigma(u)/\sigma(\overline{u})| = \left|\sigma(u)/\overline{\sigma(u)}\right| = 1$ since complex conjugation commutes with σ and any complex number has the same absolute value as its conjugate.

- Thus we see $u/\overline{u}$ is an algebraic integer all of whose conjugates have absolute value 1, which (by an earlier exercise) implies that $u/\overline{u}$ is a root of unity in K.
- Since the roots of unity in K are of the form $\pm\zeta_p^d$ that means $u/\overline{u} = \pm\zeta_p^d$.
- If we had $u/\overline{u} = -\zeta_p^d$ then for $u = c_0 + c_1\zeta_p + \cdots + c_{p-2}\zeta_p^{p-2}$ we see $u \equiv c_0 + \cdots + c_{p-2} \pmod{1-\zeta}$, and so $\overline{u} = c_0 + c_0\zeta_p^{-1} + \cdots + c_{p-2}\zeta_p^{-(p-2)} \equiv c_0 + \cdots + c_{p-2} \equiv u \equiv -\zeta_p^d\overline{u} \equiv -\overline{u} \pmod{1-\zeta_p}$. But this would imply $2\overline{u} \equiv 0 \pmod{1-\zeta_p}$ hence $2 \in (1-\zeta_p)$ since $\overline{u}$ is a unit: but $(1-\zeta_p)$ lies above the integer prime $p \neq 2$, so this is impossible.
- So in fact we have $u/\overline{u} = \zeta_p^d$ for some d. Letting $d \equiv 2b \pmod{p}$ and $w = \zeta_p^{-b}u$, we see that $\overline{w} = \zeta_p^b\overline{u} = \zeta_p^{-b}u = w$ so w is real and has $u = \zeta_p^b w$, as desired.

4. Let p be an odd prime and $K = \mathbb{Q}(\zeta_p)$ with $K_+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$. Then the unit group of $\mathcal{O}_K$ is the direct product of the group of pth roots of unity with the units of $\mathcal{O}_{K_+}$.
   - Proof: This follows immediately from (1) and (2), after noting that both K and K_+ contain ± 1.
   - Remark: More generally, it can be shown (with much more difficulty) that the product of the roots of unity in K with the units of $\mathcal{O}_K$ for $K = \mathbb{Q}(\zeta_n)$ always generates either the full unit group of $\mathcal{O}_K$, or an index-2 subgroup.
5. Let p be a prime and $K = \mathbb{Q}(\zeta_{p^d})$. Then for any integers a, b relatively prime to p, the element $(\zeta_{p^d}^a - 1)/(\zeta_{p^d}^b - 1)$ is a unit of $\mathcal{O}_K$.
   - Proof: Since b is invertible modulo p^d, there exists t with $a \equiv tb \pmod{p^d}$. Then $(\zeta_{p^d}^a - 1)/(\zeta_{p^d}^b - 1) = (\zeta_{p^d}^{tb} - 1)/(\zeta_{p^d}^b - 1) = \zeta_{p^d}^{(t-1)b} + \cdots + \zeta_{p^d}^b + 1 \in \mathcal{O}_K$.
   - By interchanging a, b we see that $(\zeta_{p^d}^b - 1)/(\zeta_{p^d}^a - 1)$ is also in $\mathcal{O}_K$, so both elements are units.
6. Suppose n has at least two distinct prime factors and let $K = \mathbb{Q}(\zeta_n)$. Then $1 - \zeta_n$ is a unit of $\mathcal{O}_K$.
   - Contrast this result with the case where $n = p^d$ is a prime power above: in that case $(1 - \zeta_{p^d})$ is a prime ideal lying over p, so $1 - \zeta_{p^d}$ is certainly not a unit!
   - Proof: From the factorization $\Phi_n(x) = \prod_{d|n}(x^d - 1)^{\mu(n/d)}$, divide each term on the right by $x - 1$. This introduces a net factor of $(x-1)^s$ where $s = \sum_{d|n}\mu(n/d)$, but this sum is easily seen to be zero whenever n has 2 or more prime factors.
   - So $\Phi_n(x) = \prod_{d|n}(x^{d-1} + \cdots + 1)^{\mu(n/d)}$; now setting $x = 1$ produces $\Phi_n(1) = \prod_{d|n} d^{\mu(n/d)} = 1$ as can be seen directly by decomposing n as a product of primes.
   - But then $N_{K/\mathbb{Q}}(1 - \zeta_n) = \prod_{\gcd(k,n)=1}(1 - \zeta_n^k) = \Phi_n(1) = 1$ so $1 - \zeta_n$ is a unit, as claimed.
7. For any a relatively prime to n, the circular unit $\omega_a = \zeta_n^{(1-a)/2}\dfrac{1-\zeta_n^a}{1-\zeta_n} = \dfrac{\zeta_n^{-a/2} - \zeta_n^{a/2}}{\zeta_n^{-1/2} - \zeta_n^{1/2}} = \dfrac{\sin(\pi a/n)}{\sin(\pi/n)}$ is a unit in $\mathcal{O}_K$ for $K_+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ hence also a unit in $\mathcal{O}_K$ for $K = \mathbb{Q}(\zeta_n)$.
   - Proof: When n is a prime power, this follows from (5), and when n is not a prime power, this follows from (6).
   - Remark: With some additional work one may show that the circular units of $\mathbb{Q}(\zeta_{p^d})$ for $1 < a < \frac{1}{2}p^d$ and p not dividing a, generate all of the circular units, and that the regulator of this set of circular units is nonzero: thus, they generate a finite-index subgroup of the full unit group of $\mathbb{Q}(\zeta_{p^d})$.

- By exploiting the maximal real subfield it is possible in some cases to compute the unit group exactly.
- Example: Show that $1 + \zeta_5$ is a fundamental unit for $\mathbb{Q}(\zeta_5)$.
  - Since $\mathbb{Q}(\zeta_5)$ has signature $(0, 2)$, its unit rank is 1. By (4) of the proposition above, we only need to find the fundamental unit of its maximal real subfield $\mathbb{Q}(\zeta_5 + \zeta_5^{-1})$. This is the quadratic subfield of $\mathbb{Q}(\zeta_5)$, which since $\mathbb{Q}(\zeta_5)$ has discriminant 5^2, must be ramified only at 5, hence can only be $\mathbb{Q}(\sqrt{5})$.
  - Indeed, we can see this more directly by noting that for $\alpha = \zeta_5 + \zeta_5^4$ with Galois conjugate $\beta = \zeta_5^2 + \zeta_5^3$, we have $\alpha + \beta = \alpha\beta = -1$ which both follow from using $\Phi_4(\zeta_5) = 0$, so α, β are roots of the quadratic $x^2 + x - 1 = 0$ whence $\alpha, \beta = \frac{-1 \pm \sqrt{5}}{2}$, and indeed by trivially observing that the real part of α is positive we see $\beta = -\frac{1+\sqrt{5}}{2}$ is the negative of the fundamental unit of $\mathbb{Q}(\sqrt{5})$.

- Thus by (4) above, we see that every unit of $\mathbb{Q}(\zeta_5)$ is of the form $\pm\zeta_5^a\beta^d$ for some d, and since $\beta = \zeta_5^2(1+\zeta_5)$ we may substitute to see that the units of $\mathbb{Q}(\zeta_5)$ are all of the form $\pm\zeta_5^c(1+\zeta_5)^d$, and so $1+\zeta_5$ is a fundamental unit.

- Exercise: Show that $1+\zeta_8+\zeta_8^2$ is a fundamental unit for $\mathbb{Q}(\zeta_8)$.

0.29 (Nov 13) Galois Actions, Decomposition and Inertia Groups

- So far, we have not really exploited the action of the Galois group on an extension of number fields in a major way, beyond using it to simplify some calculations with complex embeddings.
  - So let us now study in more detail how Galois groups act on primes and factorizations.

- Proposition (Galois Action on Primes): Let L/K be a Galois extension of number fields with Galois group $G = \mathrm{Gal}(L/K)$, and let P be a nonzero prime ideal of $\mathcal{O}_K$.

  1. If Q is any prime of $\mathcal{O}_L$ lying above P and $\sigma \in G$ is any automorphism, then $\sigma(Q)$ is also a prime lying above P. Thus, σ acts as a permutation on the primes lying above P.
     - Proof: Since L/K is Galois, we see that $\sigma(\mathcal{O}_L) = \mathcal{O}_L$.
     - Then $\mathcal{O}_L/\sigma(Q) = \sigma(\mathcal{O}_L)/\sigma(Q) \cong \sigma(\mathcal{O}_L/Q)$ is a field, so $\sigma(Q)$ is a maximal ideal of $\mathcal{O}_L$.
     - Additionally, since σ fixes K hence also P, since Q contains P we see $\sigma(Q)$ also contains P, so $\sigma(Q)$ also lies above P.
     - Finally, σ is invertible, so it permutes the primes lying above P.
  2. The action of G on the primes of $\mathcal{O}_L$ lying above P is transitive: for any Q, Q' lying above P, there exists some $\sigma \in G$ with $\sigma(Q) = Q'$.
     - Proof: Suppose otherwise, so that there exist primes Q and Q' such that $\sigma(Q) \neq Q'$ for any $\sigma \in G$.
     - Then by the Chinese remainder theorem, there exists some $\alpha \in \mathcal{O}_L$ such that $\alpha \equiv 0 \pmod{Q'}$ and $\alpha \equiv 1 \pmod{\sigma(Q)}$ for all $\sigma \in G$.
     - The latter condition implies $\sigma^{-1}(\alpha) \equiv 1 \pmod{Q}$ for all $\sigma \in G$, and thus we have $N_{L/K}(\alpha) = \prod_{\sigma\in G}\sigma^{-1}(\alpha) \equiv 1 \pmod{Q}$ as well.
     - However, since $\alpha \equiv 0 \pmod{Q'}$ we also have $N_{L/K}(\alpha) \in Q' \cap K = P$: but Q divides $P\mathcal{O}_L$, so this would imply $N_{L/K}(\alpha) \equiv 0 \pmod{Q}$, contradicting the above.
     - Thus, the action of G must be transitive, as claimed.
  3. For any primes Q_1 and Q_2 of $\mathcal{O}_L$ lying over P, we have $e(Q_1|P) = e(Q_2|P)$ and $f(Q_1|P) = f(Q_2|P)$.
     - Proof: Suppose $P\mathcal{O}_L$ has prime factorization $P\mathcal{O}_L = Q_1^{e_1}Q_2^{e_2}\cdots Q_k^{e_k}$. Via (2), let $\sigma \in G$ be such that $\sigma(Q_1) = Q_2$.
     - Then σ fixes both P and $\mathcal{O}_L$, so applying σ yields $P\mathcal{O}_L = \sigma(P\mathcal{O}_L) = \sigma(Q_1)^{e_1}\sigma(Q_2)^{e_2}\cdots\sigma(Q_k)^{e_k} = Q_2^{e_1}\sigma(Q_2)^{e_2}\cdots\sigma(Q_k)^{e_k}$.
     - By unique factorization we immediately have $e_1 = e_2$ so $e(Q_1|P) = e(Q_2|P)$ as claimed.
     - For the second part, observe as in (1) that σ yields a ring isomorphism between $\mathcal{O}_L/Q_1$ and $\mathcal{O}_L/Q_2$, so since both Q_1 and Q_2 lie over P, we see that the vector space dimensions of $\mathcal{O}_L/Q_1$ and $\mathcal{O}_L/Q_2$ over $\mathcal{O}_K/P$ are equal.
     - This means $f(Q_1|P) = f(Q_2|P)$, as desired.
  4. (The efg Theorem) If $Q_1, \ldots, Q_g$ are the primes of $\mathcal{O}_L$ lying over P, with common values $e(Q_i|P) = e$ and $f(Q_i|P) = f$, then $efg = [L:K]$.
     - Proof: We see $[L:K] = \sum_{i=1}^{g} e(Q_i|P)f(Q_i|P) = efg$ immediately from (3) and the ef-theorem.

- As noted in (1) of the proposition above, we have a group action of the Galois group $G = \mathrm{Gal}(L/K)$ on the prime ideals lying over a given P of $\mathcal{O}_K$.
  - It is now natural to consider various kinds of stabilizers for this group action.
  - The most obvious one is the stabilizer of a specific prime Q lying over P: namely, the elements $\sigma \in G$ with $\sigma(Q) = Q$.

- Another obvious one would be the stabilizer of $\mathcal{O}_L$, but any σ fixing $\mathcal{O}_L$ will fix all of L hence must be the identity by the Galois correspondence.
- Instead of the stabilizer of $\mathcal{O}_L$, we can instead consider the stabilizer of $\mathcal{O}_L$ mod Q: in other words, the set of $\sigma \in G$ such that $\sigma(\alpha) \equiv \alpha \pmod{Q}$ for all $\alpha \in \mathcal{O}_L$.

- Definition: Let L/K be a Galois extension of number fields with Galois group G, and let Q be a nonzero prime ideal of $\mathcal{O}_L$ lying over the prime P of $\mathcal{O}_K$. The decomposition group associated to Q is the subgroup of G fixing Q, where explicitly $D(Q|P) = \{\sigma \in G : \sigma(Q) = Q\}$. The inertia group associated to Q is the subgroup of G fixing $\mathcal{O}_L$ mod Q, where explicitly $E(Q|P) = \{\sigma \in G : \sigma(\alpha) \equiv \alpha \pmod{Q} \text{ for all } \alpha \in \mathcal{O}_L\}$.
  - The decomposition and inertia groups are in fact subgroups of G, since they are obviously closed under multiplication and inverses and they contain the identity.
  - When Q is clear from context we will refer to the decomposition and inertia groups simply as D and E respectively.
  - As a first observation, we note that E is a subgroup of D: if $\sigma \in E$, then for any $\alpha \in Q$ we have $\sigma(\alpha) \equiv \alpha \equiv 0 \pmod{Q}$, so $\sigma(\alpha) \in Q$ also. Thus, we must have $\sigma(Q) \subseteq Q$ hence $\sigma(Q) = Q$ since $\sigma(Q)$ is prime, whence $\sigma \in D$.

- Example: Find the decomposition and inertia groups for the primes $Q_2 = (1+i)$, $Q_3 = (3)$, and $Q_5 = (2+i)$ of $K = \mathbb{Q}(i)$.
  - The Galois group for $K/\mathbb{Q}$ is $G = \{1, \sigma\}$ where σ is complex conjugation.
  - For the prime $Q_2 = (1+i)$, we see that the decomposition group $D(Q_2|2) = G$ since $\sigma(Q_2) = Q_2$ and the inertia group $E(Q_2|2) = G$ as well since $\sigma(\alpha) = \overline{\alpha} = \alpha - 2\text{Im}(\alpha) \equiv \alpha \pmod{Q_2}$ for all $\alpha \in \mathcal{O}_L$.
  - For the prime $Q_3 = (3)$ we see that the decomposition group $D(Q_3|3) = G$ since $\sigma(Q_3) = Q_3$, but the inertia group $E(Q_3|3) = 1$ since for example $\sigma(i) \not\equiv i \pmod{Q_3}$.
  - For the prime $Q_5 = (2+i)$ we see that the decomposition group $D(Q_5|5) = 1$ since $\sigma(Q_5) = Q_5' = (2-i)$, and then the inertia group $E(Q_5|5) = 1$ immediately as well since it is a subgroup.

- Exercise: Find the decomposition and inertia groups for the primes $(\sqrt{-2})$, $(1+\sqrt{-2})$, and (5) of $\mathbb{Q}(\sqrt{-2})$.

- Example: Find the decomposition and inertia groups for the primes $Q_2 = (2)$, $Q_5 = (1-\zeta_5)$, and $Q_{11} = (2+\zeta_5)$ of $K = \mathbb{Q}(\zeta_5)$.
  - The Galois group for $K/\mathbb{Q}$ is $G = \{1, \sigma, \sigma^2, \sigma^3\}$ where $\sigma(\zeta_5) = \zeta_5^2$.
  - For the prime $Q_2 = (2)$, we see that the decomposition group $D(Q_2|2) = G$ since $\sigma(Q_2) = Q_2$.
  - On the other hand, the inertia group $E(Q_2|2) = 1$ since $\sigma(\zeta_5) - \zeta_5 = \zeta_5^2 - \zeta_5$ is not in Q_2 (since it is not divisible by 2 in $\mathcal{O}_K = \mathbb{Z}[\zeta_5]$), and neither is $\sigma^2(\zeta_5) - \zeta_5$ or $\sigma^3(\zeta_5) - \zeta_5$.
  - For the prime $Q_5 = (1-\zeta_5)$ which lies above 5 and is in fact totally ramified so that $(5) = Q_5^5$, we must have $\sigma(Q_5) = Q_5$ since Q_5 is the only prime above 5. Thus, $D(Q_5|5) = G$.
  - Exercise: Suppose L/K is a Galois extension with Galois group G and Q is a prime of $\mathcal{O}_L$ lying over P. Show that $D(Q|P) = G$ if and only if Q is the unique prime of $\mathcal{O}_L$ lying over P.
  - For the inertia group, we have $\sigma^d(\zeta_5^k) - \zeta_5^k = \zeta_5^{2^d k} - \zeta_5^k = \zeta_5^k(\zeta_5^{(2^d-1)k} - 1)$ which is divisible by $1 - \zeta_5$ hence lies in Q_5 for all d, k. Thus since $\sigma^d(\alpha) - \alpha \in Q_5$ for an integral basis of $\mathcal{O}_L$ we see $\sigma^d(\alpha) \equiv \alpha \pmod{Q_5}$ for all $\alpha \in \mathcal{O}_L$, so in fact we also have $E(Q_5|5) = G$.
  - Finally, for Q_{11}, which lies above 11, from Dedekind-Kummer and the observation that $N_{K/\mathbb{Q}}(2 + \zeta_5) = 11$, we see that (11) has prime ideal factorization $(11) = (2+\zeta_5)(2+\zeta_5^2)(2+\zeta_5^3)(2+\zeta_5^4) = Q_{11}\sigma(Q_{11})\sigma^3(Q_{11})\sigma^2(Q_{11})$.
  - So the only automorphism fixing Q_{11} is the identity, and so $D(Q_{11}|11) = 1$ hence also $E(Q_{11}|11) = 1$.

- In order to compute additional examples it will be convenient to establish some basic properties of the decomposition and inertia groups first.
  - The fixed fields of D and E, which we will refer to as the decomposition field L_D and the inertia field L_E, also carry important information, as we will now show.

- Proposition (Decomposition and Inertia, I): Let L/K be a Galois extension of number fields with Galois group G. For a nonzero prime ideal Q of $\mathcal{O}_L$ lying over the prime P of $\mathcal{O}_K$, let $D = D(Q|P)$ be the decomposition group and $E = E(Q|P)$ be the inertia group, and also let $e = e(Q|P)$ be the ramification index, $f = f(Q|P)$ be the inertial degree, and $g = g(Q|P)$ be the number of primes lying over P.

  1. The inertia group E is a normal subgroup of D, and the quotient group D/E is cyclic of order dividing $f(Q|P)$.
     - Proof: Suppose $\sigma \in D$. Then σ induces an automorphism of $\mathcal{O}_L$, and since $\sigma(Q) = Q$, it descends to an automorphism $\overline{\sigma}$ of the residue field $F_Q = \mathcal{O}_L/Q$, defined explicitly via $\overline{\sigma}(\alpha + Q) = \sigma(\alpha) + Q$ for $\alpha \in \mathcal{O}_L$.
     - Furthermore, since σ is an element of $\mathrm{Gal}(L/K)$ it fixes $\mathcal{O}_K$ hence $\overline{\sigma}$ fixes $F_P = \mathcal{O}_L/P$.
     - This means $\overline{\sigma}$ is an automorphism of $\mathcal{O}_L/Q$ that fixes $\mathcal{O}_K/P$, so it is an element of the Galois group $\mathrm{Gal}(F_Q/F_P)$.
     - It is then easy to see that the map $\psi : D \to \mathrm{Gal}(F_Q/F_P)$ with $\psi(\sigma) = \overline{\sigma}$ is a group homomorphism.
     - Now we have $\sigma \in \ker\psi \iff \overline{\sigma}$ fixes $\mathcal{O}_L/Q \iff \overline{\sigma}(\alpha + Q) = \alpha + Q$ for all $\alpha \in \mathcal{O}_L \iff \sigma(\alpha) \equiv \alpha \pmod{Q}$ for all $\alpha \in \mathcal{O}_L \iff \sigma \in E$.
     - Hence E is a normal subgroup of D and by the first isomorphism theorem we see that D/E is isomorphic to a subgroup of $\mathrm{Gal}(F_Q/F_P)$.
     - Finally, as we have previously noted, F_Q/F_P is an extension of finite fields of degree $f(Q|P)$, so its Galois group is cyclic of order $f(Q|P)$, generated by the Frobenius map. The conclusion follows.
  2. We have $[G : D] = [L_D : K] = g$, and in fact if $\tau_1, \ldots, \tau_g$ are coset representatives for D in G, then $\tau_1(Q), \ldots, \tau_g(Q)$ are the distinct primes of $\mathcal{O}_L$ lying above P.
     - Proof: As shown earlier, the group action of G on the primes lying above P is transitive, and the stabilizer of Q is the decomposition subgroup D. All of the claimed results then follow immediately from the orbit-stabilizer lemma: the elements in the orbit are obtained as the images under the cosets of the stabilizer, and the size of the orbit is equal to the index of the stabilizer.
  3. Let $Q_D = Q \cap L_D$ be the prime below Q in the decomposition field L_D. Then Q is the only prime of $\mathcal{O}_L$ lying above Q_D, and additionally $e(Q|Q_D) = e$, $f(Q|Q_D) = f$, and $e(Q_D|P) = f(Q_D|P) = 1$.
     - Proof: First observe that the primes of $\mathcal{O}_L$ lying above Q_D are permuted transitively by the Galois group $\mathrm{Gal}(L/L_D) = D$, but all of D sends Q to itself so the action is trivial and Q is the only prime lying above Q_D.
     - By (2) we know $[L_D : K] = g$ so $[L : L_D] = ef$ by the efg-theorem.
     - Then by the efg-theorem again we have $ef = [L : L_D] = e(Q|Q_D)f(Q|Q_D) \leq e(Q|P)f(Q|P) = ef$, so we must have equality everywhere, so $e(Q|P) = e(Q|Q_D)$ and $f(Q|P) = f(Q|Q_D)$.
     - Then since e, f are multiplicative in towers we immediately also have $e(Q_D|P) = f(Q_D|P) = 1$ as claimed.
  4. Let $Q_E = Q \cap L_E$ be the prime below Q in the inertia field L_E. Then Q is the only prime of $\mathcal{O}_L$ lying above Q_E, and also $f(Q|Q_E) = 1$.
     - Proof: The first statement follows immediately from (3), since Q_E lies over Q_D and Q is the only prime lying over Q_D.
     - For the second statement, we must equivalently show that the residue field extension of $F_L = \mathcal{O}_L/Q$ over $F_E = \mathcal{O}_{L_E}/Q_E$ has degree 1, which because this extension is a Galois extension of finite fields, is in turn equivalent to showing that the Galois group of this extension is trivial.
     - So let $\overline{\alpha} \in F_L$ be an element of F_L (for some $\alpha \in \mathcal{O}_L$) and consider the polynomial $g(x) = \prod_{\sigma \in E}(x - \sigma(\alpha))$ in $\mathcal{O}_L[x]$. Applying any automorphism in E to $g(x)$ leaves $g(x)$ fixed, so the coefficients of $g(x)$ in fact lie in $\mathcal{O}_{L_E}$.
     - This means that the reduction $\overline{g(x)} \in F_L[x]$ of $g(x)$ mod Q in fact has coefficients in $F_E[x]$, and so since $\overline{\alpha}$ is a root of $\overline{g(x)}$, $\overline{g(x)}$ must be a multiple of the minimal polynomial of $\overline{\alpha}$ over F_E. But also, since $\sigma(\alpha) \equiv \alpha \pmod{Q}$ for each $\sigma \in E$, we see that $\overline{g(x)} = (x - \overline{\alpha})^{\#E}$ in $F_L[x]$.
     - But now any element τ of $\mathrm{Gal}(F_L/F_E)$ must map $\overline{\alpha}$ to another root of the polynomial $\overline{g(x)}$, but the only possible root is $\overline{\alpha}$, so τ fixes $\overline{\alpha}$. This holds for all elements $\overline{\alpha} \in F_L$, so in fact τ is trivial, hence $\mathrm{Gal}(F_L/F_E)$ is trivial.

5. With Q_D and Q_E as in (3) and (4), we have $f(Q_E|Q_D) = f$ and $[D : E] = f$, whence D/E is cyclic of order f.
   - Proof: From (3) we have $f(Q|Q_D) = f$ and from (4) we have $f(Q|Q_E) = 1$, hence by multiplicativity we see $f(Q_E|Q_D) = f$.
   - Then by the ef-theorem we have $f = f(Q_E|Q_D) \leq [D : E]$ but by (1) we have $[D : E] \geq f$, so we must have equality: $[D : E] = f$. Per (1) this immediately implies that D/E is cyclic of order f.
6. With Q_D and Q_E as in (3) and (4), we have $e(Q_E|Q_D) = 1$ and $e(Q|Q_E) = e$.
   - Proof: From (5) since $f(Q_E|Q_D) = f = [D : E]$ by the ef-theorem we must have $e(Q_E|Q_D) = 1$. Then from (2) since $e(Q|Q_D) = e$, by multiplicativity we must have $e(Q|Q_E) = e$.
7. We have $[L : L_E] = e$, $[L_E : L_D] = f$, and $[L_D : K] = g$. Thus, Q_E is totally ramified from L_E to L, and Q_D is totally inert from L_D to L_E.
   - Proof: Immediate from the previous parts, multiplicativity, and the efg-theorem.

- Exercise: Show that if D is a normal subgroup of G, then P is totally split from K to L_D, and if E is also normal, then each of the primes $Q_D^{(i)}$ of L_D above P are totally inert from L_D to L_E and then are totally ramified from L_E to L. (Thus, we obtain all of the splitting of P in the decomposition field, and then all of the inertia of P in the inertia field, whence the names for these fields.)

0.30 (Nov 14) Decomposition and Inertia, II

- With these basic results about the decomposition and inertia groups and fields in hand, we can explore some more complicated examples.
  - One utility of the decomposition and inertia groups and fields is that they can allow us to obtain results about the splitting of primes in the entire extension by piecing results together from the various subfields, where calculations are easier to perform.

- Example: Let $L = \mathbb{Q}(i, \sqrt{2})$. Analyze the factorization type of the primes 2 and 3 in $\mathcal{O}_L$, and find the decomposition and inertia groups and fields for each associated prime.
  - We note that L is Galois over $\mathbb{Q}$ (being the splitting field of $(x^2+1)(x^2-2)$) with Galois group isomorphic to the Klein 4-group $V_4 = \langle \sigma, \tau \rangle$ where $\sigma(i, \sqrt{2}) = (-i, \sqrt{2})$ and $\tau(i, \sqrt{2}) = (i, -\sqrt{2})$.
  - From Dedekind-Kummer we know that 2 is ramified in all three quadratic subfields $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, and $\mathbb{Q}(\sqrt{-2})$ hence also in L. Therefore, for any prime lying above 2, the decomposition and inertia fields must both be $\mathbb{Q}$, since 2 is unramified in the decomposition and inertia fields.
  - We conclude that $f = g = 1$ and $e = 4$, so that 2 is totally ramified in L and we have the factorization $(2) = Q_2^4$. The decomposition and inertia groups are then both equal to the full Galois group V_4.
  - For 3, we can see that 3 is inert in $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$ but splits in $\mathbb{Q}(\sqrt{-2})$. Therefore, from the last observation, there are at least two primes of $\mathcal{O}_L$ lying above 3, and they must each have $f \geq 2$. Hence by the efg-theorem, we must have $e = 1$, $f = 2$, and $g = 2$, so that $(3) = Q_3 Q_3'$.
  - Then since $[L : L_E] = e$ that means the inertia field $L_E = L$, and the inertia group E is trivial.
  - Additionally, since there are two primes P_3 and P_3' lying above 3 in $\mathbb{Q}(\sqrt{-2})$, by swapping if necessary we may assume Q_3 lies above P_3 and Q_3' lies above P_3': then $f(Q_3|P_3) = f(Q_3'|P_3') = 2$. Indeed, we can compute explicitly $P_3 = (1 + \sqrt{-2})$ and $P_3' = (1 - \sqrt{-2})$, so that $\{1, \sigma\tau\}$ fix P_3 and P_3' while $\{\sigma, \tau\}$ interchange them.
  - From this explicit description we see that the decomposition group of both Q_3 and Q_3' is $D = \langle \sigma\tau \rangle$ and the corresponding decomposition field is $\mathbb{Q}(\sqrt{-2})$.

- Exercise: Let $L = \mathbb{Q}(i, \sqrt{3})$. Analyze the factorization type of the primes 2, 3, and 5 in $\mathcal{O}_L$, and find the decomposition and inertia groups and fields for each associated prime.

- Exercise: Suppose L/K is Galois and Q is a prime of $\mathcal{O}_L$ lying over the prime P of $\mathcal{O}_K$. Show that if $\sigma \in \mathrm{Gal}(L/K)$, then $D(\sigma Q|P) = \sigma D(Q|P)\sigma^{-1}$ and $E(\sigma Q|P) = \sigma E(Q|P)\sigma^{-1}$. Deduce that when G is abelian, all primes of $\mathcal{O}_L$ lying over P have the decomposition and the same inertia subgroups and subfields.

- Example: Let $L = \mathbb{Q}(2^{1/3}, \zeta_3)$. Analyze the factorization type of the primes 2, 3, and 5 in $\mathcal{O}_L$, and find the decomposition and inertia groups and fields for each associated prime.
  - We note that L is Galois over $\mathbb{Q}$ (being the splitting field of $x^3 - 2$) with Galois group isomorphic to $S_3 = \langle \sigma, \tau \rangle$ where $\sigma(2^{1/3}, \zeta_3) = (\zeta_3 2^{1/3}, \zeta_3)$ and $\tau(2^{1/3}, \zeta_3) = (2^{1/3}, \zeta_3^2)$.
  - From Dedekind-Kummer we know that 2 is totally ramified in $\mathbb{Q}(2^{1/3})$ and inert in $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$. So if Q is a prime of $\mathcal{O}_L$ lying above 2, we have $e(Q|2) \geq 3$ and $f(Q|2) \geq 2$, so by the efg-theorem we must have $e = 3$, $f = 2$, and $g = 1$, so that $(2) = Q^3$.
  - Then the decomposition field $L_D(Q|2)$ must be $\mathbb{Q}$, since $[L_D : \mathbb{Q}] = g = 1$, while the inertia field L_E must be $\mathbb{Q}(\zeta_3)$ since $[L_E : L_D] = f = 2$ and $\mathbb{Q}(\zeta_3)$ is the only quadratic subfield of L by the Galois correspondence.
  - For 3, again by Dedekind-Kummer we know that 3 is totally ramified in both $\mathbb{Q}(2^{1/3})$ and $\mathbb{Q}(\zeta_3)$, so if Q_3 is a prime of $\mathcal{O}_L$ lying above 3, then its ramification index $e(Q_3|3)$ is divisible by the ramification index in both subfields, hence must be a multiple of 6. But then by the efg-theorem we must have $e = 6$, $f = 1$, and $g = 1$, so that $(3) = Q_3^6$.
  - Then for Q_3, from the field degrees we see that the decomposition and inertia field must both be $\mathbb{Q}$ and the corresponding decomposition and inertia groups are all of S_3.
  - For 5, by Dedekind-Kummer we know that 5 is partially split in $\mathbb{Q}(2^{1/3})$ as $5 = P_5 P_5'$ where $e(P_5|5) = f(P_5|5) = 1$ while $e(P_5'|5) = 1$ and $f(P_5'|5) = 2$, and in $\mathbb{Q}(\zeta_3)$ we can see that 5 is inert.
  - Therefore, there are at least two primes lying above 5 in $\mathcal{O}_L$. Then we must have $e = 1$, $g \geq 2$, and f be a multiple of 2. The only possibility with $efg = 6$ is then to have $g = 3$ and $f = 2$, so that $(5) = Q_5 Q_5' Q_5''$ where each of Q_5, Q_5', Q_5'' has inertial degree 2.
  - Since Q_5, Q_5', Q_5'' are all unramified, their inertia fields are all L and their inertia groups are trivial.
  - The decomposition fields of Q_5, Q_5', Q_5'' are cubic extensions of $\mathbb{Q}$ inside L, hence are $\mathbb{Q}(2^{1/3})$, $\mathbb{Q}(2^{1/3}\zeta_3)$, $\mathbb{Q}(2^{1/3}\zeta_3^2)$ in some order. By observing that the Galois action is transitive on both the primes and the fields, we see that each cubic field is the decomposition field for one of these primes, and specifically, it is the decomposition field for the prime that lies above the norm-5 prime in that field's ring of integers.
  - For example, if Q_5 is the prime of $\mathcal{O}_L$ that lies above the prime P_5 in $\mathbb{Q}(2^{1/3})$, then since $f(Q_5|P_5) = 2$ that means P_5 is inert from $\mathbb{Q}(2^{1/3})$ to L, and then the conjugation map τ fixes Q_5, hence the decomposition group $D(Q_5|P_5)$ is $\langle \tau \rangle$ and the decomposition field is $\mathbb{Q}(2^{1/3})$.
  - Applying σ, if we then take $Q_5' = \sigma(Q_5)$ to be the prime of $\mathcal{O}_L$ that lies above the prime $\sigma(P_5) = P_5'$ in $\sigma[\mathbb{Q}(2^{1/3})] = \mathbb{Q}(2^{1/3}\zeta_3)$, then the decomposition group $D(Q_5'|P_5')$ is $\langle \tau\sigma^{-1} \rangle$, which is the subgroup fixing the decomposition field $\mathbb{Q}(2^{1/3}\zeta_3)$.

- Exercise: Let $L = \mathbb{Q}(10^{1/3}, \zeta_3)$. Analyze the factorization types of the primes 2, 3, and 5 in $\mathcal{O}_L$, and find the decomposition and inertia groups and fields for each associated prime.

- Example: Let $L = \mathbb{Q}(\zeta_{23})$. Analyze the factorization type of the prime 2 in L, and find the decomposition and inertia groups and fields for its associated primes.
  - For 2, first we note that 2 has order 11 modulo 23. Therefore, per our earlier observations about splitting of primes in cyclotomic fields, we see that (2) factors in $\mathcal{O}_L$ as $(2) = Q_2 Q_2'$ with $e = 1$, $f = 11$, and $g = 2$.
  - Since $e = 1$, the inertia field is simply L itself, and the inertia group is trivial.
  - The decomposition field for both Q_2 and Q_2' has $[L_D : \mathbb{Q}] = g = 2$, but since the Galois group is cyclic, there is only one such field: the unique quadratic subfield of $\mathbb{Q}(\zeta_{23})$. From our results we know that $\sqrt{(-1)^{(23-1)/2} 23^{21}} = \sqrt{\text{disc}(L)} \in L$, so $L_D = \mathbb{Q}(\sqrt{-23})$.
  - The decomposition group is the subgroup of $\text{Gal}(\mathbb{Q}(\zeta_{23}))$ fixing L_D, which corresponds to the unique subgroup of index 2 of $(\mathbb{Z}/23\mathbb{Z})^\times$: explicitly, it is the set of nonzero squares.
  - We can check this calculation by observing that 2 splits in the decomposition field $\mathbb{Q}(\sqrt{-23})$, as $(2) = P_2 P_2'$ where explicitly $P_2 = (2, \frac{1+\sqrt{-23}}{2})$ and $P_2' = (2, \frac{1-\sqrt{-23}}{2})$. Each of these ideals remains inert from $\mathbb{Q}(\sqrt{-23})$ up to L.

- Exercise: Let p be a prime and H be a subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Show that $\alpha = \sum_{\sigma \in H} \sigma(\zeta_p)$ is a generator for the fixed field of H.
- Exercise: Let $L = \mathbb{Q}(\zeta_{31})$. Analyze the factorization types of the primes 2, 5, and 7 in $\mathcal{O}_L$, and find the decomposition and inertia groups and fields for each associated prime.

0.31 (Nov 18) Student Presentations of HW4 Problems

0.32 (Nov 20) Applications of Decomposition and Inertia

- We would now like to give some characterizations of the decomposition and inertia fields in terms of their splitting and ramification properties.
- Proposition (Decomposition and Inertia, II): Let L/K be a Galois extension of number fields with Galois group G, and let Q be a nonzero prime of $\mathcal{O}_L$ lying over the prime P of $\mathcal{O}_K$. Additionally let K' be an intermediate field between L and K fixed by the subgroup H of G, and take Q' to be the prime of $\mathcal{O}_{K'}$ lying under Q.

  1. For any such field K', we have $D(Q|P') = D(Q|P) \cap H$ and $E(Q|P') = E(Q|P) \cap H$.
     - Proof: Since $\mathrm{Gal}(L/K') = H$, by definition $D(Q|P') = \{\sigma \in H : \sigma(Q) = Q\}$, and this is quite obviously the same as $D(Q|P) \cap H$.
     - Similarly, $E(Q|P') = \{\sigma \in H : \sigma(\alpha) \equiv \alpha \pmod{Q} \text{ for all } \alpha \in \mathcal{O}_L\}$ and this is again quite clearly $E(Q|P) \cap H$.
  2. For any such field K', the decomposition field $L_{D'}$ of $Q|P'$ is the composite field $L_D K'$ and the inertia field $L_{E'}$ of $Q|P'$ is the composite field $L_E K'$.
     - Proof: Immediate from (1) and the Galois correspondence, since the fixed field of an intersection of subgroups is the composite of the fixed fields of those subgroups.
  3. The decomposition field L_D is the smallest intermediate field K' such that Q is the only prime of $\mathcal{O}_L$ lying over P'.
     - Proof: Certainly L_D does have this property since $g(Q|Q_D) = 1$ as we showed earlier.
     - Now suppose K' is an arbitrary intermediate field such that Q is the only prime of $\mathcal{O}_L$ lying over P'.
     - But since the action of the Galois group $\mathrm{Gal}(L/K')$ is transitive on primes lying over P', that means $\sigma(Q) = Q$ for all $\sigma \in \mathrm{Gal}(L/K')$, whence $\mathrm{Gal}(L/K') \subseteq D = \mathrm{Gal}(L/L_D)$.
     - By the Galois correspondence we then have $L_D \subseteq K'$, and so L_D is the smallest such field as claimed.
  4. The decomposition field L_D is the largest intermediate field K' such that P splits completely in K'.
     - Proof: Certainly L_D does have this property since $g = [L_D : K]$ as we showed earlier.
     - Now suppose that P splits completely in K', so that $e(P'|P) = f(P'|P) = 1$: then $e(Q|P') = e(Q|P)$ and $f(Q|P') = f(Q|P)$ by multiplicativity.
     - But now by (2) and our results earlier, we know that $[L : L_D] = e(Q|P)f(Q|P) = e(Q|P')e(Q|P') = [L : L_{D'}] = [L : L_D K']$ whence $L_D = L_D K'$, which is to say, $K' \subseteq L_D$ as desired.
  5. The inertia field L_E is the smallest intermediate field K' such that Q is totally ramified over P'.
     - Proof: Certainly L_E does have this property since $e(Q|Q_E) = e = [L : L_E]$ as we showed earlier.
     - Now suppose K' is an arbitrary intermediate field such that Q is totally ramified over P', meaning that $e(Q|P') = [L : K']$.
     - Since $e(Q|P') = [L : L_{E'}] = [L : L_E K']$ by our earlier results and (2), we must therefore have $K' = L_E K'$ whence $L_E \subseteq K'$ as desired.
  6. The inertia field L_E is the largest intermediate field K' such that P' is unramified over P.
     - Proof: Certainly L_E does have this property since $e(P'|P) = 1$ as we showed earlier.
     - Now suppose K' is an arbitrary intermediate field such that P' is unramified over P, so that $e(P'|P) = 1$.

- Then $e(Q|P') = e(Q|P)$ by multiplicativity, so $L_E = L_{E'} = L_E K'$ again by (2) and our earlier results, whence $K' \subseteq L_E$ as desired.

7. If D is a normal subgroup of G, then the decomposition field L_D is the largest intermediate field K' such that P splits completely in $\mathcal{O}_{K'}$.
   - Proof: If P splits completely in K' then $e(P'|P) = f(P'|P) = 1$ and so $K' \subseteq L_D$ by (4).
   - The remainder follows by applying the exercise above to the result of the exercise earlier that P splits completely in L_D when D is normal in G.

- Exercise: Suppose L/K is a number field extension and P is a prime of $\mathcal{O}_K$. Suppose that P is totally split / inert / ramified in L. Show that P is totally split / inert / ramified (respectively) in every subfield of L.

- As an application of these results about the decomposition and inertia fields, we can show that various splitting and ramification properties are preserved by taking composites of fields without requiring the extension to be Galois.

- Proposition (Splitting and Ramification in Composites): Suppose that L_1 and L_2 are two number field extensions of K and P is a prime of $\mathcal{O}_K$.

1. If P is unramified in L_1 and in L_2 then it is unramified in the composite field L_1L_2.
   - Proof: Let Q be a prime of L_1L_2 lying over P. Also let $\hat{L}$ be the Galois closure of L_1L_2 over K and let $\hat{Q}$ be a prime of $\mathcal{O}_{\hat{L}}$ lying over Q.
   - Then the inertia field $L_{\hat{E}}$ of $\hat{Q}|Q$ is the largest intermediate field of $\hat{L}/K$ such that P is unramified in $L_{\hat{E}}$, hence it contains both L_1 and L_2 by hypothesis. But then it also contains the composite field L_1L_2, whence P is unramified in L_1L_2.
2. If P is totally split in L_1 and L_2 then it is totally split in the composite field L_1L_2.
   - Proof: As in (1) let Q be a prime of L_1L_2 lying over P, $\hat{L}$ be the Galois closure of L_1L_2 over K, and $\hat{Q}$ be a prime of $\mathcal{O}_{\hat{L}}$ lying over Q.
   - Then the decomposition field $L_{\hat{D}}$ of $\hat{Q}|Q$ is the largest intermediate field of $\hat{L}/K$ such that P splits completely in $L_{\hat{D}}$, hence it contains both L_1 and L_2 by hypothesis. But then it also contains the composite field L_1L_2, whence P splits completely in L_1L_2.

- We can also use these properties of the decomposition and inertia fields to give a proof of the law of quadratic reciprocity.

  - The first step is to connect the values of Legendre symbols to splitting behaviors, which we have essentially already seen via Dedekind-Kummer:
  - Exercise: Let $K = \mathbb{Q}(\sqrt{D})$ have discriminant Δ and let p be an odd prime. Show the following equivalences:
    1. p is ramified in $\mathbb{Q}(\sqrt{D}) \iff \Delta$ is zero mod $p \iff$ the Legendre symbol $\left(\frac{\Delta}{p}\right) = 0$.
    2. p is split in $\mathbb{Q}(\sqrt{D}) \iff \Delta$ is a nonzero square mod $p \iff$ the Legendre symbol $\left(\frac{\Delta}{p}\right) = +1$.
    3. p is inert in $\mathbb{Q}(\sqrt{D}) \iff \Delta$ is a nonsquare mod $p \iff$ the Legendre symbol $\left(\frac{\Delta}{p}\right) = -1$.
  - We can now exploit the decomposition and inertia fields in a cyclotomic extension to identify the splitting behavior of p in $\mathbb{Q}(\zeta_q)$.

- Theorem (Cyclotomic Fields and Quadratic Reciprocity): Let p and q be distinct odd primes.

1. If d divides $p-1$ and a is not divisible by p, then the congruence $x^d \equiv a \pmod{p}$ is solvable if and only if $a^{(p-1)/d} \equiv 1 \pmod{p}$.
   - Proof: Obviously, if $x^d \equiv a \pmod{p}$ then $a^{(p-1)/d} \equiv x^{p-1} \equiv 1 \pmod{p}$ by Euler's theorem.
   - Conversely, if d divides $p-1$ then $x^d - 1$ divides $x^{p-1} - 1$ which splits completely mod p again by Euler's theorem, so $x^d \equiv 1 \pmod{p}$ has d solutions mod p.
   - Therefore, the kernel of the dth-power map on $(\mathbb{Z}/p\mathbb{Z})^\times$ has size d, so by the first isomorphism theorem, the image, which is precisely the set of dth powers, has size $(p-1)/d$.

- But by the same observation, there are exactly $(p-1)/d$ solutions to the equation $x^{(p-1)/d} \equiv 1 \pmod{p}$, so by the above, these must be exactly the dth powers.
- Exercise: If u is a primitive root modulo p and d divides $p-1$, show that the dth powers modulo p are $u^d, u^{2d}, \ldots, u^{p-1}$. Deduce again that a is a dth power mod p if and only if the order of a divides $(p-1)/d$.

2. If d is any divisor of $p-1$, then q is a dth power mod p if and only if q splits completely in the unique subfield F_d of $\mathbb{Q}(\zeta_p)$ of degree d over $\mathbb{Q}$.
   - Proof: Let Q be a prime of $\mathbb{Q}(\zeta_p)$ lying over q.
   - From our earlier discussion of splitting in cyclotomic fields, we know that q splits as the product of $(p-1)/f$ distinct prime ideals over $\mathbb{Q}(\zeta_p)$, where $f = f(Q|q)$ is the multiplicative order of p modulo q.
   - Since the Galois group is abelian, the decomposition subgroup for $Q|q$ is automatically normal, and so the decomposition field L_D for $Q|q$ is the maximal subfield over which q splits completely. Since $[L_D : \mathbb{Q}] = g = (p-1)/f$, that means L_D is the unique subfield of degree $(p-1)/f$ over $\mathbb{Q}$.
   - Then by (1) and our results on decomposition, we see that q is a dth power mod $p \iff$ the multiplicative order f divides $(p-1)/d \iff d$ divides $(p-1)/f \iff [F_d : \mathbb{Q}]$ divides $[L_D : \mathbb{Q}] \iff F_d$ is contained in L_D (since the subfields are linearly ordered) $\iff q$ splits completely in F_d, as claimed.

3. For $p^* = (-1)^{(p-1)/2}$, we have the equality of Legendre symbols $\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$.
   - Proof: By (2), we know that $(\frac{q}{p}) = 1$ if and only if q splits completely in the unique quadratic subfield of $\mathbb{Q}(\zeta_p)$ of degree 2 over $\mathbb{Q}$.
   - But as we saw in an earlier exercise, the unique quadratic subfield of $\mathbb{Q}(\zeta_p)$ is $\mathbb{Q}(\sqrt{p^*})$.
   - By the exercise above, q splits in $\mathbb{Q}(\sqrt{p^*})$ if and only if $\left(\frac{p^*}{q}\right) = 1$, since the discriminant of $\mathbb{Q}(\sqrt{p^*})$ is either p^* or $4p^*$.
   - Therefore, we see that $(\frac{q}{p}) = 1$ if and only if $(\frac{p^*}{q}) = 1$, so since the only other possibility (for distinct p, q) is for both symbols to equal -1, we see that $(\frac{p^*}{q}) = (\frac{q}{p})$.

4. (Quadratic Reciprocity) For distinct odd primes p and q, we have $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$.
   - Proof: By multiplicativity of Legendre symbols and Euler's criterion $a^{(p-1)/2} \equiv (\frac{a}{p}) \pmod{p}$, we have $\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right) = \left(\frac{(-1)^{(p-1)/2}p}{q}\right) = \left(\frac{-1}{q}\right)^{(p-1)/2}\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}\left(\frac{p}{q}\right)$.
   - The desired result then follows immediately since each Legendre symbol squares to 1.

- Exercise: By comparing the splitting of p in $\mathbb{Q}(\zeta_8)$ to that of 2 in $\mathbb{Q}(\sqrt{p^*})$, show that $\left(\frac{2}{p}\right) = +1$ when $p \equiv 1, 3 \pmod{8}$ and $\left(\frac{2}{p}\right) = -1$ when $p \equiv 5, 7 \pmod{8}$.

0.33 (Nov 21) Frobenius Elements

- As we have noted previously, the quotient of the decomposition group $D(Q|P)$ by the inertia group $E(Q|P)$ is isomorphic to the Galois group $\mathrm{Gal}(F_Q/F_P)$ of the corresponding extension of residue fields.
  - Suppose that the inertia group is trivial, so that the prime Q, or equivalently P, is unramified, since the extension is Galois.
  - Then the decomposition group D is naturally isomorphic to the Galois group $\mathrm{Gal}(F_Q/F_P)$ of the extension of residue fields, which is a cyclic group of order $f(Q|P)$ generated by the Frobenius map $\varphi : F_Q \to F_Q$, given explicitly by $\overline{\varphi}_{Q|P}(\overline{\alpha}) = \overline{\alpha}^{N(P)}$ for $\overline{\alpha} \in F_Q$. (Remember that $\overline{\alpha} = \alpha + Q$ is a residue class in $F_Q = \mathcal{O}_L/Q$ and that $N(P) = \#F_P = p^{f(P|p)}$ is a prime power.)
  - The corresponding element $\varphi_{Q|P}$ in the decomposition group is called the Frobenius element:

- Definition: Let L/K be a Galois extension of number fields with Galois group G. If Q is an unramified prime of $\mathcal{O}_L$ lying over a prime P of $\mathcal{O}_K$, then the Frobenius element $\varphi_{Q|P} \in G$ is the automorphism with $\varphi_{Q|P}(\alpha) \equiv \alpha^{N(P)} \pmod{Q}$ for all $\alpha \in \mathcal{O}_L$.
    - The discussion above shows that $\varphi_{Q|P}$ exists and is a generator for the decomposition group $D(Q|P)$.
    - Exercise: Suppose L/K is Galois with Q of $\mathcal{O}_L$ lying over P of $\mathcal{O}_K$. Show that if $Q' = \sigma(Q)$ is another prime lying above P for some $\sigma \in \mathrm{Gal}(L/K)$, then the corresponding Frobenius element for $\sigma Q|P$ is given by the conjugate $\varphi_{\sigma Q|P} = \sigma \varphi_{Q|P} \sigma^{-1}$.
    - By the exercise above, we conclude that the Frobenius elements for all of the primes above P form a conjugacy class of the Galois group.
    - In particular when the Galois group is abelian, the Frobenius element depends only on P, and is characterized by the condition $\varphi_P(\alpha) \equiv \alpha^{N(P)} \pmod{P\mathcal{O}_L}$.

- Example: Let $K = \mathbb{Q}(\zeta_n)$ and let p be a prime not dividing n, so that p is unramified in K. Find the Frobenius element associated to p.
    - Since $\mathrm{Gal}(K/\mathbb{Q})$ is abelian, by the observations above, the Frobenius element φ_p must satisfy $\varphi_p(\alpha) \equiv \alpha^p \pmod{p\mathcal{O}_K}$ for all $\alpha \in \mathcal{O}_K$.
    - Since the elements of the Galois group are characterized by mapping ζ_n to ζ_n^k for some k, it is not hard to come up with a natural candidate: namely, the automorphism σ_p that maps $\zeta_n \mapsto \zeta_n^p$.
    - Indeed, since the pth power map is additive in characteristic p, since this automorphism σ_p maps ζ_n^a to ζ_n^{ap}, by additivity we see that for any $\alpha = \sum c_i \zeta_n^i$ for $c_i \in \mathbb{Z}$, we have $\sigma_p(\alpha) = \sum c_i \zeta_n^{pi} \equiv (\sum c_i \zeta_n^i)^p = \alpha^p \pmod{p\mathcal{O}_K}$.
    - Thus, the Frobenius element φ_p is the automorphism σ_p mapping $\zeta_n \mapsto \zeta_n^p$.

- Exercise: Suppose $n = p^v k$ where p is prime and does not divide k, and let $K = \mathbb{Q}(\zeta_n)$ and P be a prime of $\mathcal{O}_K$ lying above p.
    1. Show that the inertia field of $P|p$ is $\mathbb{Q}(\zeta_k)$. [Hint: Consider ramification.]
    2. Suppose that K' is a subfield of K in which p is unramified. Show that $K \subseteq \mathbb{Q}(\zeta_k)$.
    3. Show that the decomposition field of $P|p$ is the subfield of $\mathbb{Q}(\zeta_k)$ fixed by the automorphism $\zeta_k \mapsto \zeta_k^p$. [Hint: This is the Frobenius element.]

- Exercise: Suppose n is not a prime power. For $K = \mathbb{Q}(\zeta_n)$ and $K_+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, show that the extension K/K_+ is unramified at finite primes, so that the different $d_{K/K_+} = 1$. [Hint: Write $n = p^v k$ where $k > 1$. If P is a prime of K lying over P_+ in K_+ lying over p in $\mathbb{Q}$, observe that $E(P|P_+) = E(P|p) \cap \{1, \sigma\}$ where σ is complex conjugation. Use the exercise above and $k > 1$ to see that $\sigma \notin E(P|p)$.]

- The importance of the Frobenius element is that it carries information about how P splits, since (most obviously) the element $\varphi_{Q|P}$ has order $f(Q|P)$ in the Galois group.
    - But more usefully, we can still exploit the Frobenius element even in a non-Galois extension to analyze splitting behaviors.

- Proposition (Frobenius and Splitting): Let L/K be an extension of number fields with Galois closure $\hat{L}$ and set $G = \mathrm{Gal}(\hat{L}/K)$ and take $H = \mathrm{Gal}(\hat{L}/L)$ to be the subgroup fixing L. Also, let P be a prime of $\mathcal{O}_K$ that is unramified in L lying under the prime $\hat{Q}$ of $\mathcal{O}_{\hat{L}}$ and take $\varphi = \varphi_{\hat{Q}|P}$ to be the Frobenius element and $D = D(\hat{P}|P)$ be the decomposition group.
    1. The right cosets $\{H\sigma\}_{\sigma \in G}$ of H in G are permuted by right-multiplication by φ. The orbits are of the form $\{H\sigma, H\sigma\varphi, \ldots, H\sigma\varphi^{m-1}\}$ where $H\sigma\varphi^m = H\sigma$ and m is the smallest positive integer with $\sigma\varphi^m\sigma^{-1} \in H$.
        - Proof: Obvious.

    Now suppose that orbits of the action in (1) are given explicitly by $\{H\sigma_1, \ldots, H\sigma_1\varphi^{m_1-1}\}, \ldots, \{H\sigma_g, \ldots, H\sigma_g\varphi^{m_g-1}\}$.

2. The ideals $Q_i = \sigma_i(\hat{P}) \cap \mathcal{O}_L$ are distinct primes of $\mathcal{O}_L$ lying over P, for $1 \leq i \leq g$.
   - Proof: The prime $\sigma_i(\hat{P})$ is a prime ideal of $\mathcal{O}_{\hat{L}}$ lying over P, so $(\sigma_i\hat{P}) \cap \mathcal{O}_L = Q_i$ is a prime of $\mathcal{O}_L$ lying over P. It remains to see all of these primes are distinct, so suppose we had $Q_i = Q_j$.
   - Since the Galois action is transitive, there exists some $\tau \in H$ such that $\tau(Q_i) = Q_j$: then $Q_i = Q_j \iff \tau\sigma_i(\hat{P}) = \sigma_j(\hat{P}) \iff \sigma_j^{-1}\tau\sigma_i(\hat{P}) = \hat{P} \iff \sigma_j^{-1}\tau\sigma_i \in D \iff \sigma_j^{-1}\tau\sigma_i = \varphi^k$ for some integer k, since φ generates the decomposition group $D \iff \sigma_j\varphi^k\sigma_i^{-1} = \tau \in H \iff H\sigma_i$ and $H\sigma_j\varphi^k$ are in the same coset.
   - We conclude that the distinct cosets correspond to distinct primes, as desired.
3. For $Q_i = \sigma_i(\hat{P}) \cap \mathcal{O}_L$, we have $f(Q_i|P) \geq m_i$.
   - Exercise: Suppose $\hat{L}$ is the Galois closure of L/K and $\hat{Q}$ is an unramified prime of $\hat{L}$ lying over Q of $\mathcal{O}_L$ lying over P of $\mathcal{O}_K$. Show that $\varphi_{\hat{Q}|Q} = \varphi_{\hat{Q}|P}^{f(Q|P)}$. [Hint: Both Frobenius elements act as power maps. How are the powers related?]
   - Proof: By the exercise above and an earlier exercise we have $\varphi_{\sigma\hat{Q}|Q_i} = \varphi_{\sigma\hat{Q}|P}^{f(Q_i|P)} = (\sigma\varphi_{\hat{Q}|P}\sigma^{-1})^{f(Q_i|P)} = \sigma\varphi_{\hat{Q}|P}^{f(Q_i|P)}\sigma^{-1} = \sigma\varphi^{f(Q|P)}\sigma^{-1}$.
   - Since $\varphi_{\sigma\hat{Q}|Q_i} \in H$, this means $\sigma\varphi^{f(Q|P)}\sigma^{-1} \in H$ and thus $H\sigma = H\sigma\varphi^{f(Q|P)}$. Thus, by (1), we have $f(Q_i|P) \geq m_i$.
4. For $Q_i = (\sigma_i\hat{P}) \cap \mathcal{O}_L$, we have $P\mathcal{O}_L = Q_1 \cdots Q_g$ and $f(Q_i|P) = m_i$.
   - Proof: First note that $m_1 + \cdots + m_g = [L : K]$ by the orbit decomposition.
   - Then by the ef-theorem, the fact that P is unramified so that all $e(Q_i|P) = 1$, and the fact that all of the Q_i are distinct per (2), we have $[L : K] = \sum_i m_i \leq \sum_i f(Q_i|P) = \sum_i e(Q_i|P)f(Q_i|P) \leq [L : K]$.
   - Hence we must have equality everywhere, so the Q_i are all of the primes of $\mathcal{O}_L$ lying above P and that $f(Q_i|P) = m_i$ for each i.

- There is a very nice application of this result to the computation of Galois groups of polynomials:

- Theorem (Dedekind-Frobenius): Suppose K is a number field and $g(x) \in \mathcal{O}_K[x]$ is an irreducible polynomial of degree n with Galois group G, viewed as a subgroup of S_n. Then for any unramified prime P of $\mathcal{O}_K$, if the mod-P reduction of $g(x)$ factors over the residue field $F_P = \mathcal{O}_K/P$ as a product of terms having degrees $m_1, m_2, \ldots, m_d$, then G contains a permutation whose cycle decomposition is a product of cycles of lengths $m_1, m_2, \ldots, m_d$.

  - Proof: Let α be a root of g. By the Dedekind-Kummer factorization theorem, since P is unramified, the factorization of P in $L = K(\alpha)$ is given by $P = Q_1Q_2 \cdots Q_g$ where $Q_i = (P, f_i(\alpha))$ where $g(x) = f_1(x) \cdots f_g(x)$ in $F_P[x]$, and $f(Q_i|P) = \deg(f_i)$.
  - On the other hand, by the theorem above, $P\mathcal{O}_L = Q_1 \cdots Q_g$ and $f(Q_i|P) = m_i$ where m_i is equal to the size of the coset $\{H\sigma_1, \ldots, H\sigma_1\varphi^{m_1-1}\}$ of the Frobenius element $\varphi = \varphi_{\hat{Q}|P}$ acting on G.
  - Viewing G as a subgroup of the symmetric group S_n, the coset $\{H\sigma_1, \ldots, H\sigma_1\varphi^{m_1-1}\}$ corresponds to a cycle of length m_i, so the cycle decomposition of φ is a product of cycles of lengths $m_1, m_2, \ldots, m_d$. The result is immediate.

- The point of the theorem above is that we can find cycle decompositions of permutations in the Galois group of a polynomial $g(x)$ by factoring $g(x)$ modulo unramified primes.

  - We will mention here that the cycle decompositions only determine a permutation in S_n up to conjugacy, which reflects the fact that all of the Frobenius elements in a given extension are conjugate.
  - Under the assumption that $g(x)$ is irreducible of degree n, its Galois group as a subgroup of S_n (viewed explicitly as a permutation group on the n roots of $g(x)$ over an algebraic closure, or equivalently on the n complex embeddings of the extension $K[x]/g(x)$) is a transitive subgroup.
  - So, by listing the cycle types of transitive subgroups of S_n, and then comparing them to the factorization types of $g(x)$ modulo P for unramified primes P (i.e., primes not dividing the discriminant of g), we may in many cases identify the Galois group of g.

- We will mention also the following theorem of Chebotarev:
- Theorem (Chebotarev Density Theorem): Let L/K be a Galois extension of number fields with Galois group G, and let S be a union of conjugacy classes in G. Then the set of primes of K unramified in L whose Frobenius conjugacy class lies in S has natural and analytic density $\#S/\#G$.
    - Intuitively, this result says that the Frobenius element is (in an appropriate sense) chosen randomly and uniformly from the Galois group.
    - Applying the Chebotarev density theorem to our result above shows that if we compute the proportion of primes of norm less than a given bound X for which the polynomial $g(x)$ factors mod p with a given cycle type C, then as $X \to \infty$, this proportion tends to the proportion $\#C/\#G$ of elements in the Galois group G with cycle type C.
- We will now list the transitive subgroups of S_n for some smaller values of n (along with the distribution of cycle types):
    - There is a standard labeling of the transitive subgroups of S_n due to Conway, Hulpke, and McKay, which we include with the tables. We also remark that many subgroups have (isomorphic) conjugates inside S_n, and the list of generators is only one possibility among many.
    - For degree 4, there are 5 transitive subgroups of S_4, with generators and cycle types as follows:

#	Order	Name	Generators	1	2	2,2	3	4
5T1	4	C_4	(1 2 3 4)	1		1		2
5T2	4	$C_2 \times C_2$	(1 2)(3 4), (1 3)(2 4)	1		3		
5T3	8	$D_{2\cdot 4}$	(1 2 3 4), (1 2)(3 4)	1	2	3		2
5T4	12	A_4	(1 2 3), (2 3 4)	1		3	8	
5T5	24	S_4	(1 2 3 4), (1 2)	1	6	3	8	6

    - For degree 5, there are 5 transitive subgroups of S_5, with generators and cycle types as follows:

#	Order	Name	Generators	1	2	2,2	3	2,3	4	5
5T1	5	C_5	(1 2 3 4 5)	1						4
5T2	10	$D_{2\cdot 5}$	(1 2 3 4 5), (1 5)(2 4)	1		5				4
5T3	20	F_{20}	(1 2 3 4 5), (1 2 4 3)	1		5			10	4
5T4	60	A_5	(1 2 3), (3 4 5)	1		15	20			24
5T5	120	S_5	(1 2 3 4 5), (1 2)	1	10	15	20	20	30	24

    - For degree 6, there are 16 transitive subgroups of S_6, with generators and cycle types as follows:

#	Order	Name	Generators	1	2	2,2	2,3	2,4	2,2,2	3	3,3	4	5	6
6T1	6	C_6	(1 2 3 4 5 6)	1					1		2			2
6T2	6	S_3	(1 3 5)(2 4 6), (1 4)(2 3)(5 6)	1					3		2			
6T3	12	$S_3 \times C_2$	(1 2 3 4 5 6), (1 4)(2 3)(5 6)	1		3			4		2			2
6T4	12	A_4	(1 4)(2 5), (1 3 5)(2 4 6)	1		3					8			
6T5	18	F_{18}	(2 4 6), (1 4)(2 5)(3 6)	1					3	4	4			6
6T6	24	$A_4 \times C_2$	(3 6), (1 3 5)(2 4 6)	1	3	3			1		8			8
6T7	24	S_4 (a)	(1 4)(2 5), (1 3 5)(2 4 6), (1 5)(2 4)	1		9		6			8			
6T8	24	S_4 (b)	(1 4)(2 5), (1 3 5)(2 4 6), (1 5)(2 4)(3 6)	1		3			6		8	6		
6T9	36	$S_3 \times S_3$	(2 4 6), (1 5)(2 4), (1 4)(2 5)(3 6)	1		9			6	4	4			12
6T10	36	F_{36}	(2 4 6), (1 5)(2 4), (1 4 5 2)(3 6)	1		9		18		4	4			
6T11	48	$S_4 \times C_2$	(3 6), (1 3 5)(2 4 6), (1 5)(2 4)	1	3	9		6	7		8	6		8
6T12	60	A_5	(1 2 3 4 6), (1 4)(5 6)	1		15					20		24	
6T13	72	$F_{36} \rtimes C_2$	(2 4 6), (2 4), (1 4)(2 5)(3 6)	1	6	9	12	18	6	4	4			12
6T14	120	S_5	(1 2 3 4 6), (1 2)(3 4)(5 6)	1		15			10		20	30	24	20
6T15	360	A_6	(1 2)(3 4 5 6), (1 2 3)	1		45		90		40	40		144	
6T16	720	S_6	(1 2 3 4 5 6), (1 2)	1	15	45	120	90	15	40	40	90	144	120

    - For degree 7, there are 7 transitive subgroups of S_7, with generators and some cycle types as follows (for any cycle type not listed, S_7 is the only transitive subgroup containing it):

#	Order	Name	Generators	1	2,2	2,4	2,2,2	2,2,3	3	3,3	5	6	7
7T1	7	C_7	(1 2 3 4 5 6 7)	1									6
7T2	14	$D_{2\cdot 7}$	(1 2 3 4 5 6 7), (2 7)(3 6)(4 5)	1			7						6
7T3	21	F_{21}	(1 2 3 4 5 6 7), (1 2 4)(3 6 5)	1						14			6
7T4	42	F_{42}	(1 2 3 4 5 6 7), (1 3 2 6 4 5)	1			7			14		14	6
7T5	168	$PSL_2(\mathbb{F}_7)$	(1 2 3 4 5 6 7), (1 2)(3 6)	1	21	42				56			48
7T6	2520	A_7	(3 4 5 6 7), (1 2 3)	1	105	630		210	70	280	504		720
7T7	5040	S_7	(1 2 3 4 5 6 7), (1 2)	1	105	630	105	210	70	280	504	840	720

- We can use these tables to compute probable Galois groups for irreducible polynomials of degree ≤ 7 by computing the factorization of the polynomial modulo primes not dividing its discriminant and listing the corresponding cycles that must appear in its Galois group.
  - Exercise: Let $g(x)$ be a polynomial irreducible over $\mathbb{Q}$. Prove that the discriminant of g is a square if and only if the Galois group of $g(x)$ is a subgroup of A_n.
  - Per the exercise above, we can also determine whether G is a subgroup of A_n by checking whether the discriminant is a square.

- Example: Find the Galois group over $\mathbb{Q}$ for the polynomial $g(x) = x^4 + 2x + 2$.
  - We can compute that this polynomial has discriminant $2^4 \cdot 101$, so its Galois group is not a subgroup of A_n.
  - Computing the factorization of g modulo p for the 100 smallest primes excluding 2 and 101 yields the following cycles:

Factorization Type	1	2	2,2	3	4
# Appearances	5	24	7	32	32

  - The only transitive subgroup of S_4 containing all of these cycle types is S_4 itself, so the Galois group must be $\boxed{S_4}$.
  - Note that the distribution of the factorization types matches fairly closely with the distribution of cycle types in S_4, as should be expected per Chebotarev.

- Example: Determine the probable Galois group of $g(x) = x^5 - 5x^2 - 3$.
  - We can compute that this polynomial has discriminant $3^2 \cdot 5^6$, so its Galois group is a subgroup of A_5.
  - Computing the factorization of g modulo p for the 100 smallest primes excluding 3 and 5 yields the following cycles:

Factorization Type	1	2	2,2	3	2,3	4	5
# Appearances	8		54				38

  - The only transitive subgroups contained in A_5 having these cycle types are $D_{2\cdot 5}$ and A_5.
  - Since $D_{2\cdot 5}$ has no 3-cycles (in contrast to A_5, 1/3 of whose elements are 3-cycles) we would expect no factorizations to have a 3-cycle if the Galois group were $D_{2\cdot 5}$, while we would expect about 1/3 of them to have a 3-cycle if the Galois group were A_5.
  - Since no 3-cycles appear in the computed factorizations, it seems overwhelmingly likely that the Galois group is $D_{2\cdot 5}$.

- Example: Determine the probable Galois group of $g(x) = x^6 - x^5 - x^2 + x + 1$.
  - This polynomial has discriminant $-3^3 \cdot 433$, so its Galois group is not a subgroup of A_6.
  - Computing the factorization of g modulo p for the 100 smallest primes excluding 3 and 433 yields the following cycles:

Factorization Type	1	2	2,2	2,3	2,4	2,2,2	3	3,3	4	5	6
# Appearances	1	4	14	17	29	6	8	3			18

  - There are only two transitive subgroups that contain cycles of each of these types: the subgroup 6T13 of order 72 and the subgroup 6T16 (which is S_6).

- Since 6T16 has no 4-cycles or 5-cycles (in contrast to S_6, roughly $1/3$ of whose elements are 4-cycles or 5-cycles), and no 4-cycles or 5-cycles appear in the computed factorizations, it seems overwhelmingly likely that the Galois group is 6T13.

- Example: Determine the probable Galois group of $g(x) = x^7 - 7x + 3$.
  - We can compute that this polynomial has discriminant $3^8 \cdot 7^8$, so its Galois group is a subgroup of A_7.
  - Computing the factorization of g modulo p for the 100 smallest primes excluding 3 and 7 yields the following cycles:

Factorization Type	1	2,2	2,4	2,2,2	2,2,3	3	3,3	5	6	7
# Appearances		15	32				32			21

  - There are only two transitive subgroups contained in A_7 that contain cycles of each of these types, namely $PSL_2(\mathbb{F}_7)$ and A_7.
  - As above, since the observed factorization types match the cycles of $PSL_2(\mathbb{F}_7)$ very closely (in contrast to A_7, which also has 3-cycles, 2,2,3-cycles, and 5-cycles), the probable Galois group is $PSL_2(\mathbb{F}_7)$.

- Exercise: Find the probable Galois group for each polynomial below, given its factorization modulo the 100 smallest primes not dividing its discriminant Δ:

1. $g(x) = x^5 - x^2 - 2x - 3$, with $\Delta = 17^2 \cdot 29^2$.

Factorization Type	1	2,2	3	5
# Appearances	1	20	30	49

2. $g(x) = x^5 - 5x^3 + 5x - 20$, with $\Delta = 2^4 \cdot 3^4 \cdot 5^5 \cdot 11^2$.

Factorization Type	1	2,2	4	5
# Appearances	3	26	52	19

3. $g(x) = x^6 + x^4 + 23$, with $\Delta = -2^6 \cdot 23^3$.

Factorization Type	1	2,2	2,2,2	3,3	4
# Appearances	3	9	27	36	24

4. $g(x) = x^6 - 6x^3 - 6x^2 - 6x - 2$, with $\Delta = 2^6 \cdot 3^6 \cdot 13^2$.

Factorization Type	2,2	2,4	3	3,3	5
# Appearances	8	24	13	14	41

5. $g(x) = x^7 - 14x^5 + 56x^3 - 56x - 22$, with $\Delta = 2^6 \cdot 7^{10}$.

Factorization Type	1	3,3	7
# Appearances	2	68	30

- Once a candidate for the Galois group has been identified, it is possible to construct resolvent polynomials and use information about their roots and factorizations to eliminate the other possible Galois groups.
  - For example, to establish that a particular polynomial of degree 5 has Galois group $D_{2\cdot 5} = \langle (1\,2\,3\,4\,5), (1\,5)(2\,4) \rangle$ requires eliminating the possibility that the Galois group is $A_5 = \langle (1\,2\,3), (3\,4\,5) \rangle$.
  - One way to do this is to compute the resolvent polynomial whose roots are the S_5-permutations of $\beta_1\beta_2 + \beta_2\beta_3 + \beta_3\beta_4 + \beta_4\beta_5 + \beta_5\beta_1$, which in this case has degree 12 (since there are 11 other possible results of permuting the indices, such as $\beta_1\beta_3 + \beta_2\beta_4 + \beta_3\beta_5 + \beta_4\beta_1 + \beta_5\beta_2$). This will differentiate between $D_{2\cdot 5}$ and A_5 since $D_{2\cdot 5}$ fixes several of these elements (so the resolvent polynomial will have a rational root) but A_5 does not.

0.34 (Nov 25) Higher Ramification Groups

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