Math 129 Lecture Notes

Evan Chen*

Spring 2015

This is Harvard College's *Math 129*, instructed by Mark Kisin. The formal name for this class is "Number Fields" but a more accurate name for the class is "Algebraic Number Theory".

The permanent URL is `http://web.evanchen.cc/coursework.html`, along with all my other course notes. If you received a Dropbox link to this document, please be aware that the Dropbox link will expire after the end of the semester.

Contents

*Email: evanchen@college.harvard.edu

§1 January 26, 2015

"Despite having taught this course four times, I can never remember the name of this course. . . I wish they would just call it algebraic number theory." – Mark Kisin

- Office Hours: Monday at 2PM (SC 234) or by appointment (`kisin@math.harvard.edu`)
- Homework due Wednesday in class.
- Textbook: Algebraic Theory of Numbers
- Midterm: March 11, in class.

Midterm and final exam questions will either be things literally done in class or on the homework – "I don't believe in tricky exams".

§1.1 Overview

Topics: Unique factorization, Class groups, Unit groups, Local Fields, Adeles.

This will enable to solve the following Diophantine equations:

- (Fermat) If $p \equiv 1 \pmod 4$ is a prime, then p is a sum of two squares. (Converse is true.)
- (Pell's Equation) Solving $x^2 - dy^2 = 1$ for d squarefree.

§1.2 What is a Number Field?

Definition 1.1. A **number field** is a field K with characteristic zero (meaning K contains $\mathbb{Q}$) and K is **finite-dimensional** when regarded as a $\mathbb{Q}$-vector space.

Example 1.2

$K = \mathbb{Q}(\alpha)$ for some α the root of a monic polynomial. (In fact, all examples will be of this form.) To give a concrete example,

$$K = \mathbb{Q}(\sqrt{2}) = \mathbb{Q}[x]/(x^2 - 2) = \left\{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \right\}.$$

Lemma 1.3

If K is a number field and $\alpha \in K$ then there exists a monic polynomial f with rational coefficients such that $f(\alpha) = 0$.

First Proof. Just kill using the fact that $\{1, \alpha, \alpha^2, \dots\}$ cannot be linearly independent in a finite-dimensional space. □

Second Proof, via characteristic polynomials. Let L be a field, and V a finite dimensional L-vector space. Let $\varphi : V \to v$ be an L-linear map (which means it's linear as a L-vector space). Then we consider the (defined-later) characteristic polynomial

$$P_\varphi(X) \in L[X]$$

is a monic polynomial of degree $\dim_L V$ such that

$$P_\varphi(\varphi) \equiv 0.$$

This is the **Cayley-Hamilton Theorem**, which we'll examine in the first homework. By $P_\varphi(\varphi)$ we mean

$$\varphi^n + a_{n-1}\varphi^{n-1} + \cdots + a_0 \in \operatorname{End}_L(V)$$

where $a_0, \ldots, a_{n-1} \in L$, and φ^k means φ applied k times.

Now to do the proof, let $V = K$ and $L = \mathbb{Q}$. Define a map $\tilde{\alpha} : K \to K$ by $x \mapsto \alpha x$. Then $P_{\tilde{\alpha}}(\tilde{\alpha}) : K \to K$ is the map which sends $x \mapsto x \cdot P_{\tilde{\alpha}}(\alpha)$ (check this yourself). The Cayley-Hamilton Theorem tells us this is actually the zero map. This can only occur if $P_{\tilde{\alpha}}(\alpha) = 0$. □

§1.3 Defining Characteristic Polynomial

Let V be a finite dimensional space over L, and $\varphi : V \to V$ an L-linear map. Consider the $L[X]$-module

$$V \otimes_L L[X].$$

If we identify $V = L^d$, you can consider this as $L[X]^d$. Consider the map

$$X - \varphi : V \otimes L[X] \to V \otimes L[X].$$

You can think of this as a $d \times d$ matrix with entries in $L[X]$.

Definition 1.4. The **characteristic polynomial** is defined by

$$P_\varphi(X) = \det(X - \varphi).$$

Remark. Everything we've done so far works for a free finitely generated module M over a ring R.

§1.4 Ring of Integers

Definition 1.5. If K is a number field then the ring of integers $\mathcal{O}_K \subseteq K$ is the set of roots of some *monic* polynomial with integer coefficients.

Example 1.6

Using the rational root theorem, $\mathcal{O}_{\mathbb{Q}} \cong \mathbb{Z}$.

Lemma 1.7

Let K be a number field and $\alpha \in K$. The following are equivalent:

- $\alpha \in \mathcal{O}_K$
- The minimal $\mathbb{Q}$-polynomial of α has integer coefficients.

Proof. Gauss Lemma. □

"Ahh, it's already 2!" A small teaser:

Example 1.8

If $K = \mathbb{Q}[\sqrt{2}]$ then $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$. But if $K = \mathbb{Q}[\sqrt{5}]$ then $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.

§2 January 28, 2015

Review.

Instructor manually computes the ring of integers for the rings $\mathbb{Q}(\sqrt{2})$ and does half the calculation for $\mathbb{Q}(\sqrt{5})$.

§2.1 Ring of integers deserves its name

Also, obligatory following lemma.

Lemma 2.1

$\mathcal{O}_K$ is actually a subring of K.

We'll prove this even more generally.

Definition 2.2. Suppose we have a commutative subring $A \subseteq R$ (with identity). An element $\alpha \in R$ is called **integral** over A if $\exists f(x) \in A[x]$ monic which annihilates α.

Proposition 2.3

Given $A \subseteq R$ a commutative subring, the set of integral elements is a subring.

Lemma 2.4

Let A be a ring, and M a finitely-generated A-module. Let $\alpha : M \to M$ be an A-linear map. Then there exists a monic polynomial $f(x) \in A[x]$ such that $f(\alpha)$ is the zero map.

Proof. If M is free over A (meaning $M = A^n$), then we can apply the Cayley-Hamilton Theorem to see the characteristic polynomial of α works.

In general, we have a surjection $A^n \twoheadrightarrow M$ and we can lift $\alpha : M \to M$ to a map as

$$\begin{array}{ccc} A^n & \twoheadrightarrow & M \\ \downarrow{\scriptstyle \widehat{\alpha}} & & \downarrow{\scriptstyle \alpha} \\ A^n & \twoheadrightarrow & M \end{array}$$

Then we use Cayley-Hamilton on $\tilde{\alpha}$. □

Remark 2.5. The Cayley-Hamilton theorem applies only for maps between finitely generated free modules. That's why we need to split into the two cases above, and add the hypothesis that M is a finitely generated A-module.

Example 2.6

There are easy counterexamples if we drop the condition that M is finitely generated. For example, let $A = \mathbb{Z}$, and $M = \mathbb{Z}[x]$ and take the "multiplication" map $\tilde{x}$ by $g \mapsto x \cdot g$. Then there is no way to get this map to vanish! One can't get $f(\tilde{x})$ to be the zero map.

Remark 2.7. As a reminder, "finitely generated" is weaker than "free". For example, $\mathbb{Z}/2\mathbb{Z}$ is finitely generated but certainly not free.

Lemma 2.8

If $A \subseteq R$ is a subring and $\alpha \in R$, then the following are equivalent.

- α is integral.
- The ring $A[\alpha]$ generated by α is a finitely generated A-module.
- $A[\alpha]$ is contained in some subring $B \subseteq R$ which is finitely generated.

Proof. First part is standard.

To show the second implies the third, just take $B = A[\alpha]$.

Finally, we will show that if $A[\alpha] \subseteq B \subseteq R$ then α is integral. Consider the map $\tilde{\alpha} : B \to B$ by $b \mapsto \alpha \cdot b$. Hence by our previous lemma we get that $f(\tilde{\alpha})$ is the zero map; hence $f(\alpha) = 0$. □

Remark 2.9. This proof implies that if $A[\alpha]$ is contained in something finitely generated, then it is itself finitely generated. It is tempting to try to apply this line of reasoning directly: certainly submodules of finitely generated modules are themselves finitely generated, right? Unfortunately, this turns out to be true only given additional conditions on A: we need it to be *Noetherian* (whatever that means).

In practice, most structures we deal with will be Noetherian. But in any case the lemma lets us argue "if $A[\alpha]$ is contained in something finitely generated, then $A[\alpha]$ is finitely generated, and hence α is integral" in total generality.

Now we can prove the proposition that $\mathcal{O}_K$ is a ring.

Proof. Let $A' = \{\alpha \in R : \alpha \text{ integral over } A\}$. If $\alpha, \beta \in A'$ then $A[\alpha, \beta]$ is finitely generated over A (by multiplying all the bases together). Now $A[\alpha + \beta]$ and $A[\alpha\beta]$ are contained in the finitely generated $A[\alpha, \beta]$. Thus $\alpha + \beta$ and $\alpha\beta$ are integral over A. □

§3 January 30, 2015

Recall that if A is a subring of a ring R, then the set of integral elements over A is also a subrbring of R.

§3.1 Corollaries

Corollary 3.1

If $A \subseteq B \subseteq C$ be subrings. If B is integral over A, and C is integral over B then C is integral over A.

Proof. Let $\alpha \in C$, $f(x) \in B[x]$ its monic minimal polynomial over B, and let B' be the ring $A[b_0, \dots, b_{n-1}]$, where

$$f(x) = x^n + b_{n-1}x^{n-1} \cdots + b_0$$

(here $b_i \in B$). Then $B'[\alpha]$ is finitely generated over B'. Moreover, B' is finitely generated over A. Hence $B'[\alpha]$ is finitely generated over A, and so is $A[\alpha]$, as needed. □

Also, we saw last time that the ring of integers $\mathcal{O}_K$ is indeed a subring of the field K.

By definition, $\mathcal{O}_K$ is integral over $\mathbb{Z}$. This leads us to ask if $\mathcal{O}_K$ is also *finitely generated* as a $\mathbb{Z}$-module. In fact it is, but this is not entirely trivial.

Example 3.2 (Integral Rings Over $\mathbb{Z}$ Need Not Be Finitely Generated)

Let $\overline{\mathbb{Q}}$ be the algebraic numbers, and let $\overline{\mathbb{Z}} \subseteq \overline{\mathbb{Q}}$ be its ring of integers

Now let's consider the $\mathbb{Q}$-span of $\overline{\mathbb{Z}}$, clearly this a subspace of $\overline{\mathbb{Q}}$. In a moment we will show it actually equals $\overline{\mathbb{Q}}$. Hence $\overline{\mathbb{Z}}$ is not finitely generated, since we can show that $\overline{\mathbb{Q}}$ is infinite dimensional over $\mathbb{Q}$.

§3.2 Algebraic Integers and Algebraic Numbers

Proposition 3.3

The $\mathbb{Q}$-span of the algebraic integers is the algebraic numbers. That is, for any α an algebraic integer, there exists a positive integer M such that $M\alpha \in \overline{\mathbb{Z}}$.

Proof. Trivial. Scale so that polynomials become monic. □

We can obfuscate the above statement by saying that there's an isomorphism

$$\overline{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q} \to \overline{\mathbb{Q}} \text{ by } z \otimes q \mapsto qz.$$

The above shows that the map is surjective; injectivity is slightly more work.

§3.3 Quadratic Fields

Suppose $K/\mathbb{Q}$ is two-dimensional (i.e. K is a quadratic extension). If $\alpha \in K$ is irrational, then $\mathbb{Q}(\alpha) \neq \mathbb{Q}$, forcing $Q(\alpha) = K$. Now the minimal polynomial of α is a quadratic; hence we can put $K = \mathbb{Q}(\sqrt{d})$ for $0 \neq d \in \mathbb{Q}$. Simple reductions let us assume d is an integer and squarefree. Hence every quadratic extension K is of the form $\mathbb{Q}(\sqrt{d})$ for some squarefree integer d.

Instructor proceeds to compute $\mathcal{O}_K$, to arrive at conclusion

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & d \equiv 1 \pmod 4 \\ \mathbb{Z}[\sqrt{d}] & d \not\equiv 1 \pmod 4. \end{cases}$$

§4 February 4, 2015

Recall that last week we considered number fields K, for which we had the ring of integers $\mathcal{O}_K$. Hence for $\alpha \in \mathcal{O}_K$, $\mathbb{Z}[\alpha]$ is finitely generated as a $\mathbb{Z}$-module.

Today we will show more strongly that

Proposition 4.1

$\mathcal{O}_K$ is finitely generated as $\mathbb{Z}$-module. More precisely, if $\dim_{\mathbb{Q}} K = n$ then $\mathcal{O}_K \simeq \mathbb{Z}^n$.

Primitive Element Theorem meow.

§4.1 The Trace of an Element

Definition 4.2. Let B be a ring (commutative with 1 as usual) and let $A \subseteq B$ be a subring such that B is a finitely generated and free A-module (meaning $B \simeq A^n$ as an A-module).

For $\alpha \in B$, we consider $\tilde{\alpha} : B \to B$ by $x \mapsto a \cdot x$. Then we define the **trace** $\operatorname{Tr}_{B/A}(\alpha) \in A$ to be the trace of the matrix associated to $\tilde{\alpha}$. Similarly we define the **norm** $\operatorname{N}_{B/A}(\alpha) \in A$ to be the determinant of the matrix associated to $\tilde{\alpha}$.

We can see that this corresponds to the Vieta-style coefficients of the characteristic polynomial.

We might have seen this in the context of fields. If L/K is a finite extension of fields which is Galois, and we take $\alpha \in L$, we may have seen the "sum of conjugates" definition

$$\operatorname{Tr}_{L/K}(\alpha) = \sum_{\sigma \in \operatorname{Gal}(L/K)} \sigma(\alpha) \in K.$$

It turns out these definitions coincide; we'll see this later.

Lemma 4.3

Let K be a number field. If $\alpha \in \mathcal{O}_K$, then $\operatorname{Tr}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$.

(A priori, we would only expect $\operatorname{Tr}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Q}$.)

Proof. Let f be the minimal polynomial of α; by Gauss it has integral coefficients. Note that it is the characteristic polynomial p of $\tilde{\alpha}$ which acts on $\mathbb{Q}(\alpha)$. (This is trivial. One way to see it is by noting that $\deg f = \deg p$, and by Cayley-Hamilton, f divides p.)

If $K = \mathbb{Q}(\alpha)$ we would be done, but we're not necessarily so lucky. In general, we have a tower of fields

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq K.$$

We can interpret K as a $\mathbb{Q}(\alpha)$ vector space. Then $\tilde{\alpha}$ over K as a matrix is just a bunch of copies of the matrix $\tilde{\alpha}$ over $\mathbb{Q}(\alpha)$ (diagonal copies). □

§4.2 Trace Pairing

Define a map $K \times K \to \mathbb{Q}$ by

$$(x, y) \mapsto \operatorname{Tr}_{K/\mathbb{Q}}(xy).$$

This map is $\mathbb{Q}$-bilinear. By currying, this gives a map

$$K \to \operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{Q}) = K^\vee$$

by

$$y \mapsto \Psi_y \stackrel{\text{def}}{=} (x \mapsto \operatorname{Tr}_{K\mathbb{Q}}(xy)).$$

Here $K^\vee$ is the *dual* vector space (in the notation of Gaitsgory). Now,

Proposition 4.4

The map $y \mapsto \Psi_y$ is actually an isomorphism $K \xrightarrow{\sim} K^\vee$.

Proof. First, we check that the map is injective. It suffices to check that it has nontrivial kernel: letting $y \neq 0$, we note that the map for y, Ψ_y is not the zero map since

$$\Psi_y(y^{-1}) = \operatorname{Tr}_{K/\mathbb{Q}} 1 = [K : \mathbb{Q}] \neq 0.$$

For dimension reasons, any map $K \to K^\vee$ which is injective must be an isomorphism. □

Remark 4.5. This proof would fail if we tried to replace $\mathbb{Q}$ with a field of characteristic p, because in that case $[K : \mathbb{Q}]$ may not be zero.

§4.3 Dual Subgroups

Definition 4.6. For any *additive subgroup* $L \subseteq K$, define the **complementary subgroup** $L^\vee \subseteq K$ by

$$L^\vee \stackrel{\text{def}}{=} \left\{ \alpha \in K \mid \operatorname{Tr}_{K/\mathbb{Q}}(\alpha x) \in \mathbb{Z} \quad \forall x \in L \right\} \subseteq K.$$

Question 4.7. Show that if $A \subseteq B$ then $A^\vee \supseteq B^\vee$.

Example 4.8 (Example of a Complementary Subgroup)

Let $e_1, \dots, e_n$ be a $\mathbb{Q}$-basis of K, and consider the case $L = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_n$ (i.e. the subgroup generated by the e_i's). Using the trace pairing isomorphism, $L^\vee$ viewed as a subgroup of $K^\vee$ is given by

$$\mathbb{Z}e_1^\vee + \cdots + \mathbb{Z}e_n^\vee$$

Proof. This is tautology...

Let $e_1^\vee, \dots, e_n^\vee$ to be the dual basis (it's a $\mathbb{Q}$-basis). We have $e_i \in K^\vee$, but we can now think of each $e_i^\vee$ as an element of K using the isomorphism.

Unwinding the definition, $L^\vee$ viewed as a subgroup of $K^\vee$ means

$$\left\{ \xi \in K^\vee \mid \xi(x) \in \mathbb{Z} \quad \forall x \in L \right\}.$$

Here ξ is the image of α under the definition. Tautologically, the condition on ξ is the one we gave. □

§4.4 Proving the main theorem

Let's actually do something now. We showed that $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ for all $\alpha \in \mathcal{O}_K$.

Question 4.9. Viewing $\mathcal{O}_K$ as an additive subgroup of K, we have

$$(\mathcal{O}_K)^\vee \supseteq \mathcal{O}_K.$$

(Recall that $(\mathcal{O}_K)^\vee \subseteq K$ is a complementary subgroup.)

Now we claim that $\mathcal{O}_K$ is finitely generated over $\mathbb{Z}$. Take a $\mathbb{Q}$-basis $e_1, \dots, e_n$ of K. We can assume $e_1, \dots, e_n \in \mathcal{O}_K$ by scaling the basis appropriately (recall that for any $\alpha \in K$, $n\alpha \in \mathcal{O}_K$ for some n).

Remark 4.10. I don't claim that the e_i's generate $\mathcal{O}_K$, but at least they are contained in it.

Hence define $L = \mathbb{Z} \cdot e_1 + \dots + \mathbb{Z} \cdot e_n \subseteq \mathcal{O}_K$. Now we can take the complementary subgroups, to obtain

$$(\mathcal{O}_K)^\vee \subseteq L^\vee.$$

Hence by the question,

$$L \subseteq \mathcal{O}_K \subseteq (\mathcal{O}_K)^\vee \subseteq L^\vee.$$

So $\mathcal{O}_K$ is trapped inside $L^\vee$ which is finitely generated, and hence $\mathcal{O}_K$ is itself finitely generated.

Example 4.11

Let $K = \mathbb{Q}(\sqrt{d})$ and let $L = \mathbb{Z}[\sqrt{d}]$. We wish to compute $L^\vee$. We can let $e_1 = 1$ and $e_2 = \sqrt{d}$. Then $e_1^\vee = \frac{1}{2}$ and $e_2^\vee = \frac{1}{2}d^{-1/2}$. (Do some blah computation. We have

$$\sqrt{d} \sim \begin{pmatrix} 0 & 1 \\ d & 0 \end{pmatrix}$$

and so some computation gives you that this is the dual basis (i.e. that $e_i^\vee(e_j)$ really is 1 for $i = j$ and 0 otherwise.))

Remark 4.12. One might wonder if the inclusion $\mathcal{O}_K \subseteq (\mathcal{O}_K)^\vee$ is strict. In fact, it's a deeper theorem (which we'll prove) that $\mathcal{O}_K \subsetneq (\mathcal{O}_K)^\vee$ holds if and only if $K = \mathbb{Q}$.

§5 February 6, 2015

Last time we showed that if K is a number of a field of rank r, then $\mathcal{O}_K$ turns out to be isomorphic to $\mathbb{Z}^r$. We used the trace pairing to get an isomorphism from K to $\text{Hom}_{\mathbb{Q}}(K, \mathbb{Q})$. We also defined the complementary module.

§5.1 Discriminant

Let $\mathcal{O}_K^\vee$ be the complementary subgroup of $\mathcal{O}_K$. We saw that $\mathcal{O}_K \subseteq \mathcal{O}_K^\vee$ and both are of rank r. Hence the additive group

$$\mathcal{O}_K^\vee / \mathcal{O}_K$$

is a finite abelian group. We define this to be the **discriminant** of K (up to sign; we're about to give a signed definition of discriminant).

Lemma 5.1

Let $\alpha_1, \dots, \alpha_n$ be a $\mathbb{Z}$-basis of $\mathcal{O}_K$. Consider the $n \times n$ matrix M whose (i,j)th entry is $\text{Tr}_{K/Q}(\alpha_i \alpha_j)$. Then $\det M$ is the discriminant of K, i.e.

$$\det M = \pm \left[\mathcal{O}_K^\vee : \mathcal{O}_K \right].$$

This should be surprising: it's not at all clear that the matrix M does not depend on the choice of basis.

Before we do anything, let's compute the discriminant of our standard example $\mathbb{Q}(\sqrt{d})$.

Example 5.2 (Discriminant when $d \not\equiv 1 \pmod 4$)

If $d \not\equiv 1 \pmod 4$, then

$$\mathcal{O}_K = \mathbb{Z} + \mathbb{Z} \cdot \sqrt{d}$$

and $\{1, \sqrt{d}\}$ is a basis. One can check that $\text{Tr}(\sqrt{d}) = 0$, while $\text{Tr}(1) = 2$ and $\text{Tr}(d) = 2d$, so in this case the discriminant is equal to

$$\det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d$$

Example 5.3 (Discriminant when $d \equiv 1 \pmod 4$)

One can check that if $d \equiv 1 \pmod 4$, then $\mathcal{O}_K$ has $\mathbb{Z}$-basis $1, \frac{1+\sqrt{d}}{2}$.

Since $\text{Tr}(1) = 2$ and $\text{Tr}(\sqrt{d}) = 0$, we get in general that $\text{Tr}(a + b\sqrt{d}) = 2a$. So we may compute the discriminant to be

$$\det \begin{pmatrix} 2 & 1 \\ 1 & \frac{1}{2}(d+1) \end{pmatrix} = d.$$

These will become important later when we study ramified things.

§5.2 Left-Hand Side is Invariant

More generally, suppose we have $\alpha_1, \dots, \alpha_n \in K$ and $\beta_1, \dots, \beta_n \in K$ elements (not necessarily a basis). Denote

$$\underline{\alpha} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} \quad \text{and} \quad \underline{\beta} = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix}.$$

Then we can look at the matrix $\underline{\alpha} \cdot \underline{\beta}^T$, and look at the term-wise traces.

Lemma 5.4

If M is a $n \times n$ matrix with rational coefficients and $\underline{\alpha}' = M \cdot \underline{\alpha}$, then

$$\det \left(\operatorname{Tr}_{K/Q}(\underline{\alpha}' \cdot \underline{\beta}^T)_{i,j} \right) = \det M \cdot \det \left(\operatorname{Tr}_{K/Q}(\underline{\alpha} \cdot \underline{\beta}^T)_{i,j} \right)$$

Here, again, we're taking termwise traces.

Proof. The main observation is that $\operatorname{Tr}_{K/\mathbb{Q}}(q \cdot x) = q \operatorname{Tr}_{K/\mathbb{Q}}(x)$ for $q \in \mathbb{Q}$ and $x \in K$. Writing out the matrix multiplication, you can get

$$\operatorname{Tr}_{K/Q}(\underline{\alpha}' \cdot \underline{\beta}^T)_{i,j} = M \cdot \operatorname{Tr}_{K/Q}(\underline{\alpha} \cdot \underline{\beta}^T)_{i,j}.$$

At this point, the teacher makes the following remark of which I'm very happy because it strongly agrees with part of my teaching philosophy.

> This is one of those things that if I write out, one of two things will happen: either I will get confused, or even if that doesn't happen, anyone who is already confused will be confused. You should just do the calculation for a 2×2 matrix and it will be immediately clear why this is true.

Anyways, this completes the proof. □

Corollary 5.5

Given α and β as above such that the $\{\alpha_i\}$ and $\{\beta_i\}$ are $\mathbb{Q}$-bases, then the quantity $\det \operatorname{Tr}(\underline{\alpha} \cdot \underline{\beta}^T)_{i,j}$ depends only up to sign on the groups

$$L = \mathbb{Z} \cdot \alpha_1 + \dots + \mathbb{Z} \cdot \alpha_n$$
$$L' = \mathbb{Z} \cdot \beta_1 + \dots + \mathbb{Z} \cdot \beta_n$$

Proof. If $\alpha_1', \dots, \alpha_n'$ is another $\mathbb{Z}$-basis for L, then $\underline{\alpha}' = M \cdot \alpha$. From the fact that α is a basis, we obtain that M has integer coefficients. Going the other way, we get that M^{-1} has integer coefficients. Hence $\det M$ and $\det M^{-1} = (\det M)^{-1}$ are both integers, so they are ± 1.

So the cost of switching from $\{\alpha_i\}$ to the $\{\alpha_i'\}$ is just a factor of ± 1. The cost for switching β is also ± 1. □

During the next corollary:

cell phone rings
"It's my wife!"
pause
"I'm explaining the discriminant!'
resumes writing

Corollary 5.6
If $\alpha_1, \dots, \alpha_n$ is a $\mathbb{Q}$-basis, then $\det \operatorname{Tr}(\alpha_i\alpha_j)_{i,j}$ depends only on the value of $I = \mathbb{Z} \cdot \alpha_1 + \cdots + \mathbb{Z}\alpha_n$ (not even up to sign).

Proof. This comes through the proof of the previous lemma.

Note that in the previous proof, if we do the change twice we pick up a factor of $\det M$ for changing one guy and $\det M$ for changing the other guy, so in fact the cost is $(\det M)^2 = 1$ – no minus signs. □

§5.3 Finishing the Proof

Let's pause for a moment. We were trying to prove

$$\det \operatorname{Tr}\left(\alpha_i\alpha_j\right)_{i,j} = \pm[\mathcal{O}_K^\vee : \mathcal{O}_K].$$

All of our sublemmas let us show that the left-hand side does not depend on the choice of basis (here $L = \mathcal{O}_K$). Now, let's prove a next lemma.

Lemma 5.7
Suppose $\alpha_1, \dots, \alpha_n$ is a $\mathbb{Q}$-basis of K, that $L = \alpha_1\mathbb{Z} \oplus \cdots \oplus \alpha_n\mathbb{Z}$ as before, and M is a matrix with integer coefficients with $\det M \neq 0$. Let $\underline{\alpha}' = M \cdot \underline{\alpha}$ and L' its $\mathbb{Z}$-span. Then
$$[L : L'] = \pm \det M.$$

We'll prove this next time for time reasons. Let's complete the proof.

Now we can finally prove the main theorem. Let $\alpha_1^\vee$, …, $\alpha_n^\vee$ be the dual basis of $\alpha_1, \dots, \alpha_n$ the $\mathbb{Z}$-basis of $\mathcal{O}_K$. Then $\mathcal{O}_K^\vee \supseteq \mathcal{O}_K$, so we may write $\underline{\alpha} = M \cdot \underline{\alpha}^\vee$ where M is an integer matrix (can you guess what $\underline{\alpha}^\vee$ is?).

In that case,
$$\det\left(\operatorname{Tr}(\underline{\alpha} \circ \underline{\alpha}^T)_{i,j}\right) = \det M \cdot \det\left(\operatorname{Tr}(\underline{\alpha}^\vee \cdot \underline{\alpha}^T)_{i,j}\right)$$
but $\underline{\alpha}^\vee \cdot \underline{\alpha}^T$ is the identity for everything by definition, so the determinant is 1. On the other hand $\det M = \pm|\mathcal{O}_K^\vee : \mathcal{O}_K|$.

§6 February 11, 2015

Now let us prove the lemma from last time.

§6.1 Finishing the Proof of Lemma

We have the following reformulation.

Lemma 6.1

If $L \subseteq V$ is a finitely generated abelian group, which contains a $\mathbb{Q}$-basis for V. Let $M : L \to L$ be linear and suppose $\det M \neq 0$ (meaning M is injective), and set $L' = M\text{“}(L)$ the image of M.

Then $[L : L'] = \pm \det M$.

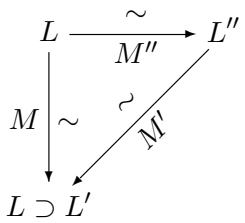
Sanity checks: The fact that L contains a $\mathbb{Q}$-basis of V means that it's a free group of some rank; say $L \cong \mathbb{Z}^r$. The fact that $\det M \neq 0$ means that M is injective, so L', so L' also has rank r.

Now we prove the lemma. The idea is that we want to use induction.

Suppose we have a chain of finite abelian groups

$$L \supsetneq L'' \supsetneq L'$$

where all groups are free $\mathbb{Z}$-modules. Then we can get a commutative diagram of maps



by projecting bases. In that case we have

$$\det M = \det M' \cdot \det M''.$$

Moreover, $[L : L''][L'' : L'] = [L : L']$, and so we have an "inductive step".

Hence, we only need to consider the case where no such intermediate L'' exists. In that case $[L : L']$ is of prime order. (Indeed, choices of L'' correspond to nontrivial proper subgroups of L/L'.) Hence the whole song and dance reduces us to the prime order case; as we'll soon see this makes the manipulation much nicer.

Suppose $L/L' \cong \mathbb{Z}/p\mathbb{Z}$. Choose any basis $\alpha_1, \dots, \alpha_n$ of L. Then consider the projection of

$$L = \bigoplus \alpha_i \mathbb{Z} \twoheadrightarrow L/L' \cong \mathbb{Z}/p\mathbb{Z}.$$

So some α_i, say α_1, must have nonzero kernel. Then by fiddling with the α_i for $i > 2$, we can replace α_i with $\alpha_i - c\alpha_1$ for some α's; hence we may assume without loss of generality that α_1 has nonzero image but $\alpha_2, \dots, \alpha_n$ live in the kernel L'.

Look at $p \cdot \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \dots + \alpha_n\mathbb{Z}$ Clearly it's a subset of L'; then for index reasons it must equal L'. Thus the matrix is actually

$$\begin{pmatrix} p & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

which has determinant p.

There's also a case to handle where $L = L'$, but in this case that means M is a bijection, and hence has an inverse, and again we have $\mathbb{Z} \ni \det M, \det M^{-1} = (\det M)^{-1}$ and so $\det M = \pm 1$.

§6.2 A Second Argument

Let $L \supset L'$ and consider $U = L \otimes \mathbb{R}/L' \otimes \mathbb{R}$. This gives us a covering map $U/L' \to U/L$ which has degree $[L : L']$.

Then, informally speaking, the covering map has a notion of volume via

$$\operatorname{Vol}(U/L') = [L : L'] \operatorname{Vol}(V/L).$$

Hence $\det M = [L : L']$.

§6.3 Application of the Discriminant

Let D_K denote the discriminant of the number field K. Next time we hope to prove the following.

Proposition 6.2

Let K and L be linearly disjoint number fields over $\mathbb{Q}$. Then

$$\mathcal{O}_K \cdot \mathcal{O}_L \subseteq \mathcal{O}_{K \cdot L} \subseteq \frac{1}{\gcd(D_K, D_L)} \mathcal{O}_K \cdot \mathcal{O}_L.$$

In particular if $\gcd(D_K, D_L) = 1$ the inclusions are equalities.

Here, recall that K, L live in algebraic closure $\overline{\mathbb{Q}}$; then $K \cdot L$ is the subfield (in $\overline{\mathbb{Q}}$) generated by K and L. We will define "linearly disjoint" later.

Note that the inclusion $\mathcal{O}_K \cdot \mathcal{O}_L \subseteq \mathcal{O}_{K \cdot L}$ is obvious.

Example 6.3

Let $K = \mathbb{Q}(\sqrt{5})$ and $L = \mathbb{Q}(\sqrt{7})$. Then $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ and $\mathcal{O}_L = \mathbb{Z}[\sqrt{7}]$. Then $D_K = 5$, $D_L = 28$ and so we conclude

$$\mathcal{O}_{K \cdot L} = \mathbb{Z}[\sqrt{7}, \frac{1+\sqrt{5}}{2}].$$

Example 6.4

For an example when $\gcd(D_K, D_L) \neq 1$ and equality fails, we may take $K = \mathbb{Q}(\sqrt{7})$ (hence $\mathcal{O}_K = \mathbb{Z}[\sqrt{7}]$, $D_K = 28$) and $L = \mathbb{Q}(\sqrt{11})$ (hence $\mathcal{O}_L = \mathbb{Z}[\sqrt{11}]$, $D_L = 44$). And you can check that

$$\frac{\sqrt{7} - \sqrt{11}}{2} \in \mathcal{O}_{K \cdot L}.$$

§7 February 13, 2015

In this lecture we'll define "linearly disjoint" and then prove the proposition of last time, namely:

> Let K and L be linearly disjoint number fields over $\mathbb{Q}$. Then
> $$\mathcal{O}_K \cdot \mathcal{O}_L \subseteq \mathcal{O}_{K\cdot L} \subseteq \frac{1}{\gcd(D_K, D_L)} \mathcal{O}_K \cdot \mathcal{O}_L.$$
> In particular if $\gcd(D_K, D_L) = 1$ the inclusions are equalities.

§7.1 Linearly Disjoint Fields

Let K and L be number fields over $\mathbb{Q}$; hence they live in some algebraic closure $\overline{\mathbb{Q}}$. Then we say K and L are **linearly disjoint** if

$$[K \cdot L : \mathbb{Q}] = [K : \mathbb{Q}]\,[L : \mathbb{Q}]\,.$$

Here $K \cdot L$ is the smallest field containing both. Equivalently, the projection

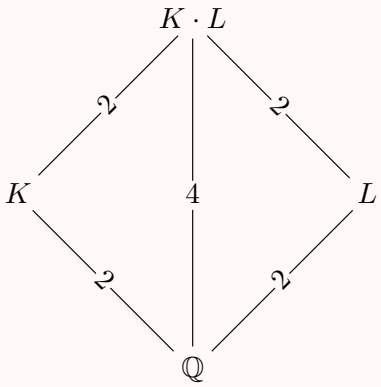
$$K \otimes L \twoheadrightarrow K \cdot L \subseteq \overline{\mathbb{Q}}$$

by the map $\alpha \otimes \beta \to \alpha \cdot \beta$ should be an isomorphism.

Intuitively, this just means the fields should be "as disjoint as impossible".

Example 7.1

For any quadratic fields K, L which are distinct, we claim the fields K and L are linearly independent. Indeed, just consider the towers



The point is that if $K \neq L$ then $[KL : L] > 1 \implies [KL : L] \geq 2$.

§7.2 Traces are Integers

Proposition 7.2

Let $\mathbb{Q} \subseteq K \subseteq L$ be number fields and consider the map $\operatorname{Tr}_{L/K} : L \to K$. Then $\operatorname{Tr}_{L/K}(\mathcal{O}_L) \subseteq \mathcal{O}_K$.

Proof. This is similar to our solution when $K = \mathbb{Q}$. Consider the characteristic polynomial

$$P_\alpha(X) = \det_K \left(X - \tilde{\alpha}|_L\right)$$

We will prove more strongly that all coefficients of P_α are in $\mathcal{O}_K$.

Let $\alpha \in \mathcal{O}_L$. Let $P_{\alpha,K}(X) \in K[X]$ be the minimal polynomial. It's enough to show $P_{\alpha,0}(X)$ has coefficients in $\mathcal{O}_K$, because then we have a tower

$$K \subseteq K(\alpha) \subseteq L$$

so that the characteristic polynomial is a power of $P_{\alpha,0}$.

Let $P_{\alpha,\mathbb{Q}}$ be the minimal polynomial over $\mathbb{Q}$. Then $P_{\alpha,K}$ divides it in the ring $K[X]$. We know that $P_{\alpha,\mathbb{Q}}(X)$ has integer coefficients (since α is an algebraic integer, from the first lecture).

All roots of $P_{\alpha,\mathbb{Q}}$ are integral over $\mathbb{Z}$, so all roots of $P_{\alpha,K}$ are integral over $\mathbb{Z}$. Hence the coefficients of $P_{\alpha,K}$ are integral over $\mathbb{Z}$, which means exactly that $P_{\alpha,K} \in \mathcal{O}_K[X]$. □

§7.3 Gauss's Lemma

A closely related lemma (i.e. with around the same proof) is as follows.

Lemma 7.3 (Gauss's Lemma for $\mathcal{O}_K$)
If $g, h \in K[X]$ are monic, $g \cdot h \in \mathcal{O}_K[X]$. Then g and h are also in $\mathcal{O}_K[X]$.

Proof. Let $L \subseteq \overline{K}$ be a splitting field of $g \cdot h$. If $\alpha \in L$ is a root of L, then α is integral over $\mathcal{O}_K$, *id est*, α is in the integral closure of $\mathcal{O}_K$ in L. So the coefficients of g are symmetric sums of such α's and hence themselves integral over $\mathcal{O}_K$. □

§7.4 Trace as Sums of Galois Things

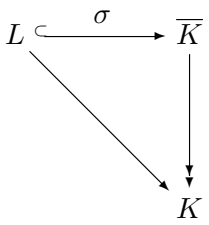
Lemma 7.4
Let L/K be a field extension. If $\overline{K}$ is the algebraic closure of K and $\alpha \in L$ then

$$\operatorname{Tr}_{L/K}(\alpha) = \sum_{\sigma : L \hookrightarrow \overline{K}} \sigma(\alpha) \in K.$$

Here the sum runs over all maps $\sigma : L \to \overline{K}$ which fix K.

A priori we would only expect the sum to live in $\overline{K}$.

To elaborate on the summation, we want



If L/K is Galois, then for a fixed embedding $\tau : L \to \overline{K}$, then all other morphism are of the form $\tau \circ \phi$ where $\phi \in \operatorname{Gal}(L/K)$.

Proof in next lecture.

§8 February 18, 2015

§8.1 Loose Ends

Let's complete the proof of last time. Recall we were trying to prove

> Let L/K be a field extension. If $\overline{K}$ is the algebraic closure of K and $\alpha \in L$ then
> $$\operatorname{Tr}_{L/K}(\alpha) = \sum_{\sigma : L \hookrightarrow \overline{K}} \sigma(\alpha) \in K.$$
> Here the sum runs over all maps $\sigma : L \to \overline{K}$ which fix K.

A priori we would only expect the sum to live in $\overline{K}$.

Proof. Suppose first $L = K(\alpha)$, and let $n = [L : K]$. Let

$$p(X) \stackrel{\text{def}}{=} \det_K(X - \alpha|_L).$$

We claim this equals

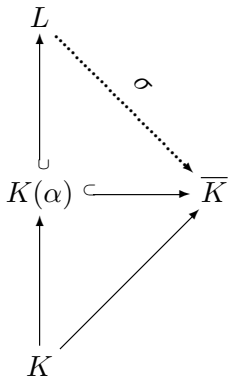
$$\prod_{\sigma : L \to \overline{K}} (X - \sigma\alpha).$$

In $\overline{K}$ we see $p(X)$ decomposes as

$$(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$$

where $\alpha_1, \dots, \alpha_n \in \overline{K}$ are distinct (since we're in characteristic zero, all irreducible polynomials are separable). Every map σ is required to send $\alpha \in L$ to a given $\alpha_i \in \overline{K}$; hence at most n embeddings exist. But $\deg p = n$, so they must all work.

For the general case, let $\alpha \in K \setminus L$, and consider the diagram



We claim there are exactly $[L : K(\alpha)]$ embeddings. This will imply the conclusion, because then we will get

$$\sum_{L \hookrightarrow \overline{K}} \sigma(\alpha) = [L : K(\alpha)] \sum_{\sigma_0 : K(\alpha) \hookrightarrow \overline{K}} \sigma_0(\alpha)$$

and the trace has the same property.

Now just throw the primitive element theorem at it. □

Note that by the same proof we obtain

Corollary 8.1

The norm of α over L/K is

$$\mathrm{N}_{L/K}(\alpha) = \prod_{\sigma : L \to \overline{K}} \sigma(\alpha).$$

§8.2 Finishing the proof

Now we will finally finish proving this result from like a week ago.

Let K and L be linearly disjoint number fields over $\mathbb{Q}$. Then

$$\mathcal{O}_K \cdot \mathcal{O}_L \subseteq \mathcal{O}_{K \cdot L} \subseteq \frac{1}{\gcd(D_K, D_L)} \mathcal{O}_K \cdot \mathcal{O}_L.$$

In particular if $\gcd(D_K, D_L) = 1$ the inclusions are equalities.

We need to define the following generalization of the dual subgroup.

Definition 8.2. For any extension of number fields $K \subseteq K'$ and $\mathcal{O}_K$ submodule $L \subseteq K'$, then

$$L^{\vee_K} \stackrel{\text{def}}{=} \left\{ \alpha \in K' \mid \mathrm{Tr}_{L/K}(\alpha\beta) \in \mathcal{O}_K \ \forall \beta \in L. \right\}.$$

We saw before just the case where $K = \mathbb{Q}$.

Proposition 8.3

If K, L are linearly disjoint then

$$(\mathcal{O}_K \otimes \mathcal{O}_L)^{\vee_K} = \mathcal{O}_K \otimes \mathcal{O}_L^\vee = \mathcal{O}_K \cdot \mathcal{O}_L^\vee \subseteq K \cdot L.$$

Proof. This is carefully unwinding definitions. If $\alpha \in L$, then

$$\det_K (X - \alpha \mid_{K \cdot L}) = \det_{\mathbb{Q}}(X - \alpha|_L)$$

just because a $\mathbb{Q}$-basis of L is a K-basis for $K \cdot L$ (we use linear independence here).

Let $e_1, \dots, e_s$ be a $\mathbb{Z}$-basis for $\mathcal{O}_K$ so

$$\mathcal{O}_K = \bigoplus_i \mathbb{Z} e_i.$$

meaning it's a $\mathbb{Q}$-basis for K. Then

$$\mathcal{O}_K \otimes \mathcal{O}_L = \bigoplus \mathcal{O}_L \cdot e_1.$$

For any $\beta \in L$,

$$\begin{aligned}
\mathrm{Tr}_{LK/K}(\alpha \cdot \beta) &= \mathrm{Tr}_{LK/K}(\sum_i e_i \alpha_i \beta) \\
&= \sum e_i \, \mathrm{Tr}_{LK/K}(\sum_i e_i \alpha_i \beta) \\
&= \sum_i e_i \, \mathrm{Tr}_{LK/K}(\alpha_i \beta) \\
&= \sum_i e_i \, \mathrm{Tr}_{L/\mathbb{Q}}(\alpha_i \beta)
\end{aligned}$$

Now suppose $\beta \in \mathcal{O}_L$. Then

$$\operatorname{Tr}_{LK/K}(\alpha\beta) \in \mathcal{O}_K \iff \operatorname{Tr}_{L/\mathbb{Q}}(\alpha_i \cdot \beta) \in \mathbb{Z} \quad 1 \le i \le s. \qquad \square$$

§9 February 20, 2015

Didn't attend class. Here is a very short summary.

Let p be an odd prime and ζ_p be a primitive pth root of unity. We showed that

$$\operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^*$$

is the cyclic group of order $p-1$, in the canonical way $\zeta_p \mapsto \zeta_p^i$. In particular, $x^{p-1}+\cdots+1$ is irreducible over $\mathbb{Q}$.

§10 February 23, 2015

Assume the results of the previous lecture. Last time we established the following.

Let p be an odd prime.

> "If p is even, the theory is trivial. Left as an exercise."

Theorem 10.1
$\mathbb{Q}(\zeta_p)/\mathbb{Q}$ has Galois group $(\mathbb{Z}/p\mathbb{Z})^*$.

§10.1 The ring of integers of the cyclotomic field

Let $K = \mathbb{Q}(\zeta_p)$. We continue our investigation of cyclotomic fields by proving that $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$.

First, an intermediate proposition.

Proposition 10.2
$\mathrm{Tr}_{K/\mathbb{Q}}(\zeta_p) = -1$ and $\mathrm{N}_{K/Q}(1-\zeta_p) = p$.

Proof. Just use the minimal polynomial. This is an olympiad exercise. □

The norm calculation is what Kisin calls a "dinner party problem", because of the elementary phrasing and the "one-trick" solution: given a regular p-gon $A_1A_2\dots A_p$ in a unit circle, we have

$$A_pA_1 \cdot A_pA_2 \cdot \dots \cdot A_pA_{p-1} = p.$$

Remark 10.3. This implies that $1-\zeta_p$ is not a unit in $\mathcal{O}_K$; note that $\mathrm{N}_{K/Q}(1-\zeta_p) = p$ is not a unit and any unit must have norm ± 1.

Lemma 10.4
The rational integers contained in $\mathcal{O}_K \cdot (1-\zeta_p)$ are precisely the multiples of p.

Proof. We can see that $p \in \mathcal{O}_K \cdot (1-\zeta_p)$ from the above, since $1-\zeta_p^k \in \mathcal{O}_K$ for every integer k and we can use the fact that

$$(1-\zeta_p)\mathcal{O}_K \ni (1-\zeta_p)\prod_{k=2}^{p-1}\left(1-\zeta_p^k\right) = p.$$

Hence, $p\mathbb{Z}$ is contained inside this set. Now assume some other integer relatively prime to p is contained in the set. By Bezout's Lemma, we force $1 \in (1-\zeta_p)\mathcal{O}_K$. Hence $(1-\zeta_p)\alpha = 1$ for some $\alpha \in \mathcal{O}_K$ which is impossible because by taking norms (or from the remark earlier that $1-\zeta_p$ is not a unit). □

Corollary 10.5
$\mathrm{Tr}_{K/\mathbb{Q}}(y(1-\zeta_p)) \in p\mathbb{Z}$ for any $y \in \mathcal{O}_K$.

Proof. We compute

$$\begin{aligned}
\mathbb{Z} &\ni \operatorname{Tr}_{K/\mathbb{Q}}(y(1-\zeta_p)) \\
&= \sum_{\sigma \in \operatorname{Gal}(K/\mathbb{Q})} \sigma(y(1-\zeta_p)) \\
&= \sum_{\sigma \in \operatorname{Gal}(K/\mathbb{Q})} \sigma(y)(1-\sigma(\zeta_p)) \\
&= \sum_{\sigma \in \operatorname{Gal}(K/\mathbb{Q})} \sigma(y)(1-\zeta_p^{\text{something}}) \\
&\in (1-\zeta_p) \cdot \mathcal{O}_K.
\end{aligned}$$

But it's also in $\mathbb{Z}$ as needed. □

Now we can prove the main result.

Theorem 10.6

The ring of integers of K is precisely $\mathbb{Z}[\zeta_p]$.

Proof. Since each ζ_p^k is in K, we only need the other inclusion.

Let $x \in \mathcal{O}_K$, and write it in the basis

$$x = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2}$$

where $a_i \in \mathbb{Q}$. (Notice we only go up to $p-2$! There's a relation between all $p-1$ powers: they have sum -1.)

We want to show that each a_i is in fact an integer. It would be nice if we could just take the trace directly, but this doesn't work. So we instead do the following trick:

$$\mathcal{O}_K \ni (1-\zeta_p)x = a_0(1-\zeta_p) + a_1(\zeta_p - \zeta_p^2) + \cdots + a_{p-2}(\zeta_p^{p-2} - \zeta_p^{p-1}).$$

Now we take the trace of this. We see that $\operatorname{Tr}_{K/\mathbb{Q}}(\zeta_p - \zeta_p^2) = 1 - 1 = 0$ (or even more lazily, these terms are Galois conjugates so they have the same trace). Similarly all the other terms vanish. On the other hand, $\operatorname{Tr}_{K/\mathbb{Q}}(1-\zeta_p) = p$. Hence we obtain

$$a_0 p = \operatorname{Tr}_{K/\mathbb{Q}}\left(x(1-\zeta_p)\right)$$

which is in $p\mathbb{Z}$ by the corollary (a priori we only expect $\mathbb{Z}$), hence $a_0 \in \mathbb{Z}$.

To get the rest of the coefficients are integers, just use do cyclic shifts, considering $(x - a_0)/\zeta_p \in \mathcal{O}_K$. □

§10.2 Discriminant

We finish our study with the following result.

Theorem 10.7

The discriminant of $\mathbb{Q}(\zeta_p)$ is $p^{p-2} \cdot (-1)^{\frac{1}{2}(p-1)}$.

I am somewhat dismayed to see this proven in class, because I submitted my homework two weeks early and stayed up an hour proving it myself because I had no idea we would get it for free. So I'll just copy the proof I put on my homework.

We can compute the discriminant of K as follows. It is not hard to see that for $k = 0, 1, \dots, p-1$ we have

$$\operatorname{Tr}_{K/\mathbb{Q}}(\zeta_p^k) = \begin{cases} p-1 & k = 0 \\ -1 & \text{otherwise} \end{cases}$$

since $\widetilde{\zeta_p^k}$ permutes basis elements, other than $\zeta_p^{p-1} = -(1 + \cdots + \zeta_p^{p-2})$. It follows that the discriminant is

$$\det \begin{pmatrix} p-1 & -1 & -1 & \dots & -1 & -1 & -1 \\ -1 & -1 & -1 & \dots & -1 & -1 & -1 \\ -1 & -1 & -1 & \dots & -1 & -1 & p-1 \\ -1 & -1 & -1 & \dots & -1 & p-1 & -1 \\ -1 & -1 & -1 & \dots & p-1 & -1 & -1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ -1 & -1 & p-1 & \dots & -1 & -1 & -1 \end{pmatrix}.$$

Adding the second column to all the others gives

$$\det \begin{pmatrix} p & -1 & 0 & \dots & 0 & 0 & 0 \\ 0 & -1 & 0 & \dots & 0 & 0 & 0 \\ 0 & -1 & 0 & \dots & 0 & 0 & p \\ 0 & -1 & 0 & \dots & 0 & p & 0 \\ 0 & -1 & 0 & \dots & p & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & -1 & p & \dots & 0 & 0 & 0 \end{pmatrix} = p^{p-2} \cdot (-1)^{\frac{1}{2}(p-1)}$$

where the $\frac{1}{2}(p-1)$ is found by permuting columns.

§10.3 Square Definition of Discriminant

Lemma 10.8

Let L/K be a finite extension of number fields, and let $\underline{\alpha} = (\alpha_1, \dots, \alpha_n)$ be a $\mathbb{Z}$-basis of L. Let $\sigma_1, \dots, \sigma_n : L \to \overline{K}$ be the n embeddings of L.

Then the discriminant $D_L = D(\underline{\alpha})$ is also given by

$$D(\underline{\alpha}) = \left[\det(\sigma_j(a_i))_{i,j}\right]^2.$$

Proof. Let M be the matrix whose (i,j)th entry is $\sigma_j(a_i)$. We wish to show the discriminant is $(\det M)^2$. We have that

$$\begin{aligned} D_{L/K}(\underline{\alpha}) &= \det\left(\operatorname{Tr}_{L/K}(\alpha_i\alpha_j)\right)_{ij} \\ &= \det\left(\sum_k \sigma_k(\alpha_i\alpha_j)\right)_{ij} \\ &= \det\left(\sum_k \sigma_k(\alpha_i)\sigma_k(\alpha_j)\right)_{ij} \end{aligned}$$

Recognizing the sum of a matrix multiplication we discover

$$\begin{aligned} &= \det(MM^T) \\ &= (\det M)^2. \end{aligned}$$

□

Specifically, the point of the above proof is that

$$\begin{pmatrix} \sigma_1(\alpha_1) & \dots & \sigma_n(\alpha_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(\alpha_n) & \dots & \sigma_n(\alpha_n) \end{pmatrix} \begin{pmatrix} \sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \dots & \sigma_n(\alpha_n) \end{pmatrix}$$

equals

$$\begin{pmatrix} \operatorname{Tr}_{K/\mathbb{Q}}(\alpha_1\alpha_1) & \dots & \operatorname{Tr}_{K/\mathbb{Q}}(\alpha_1\alpha_n) \\ \vdots & \ddots & \vdots \\ \operatorname{Tr}_{K/\mathbb{Q}}(\alpha_n\alpha_1) & \dots & \operatorname{Tr}_{K/\mathbb{Q}}(\alpha_n\alpha_n) \end{pmatrix}$$

from matrix multiplication, and we can take the determinant of both sides.

§11 February 25, 2015

Didn't attend class. These notes are from W Mackey (thanks!).

We have proved the following statement: if L/K is an extension of degree n, and $\alpha_1, ..., \alpha_n \in L$, then $D(\underline{\alpha}) = \det(\mathrm{Tr}_{L/K}(\alpha_i\alpha_j)) - \det(\sigma_k(\alpha_i))^2$ for $\sigma_i : L \hookrightarrow \overline{K}$.

§11.1 Vandermonde Determinant

Corollary 11.1

If $L = K[x]$, $x \in L$ with minimal polynomial $f(X) \in K[X]$, then $D(1, x, ..., x^{n-1}) = (-1)^{n(n-1)/2} N_{L/K}(f'(x))$ where f' is the derivative of the polynomial.

The proof of this is our previous proposition: Let $x_1, \dots, x_n$ be the distinct roots of $f(X)$ in $\overline{K}$. Now f must be sent to one of these roots, since it evaluates to 0 on x, so $\det(\sigma_k(x^i))^2 = \det(x_k^i)_{k,i}^2$, which gives the determinant of

$$\begin{pmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{pmatrix}^2,$$

which is the **Vandermonde determinant**[1]

$$\left(\prod_{i<j} (x_i - x_j) \right)^2.$$

Anyways, this is also equal to

$$(-1)^{n(n-1)/2} \prod_{i \neq j} (x_i - x_j).$$

Then this is equal to $(-1)^{n(n-1)/2} \prod_i f'(x_i)$ since the derivative, by the product rule (since $f'(x_i) = \sigma_i(f'(x))$, and we nicely annihilate everything that has x_i in it), gives exactly the elements we want going over the js for an individual i, then we just take the product of these to get what we want. Then this is just equal to $(-1)^{n(n-1)/2} N_{L/K}(f'(x))$.

§11.2 Discriminant of Cyclotomic Field

Corollary 11.2

If $L = \mathbb{Q}(\zeta_p)$, and $K = \mathbb{Q}$, then $D_L = p^{p-2}(-1)^{(p-1)/2}$.

This is just a bit of ugly computation applying the above. We have $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^\times$ has even order, therefore it has a unique subfield of order 2, so we want to find a degree 2 extension of the field.

[1] We won't actually prove this, but it makes sense: if any $x_i = x_j$, then the matrix will have linearly dependent rows and should be annihilated by det.

§11.3 Divisibility of Discriminant

Lemma 11.3

Let $\mathbb{Q} \subseteq K \subseteq L$ be an extension of number fields. Then D_K divides D_L.

This gives the result: Let $H = \mathbb{Z}/(p-1)\mathbb{Z} \simeq (\mathbb{Z}/p\mathbb{Z})^\times$. Then $K = \mathbb{Q}(\zeta_p)^H$ is a quadratic extension of $\mathbb{Q}$, with $L = \mathbb{Q}(\zeta_p)$. If $K = \mathbb{Q}(\sqrt{d})$, with d squarefree, we have $D_k = d$ if $d \equiv 1 \pmod 4$, and $4d$ otherwise. Then

$$D_L = \pm p^{p-2}.$$

Since p is odd, we have $d \equiv 1 \pmod 4$, and since it's squarefree, we must have only p, hence $d = \pm p$. Then, of course, these two facts completely determine what d is.

Before proving the lemma, we first prove the following. As a sublemma:

Lemma 11.4

If $K \subseteq L \subseteq M$ is an extension of number fields, and $\alpha \in M$, then $\operatorname{Tr}_{M/K}(\alpha) = \operatorname{Tr}_{L/K} \circ \operatorname{Tr}_{M/L}(\alpha)$.

Proof. Let $\overline{K}$ be an algebraic closure of K. Then $\operatorname{Tr}_{M/K}(\alpha) = \sum_{\sigma : M \to \overline{K}} \sigma(\alpha) = \sum_{i : L \to \overline{K}} \sum_\sigma \sigma(\alpha)$ where σ extends the embedding of L into an embedding of M. Then this is just the composition of the two traces. ∎

Now we claim the following.

Claim 11.5. $\mathcal{O}_K^\vee \subseteq \mathcal{O}_L^\vee$.

Proof. This comes straight from the definition $\mathcal{O}_K^\vee = \{\alpha \in K : \operatorname{Tr}_{K/\mathbb{Q}}(\alpha\beta) \in \mathbb{Z} \forall \beta \in \mathcal{O}_K\}$. From the sublemma, for $\alpha \in \mathcal{O}_K^\vee$, and $\beta \in \mathcal{O}_L$, we have $\operatorname{Tr}_{L/\mathbb{Q}}(\alpha\beta) = \operatorname{Tr}_{K/\mathbb{Q}} \operatorname{Tr}_{L/K}(\alpha\beta) = \operatorname{Tr}_{K/\mathbb{Q}}(\alpha \operatorname{Tr}_{L/K}(\beta)) \in \mathbb{Z}$ by hypothesis. ∎

Then we have the sequence

$$\mathcal{O}_K^\vee \hookrightarrow \mathcal{O}_L^\vee \twoheadrightarrow \mathcal{O}_L^\vee / \mathcal{O}_L.$$

Then $\mathcal{O}_L \cap \mathcal{O}_K^\vee \subseteq \mathcal{O}_L \cap K = \mathcal{O}_K$, so the above composition annihilates elements in $\mathcal{O}_K$. Hence we obtain an inclusion $\mathcal{O}_K^\vee / \mathcal{O}_K \to \mathcal{O}_L^\vee / \mathcal{O}_L$ is an inclusion, so $D_K | D_L$.

§12 February 27, 2015

We want another way to see the result from last lecture.

§12.1 Recap

From Wikipedia:

> A classical example of the construction of a quadratic field is to take the unique quadratic field inside the cyclotomic field generated by a primitive p-th root of unity, with p an odd prime. (The uniqueness is a consequence of Galois theory, there being a unique subgroup of index 2 in the Galois group over $\mathbb{Q}$). As explained at Gaussian period, the discriminant of the quadratic field is p for $p = 4n + 1$ and p for $p = 4n + 3$. This can also be predicted from enough ramification theory. In fact p is the only prime that ramifies in the cyclotomic field, so that p is the only prime that can divide the quadratic field discriminant. That rules out the "other" discriminants $-4p$ and $4p$ in the respective cases.

We saw that as $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\zeta_p)$, we have

$$d = \begin{cases} p & p \equiv 1 \pmod 4 \\ -p & p \equiv 3 \pmod 4. \end{cases}$$

§12.2 Legendre Symbol and the unique quadratic subfield

Let $\sqrt{d}$ be the unique squarefree element so that $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\zeta_p)$.

Define the **Legendre symbol** as follows. Consider a map

$$\operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^* \twoheadrightarrow \{\pm 1\}.$$

Thus $\pm\sqrt{d}$ is fixed by any σ in the Galois group. So we define $\left(\frac{\sigma}{p}\right)$ by

$$\left(\frac{\sigma}{p}\right) = \begin{cases} 1 & \sigma(\sqrt{d}) = \sqrt{d} \\ -1 & \sigma(\sqrt{d}) = -\sqrt{d}. \end{cases}$$

This is an (abelian) **character** in the sense that it's a map from a group to $\mathbb{C}^*$.

Let G denote the Galois group and consider

$$g \stackrel{\text{def}}{=} \sum_{\sigma \in G} \left(\frac{\sigma}{p}\right) \sigma(\zeta_p) \in \mathcal{O}_{\mathbb{Q}(\zeta_p)}.$$

Observe that for any $\tau \in G$ we get

$$\tau(g) = \sum_{\sigma \in G} \left(\frac{\sigma}{p}\right) \tau\sigma(\zeta_p) = \left(\sum_{\sigma \in G} \left(\frac{\sigma\tau}{p}\right) (\tau\sigma)(\zeta_p) \right) \left(\frac{\tau}{p}\right) = \left(\frac{\tau}{p}\right) g.$$

Now, write

$$G \cong (\mathbb{Z}/p\mathbb{Z})^* = \{1, \dots, p-1\}.$$

Then

$$g^2 = \sum_{a,b \in (\mathbb{Z}/p\mathbb{Z})^*} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \zeta_p^{a+b}.$$

Letting $t = ba$, this becomes

$$\begin{aligned} g^2 &= \sum_{a,t \in (\mathbb{Z}/p\mathbb{Z})^*} \left(\frac{a^2 t}{p}\right) (\zeta_p^a)^{1+t} \\ &= \sum_{a,t \in (\mathbb{Z}/p\mathbb{Z})^*} \left(\frac{t}{p}\right) (\zeta_p^a)^{1+t} \\ &= \sum_t \left(\frac{t}{p}\right) \sum_a (\zeta_p^a)^{1+t} \end{aligned}$$

Unless $t = -1$, the $1 + t$ does nothing and the sum is just equals the trace -1. So we obtain

$$\begin{aligned} &= \left(\frac{-1}{p}\right)(p-1) + \sum_{t \neq -1} \left(\frac{t}{p}\right) \cdot (-1) \\ &= p\left(\frac{-1}{p}\right) - \sum_t \left(\frac{t}{p}\right) \\ &= p\left(\frac{-1}{p}\right). \end{aligned}$$

Now we're done if we know olympiad number theory! Indeed, recall that we had

$$\left(\frac{-}{p}\right) : G \to (\mathbb{Z}/p\mathbb{Z})^* \twoheadrightarrow \{\pm 1\}.$$

So yeah whatever.

§12.3 Dedekind domains

We now move on to a new topic.

Definition 12.1. A **Dedekind domain** is a ring (commutative with 1) A such that the following three conditions hold.

(a) A is Noetherian.

(b) Any nonzero prime ideal $\mathfrak{p} \subseteq A$ is maximal. (Equivalently, "prime" and "maximal" coincide.)

(c) A is integrally closed in its field of fractions.

Point (b) is the most important one; it's very strong.

Example 12.2

$A = \mathbb{Z}$ and $A = \mathbb{C}[x]$ are Dedekind domains. (So is $A = \mathbb{C}$ or $A = \mathbb{Q}$, but that's a disappointing example. Note that $\mathbb{Q}$ is integrally closed in $\mathbb{Q}$ because lol.)

Proposition 12.3

Let K be a number field. Then $\mathcal{O}_K$ is a Dedekind domain.

Proof. Since $\mathcal{O}_K \cong \mathbb{Z}^d$ as a $\mathbb{Z}$-module, we see that there are no ascending chains.

Integral closure was done ages ago (as homework).

Hence the point is to check that nonzero prime ideals are maximal. We will use the following lemma.

Lemma 12.4

If $I \subseteq \mathcal{O}_K$ is a nonzero ideal then $\mathcal{O}_K/I$ is finite.

Proof. The point is to show that $0 \neq n = \mathrm{N}_{K/\mathbb{Q}}(\alpha) \in I$, which will imply the conclusion, since in that case we have a surjection

$$\mathbb{Z}^d/(n\mathbb{Z}^d) \cong \mathcal{O}_K/n\mathcal{O}_K \twoheadrightarrow \mathcal{O}_K/I$$

and the left-hand side has order n^d.

We use the characteristic polynomial. Let $0 \neq \alpha \in I$, and consider its characteristic polynomial

$$P_\alpha(X) = \det_{\mathbb{Z}}(X - \alpha\,|_{\mathcal{O}_K}) = x^n + c_{n-1}x^{n-1} + \cdots + c_0$$

where $0 \neq c_0 = \pm n \in \mathbb{Z}$. Since α satisfies its own characteristic polynomial, we see that $n \in \alpha\mathcal{O}_K$. But $\alpha\mathcal{O}_K \subseteq I$ since ideals absorb multiplication. Hence $n \in I$, as needed. ■

Let $0 \neq \mathfrak{p} \subseteq \mathcal{O}_K$ be prime. Then $\mathcal{O}_K/\mathfrak{p}$ is an integral domain. Since it's also finite by the lemma, it's a field (classical algebra exercise). So $\mathfrak{p}$ is maximal. □

§13 March 2, 2015

We continue Dedekind domains. Recall that a Dedekind domain is a Notherian ring integrally closed in its field of fractions with the *very special* property that every nonzero prime ideal is actually maximal.

We showed that for any number field K, $\mathcal{O}_K$ is a Dedekind domain.

§13.1 Fractional Ideals

Let A be a Dedekind domains, and K be the field of fractions. Let I and J be additive subgroups of K, and define $I \cdot J$ to be the subgroup generated by elements $\alpha\beta$, where $\alpha \in I$ and $\beta \in J$.

Remark that if I, J are $\mathcal{O}_K$ submodules then so is $I \cdot J$.

Definition 13.1. A **fractional ideal** $I \subseteq K$ is a nonzero A-submodule such that for some $0 \neq d \in A$, we have $dI \subseteq A$, *id est*, $I \subseteq d^{-1}A$.

Remark 13.2. Observe if $d' \in I$, we have

$$d' \cdot A \subseteq I \subseteq d^{-1} \cdot A.$$

Example 13.3

When $A = \mathbb{Z}$, $\frac{1}{2}\mathbb{Z}$ is the canonical example of a fractional ideal. But $\mathbb{Z}[\frac{1}{2}]$ is not a fractional ideal (no single d works).

Lemma 13.4

If I, J are fractional ideals, then so are $I + J$ and $I \cdot J$.

Proof. It's easy to check everyone is a submodule. If we pick d_1, d_2 so that $d_1 I$ and $d_2 J$ are contained in A, then $d = d_1 d_2$ is enough for both $I + J$ and $I \cdot J$. □

Remark 13.5. $I \cdot A = I$ for any A-submodule I. So A behaves like an "identity".

§13.2 Unique factorization

For $m > 0$ we put $\mathfrak{p}^{-m} \stackrel{\text{def}}{=} (\mathfrak{p}^{-1})^m$. Now we can present the main theorem on unique factorization.

Theorem 13.6 (Unique Factorization into Fractional Ideals)
Let A be a Dedekind domain and K its field of fractions.

(a) The fractional ideals of A form a group under ideal multiplication, with identity A. In particular, given a fractional ideal I there exists a fractional ideal denoted "I^{-1}" such that $I \cdot I^{-1} = A$.

(b) Every fractional ideal I can be written uniquely in the form

$$I = \prod_{\mathfrak{p}} \mathfrak{p}^{n(p)}$$

where the multiplication is an ideal product, at most finitely many $n(p)$ are nonzero (so the product is finite), and the product runs over all the nonzero prime (i.e. maximal) ideals $\mathfrak{p} \subseteq A$.

(It's not terribly obvious that what we think of $\mathfrak{p}^{-1}$ happens to be a fractional ideal; this is part of the theorem.) Needless to say, when $A = \mathbb{Z}$ we get the fundamental theorem of arithmetic on $\mathbb{Q}$.

Example 13.7
Fractional ideals of $\mathbb{Z}$ are precisely $q\mathbb{Z}$, for some nonzero $q \in \mathbb{Q}$.

A quick remark here. The most obvious analog of a prime number is the following.

Definition 13.8. An element $f \in A$ is called **irreducible** if it is not a unit, and whenever $f = gh$ for $g, h \in A$, then either g or h is a unit.

However it turns out that ideals are nicer, and in general the concept "(p) is prime" and "p is irreducible" do not coincide.

Example 13.9
Let $\mathcal{O}_K = \mathbb{Z}(\sqrt{-5})$ arise from $K = \mathbb{Q}(\sqrt{-5})$. It does not have unique factorization of *irreducibles* since

$$6 = 2 \cdot 3 = \left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right)$$

and for norm reasons, you can show that these factors are irreducible.

Now let's factor into ideals. Let

$$\mathfrak{p} = \left(1 + \sqrt{-5}, 2\right) = \left(1 - \sqrt{-5}, 2\right).$$

Also, let $\mathfrak{q}_1 = (1 + \sqrt{-5}, 3)$ and $\mathfrak{q}_2 = (1 - \sqrt{-5}, 3)$. Then the point is that the factorization reads

$$(6) = \mathfrak{p}\mathfrak{q}_1 \cdot \mathfrak{p}\mathfrak{q}_2 = \mathfrak{p}^2 \cdot \mathfrak{q}_1\mathfrak{q}_2.$$

Example 13.10

Let $\mathcal{O}_K = \mathbb{Z}(\sqrt{-17})$ arise from $K = \mathbb{Q}(\sqrt{-17})$. Let's find all factorizations of 21 into irreducible elements. Of course, we have $21 = 3 \cdot 7$. So we would like to factor 3 and 7.

We begin by factoring 3. We know $\mathcal{O}_K \cong \mathbb{Z}[x]/(x^2+17)$. Now

$$\mathcal{O}_K/3\mathcal{O}_K \cong \mathbb{Z}[x]/(3, x^2+17) \cong \mathbb{F}_3[x]/(x^2+2) \cong \mathbb{F}_3[x]/\left((x-1)(x+1)\right).$$

This already shows that (3) cannot be a prime (i.e. maximal) ideal, since otherwise our result should be a field.

Thus we have a map

$$\mathcal{O}_K \twoheadrightarrow \mathbb{F}_3[x]/\left((x-1)(x+1)\right).$$

Let $\mathfrak{q}_1$ be the pre-image $(x-1)$ in the image. You can compute $\mathfrak{q}_1 = (3, \sqrt{-17}-1)$. Similarly, $\mathfrak{q}_2 = (3, \sqrt{-17}+1)$. We have $\mathcal{O}_K/\mathfrak{q}_1 \cong \mathbb{F}_3$, so $\mathfrak{q}_1$ is maximal (prime). Similarly $\mathfrak{q}_2$ is prime. Magically, you can check explicitly that

$$\mathfrak{q}_1\mathfrak{q}_2 = (3)$$

and in fact this holds more generally, but in any case it will follow from the theorem later.

Hence we've factored (3). The factoring of (7) will be similar. We can compute

$$\mathcal{O}_K/7\mathcal{O}_K \cong \mathbb{F}_7[x]/(x^2+17) = \mathbb{F}_7[x]/\left((x-2)(x+2)\right)$$

and so the primes are $(7, \sqrt{-17} \pm 2)$.

§13.3 A Quick Note

In showing 2, 3, $1+\sqrt{5}$ and $1-\sqrt{5}$ were irreducible in $\mathbb{Z}(\sqrt{-5})$ we implicitly used the following.

Lemma 13.11

Let $\alpha \in \mathcal{O}_K$ for K a number field. If $\mathrm{N}(\alpha) = \pm 1$, then $\alpha^{-1} \in \mathcal{O}_K$.

Proof. Look at the minimal polynomial and flip it on its head.

Specifically, it is

$$x^n + c_{n-1}x^{n-1} + \cdots + c_1 x \pm 1.$$

Then α^{-1} is a root of

$$\mp x^n \left[\left(\frac{1}{x}\right)^n + c_{n-1}\left(\frac{1}{x}\right)^{n-1} + \cdots + c_1\left(\frac{1}{x}\right) \pm 1 \right]. \qquad \square$$

§14 March 4, 2015

Instructor begins by factoring 21 completely in $\mathbb{Q}(\sqrt{-17})$. Since I submitted my homework already, I have not enough patience to copy down the steps.

§14.1 Class group

Definition 14.1. Let K be a number field. Let J_K be the group of fractional ideals, and P_K the subgroup of principal fractional ideals. We can view these as groups (with respect to ideal multiplication). The **class group** is defined as

$$\mathrm{Cl}_K \stackrel{\text{def}}{=} J_K/P_K.$$

For example, when $K = \mathbb{Q}(\sqrt{-17})$ it turns out that $\mathrm{Cl}_K = \mathbb{Z}/4\mathbb{Z}$. It's a beautiful theorem that Cl_K is always finite, and we will prove this later in the course.

§14.2 Unique Factorization

Proposition 14.2

Let A be a Dedekind domain which is not a field. Then every maximal ideal $\mathfrak{m} \subseteq \mathring{A}$ has an inverse: that is, there exists a fractional ideal $\mathfrak{m}'$ such that

$$\mathfrak{m}\mathfrak{m}' = A.$$

Proof. Let K be the field of fractions of A. The claim is that

$$\mathfrak{m}' = \{x \in K \mid x\mathfrak{m} \subseteq A\}$$

works. We need to show that $\mathfrak{m}\mathfrak{m}' = A$ (we have $\mathfrak{m}\mathfrak{m}' \subseteq A$) and that $\mathfrak{m}'$ is indeed a fractional ideal.

First, we check that $\mathfrak{m}'$ is a fractional ideal. Clearly $\mathfrak{m}'$ is an A-submodule (meaning that it's closed under addition and absorbs multiplication by A). Also $A \subseteq \mathfrak{m}'$, so $\mathfrak{m}'$ is nonzero. Taking any $0 \neq d \in \mathfrak{m}$, we have $d \cdot \mathfrak{m}' \subseteq A$. Okay yeah this is all tautology.

Also,

$$\mathfrak{m} \subseteq \mathfrak{m}\mathfrak{m}' \subseteq A.$$

But $\mathfrak{m}$ was supposed to be maximal. This can only occur if $\mathfrak{m}\mathfrak{m}' = A$ or $\mathfrak{m}\mathfrak{m}' = \mathfrak{m}$. assume for contradiction we're in the latter situation.

So suppose for contradiction that $\mathfrak{m} \cdot \mathfrak{m}' = \mathfrak{m}$. We first show this the inclusion $A \subseteq \mathfrak{m}'$ is an equality.

Consider any $x \in \mathfrak{m}'$, and pick any $0 \neq d \in \mathfrak{m}$. We have $x\mathfrak{m} \subseteq \mathfrak{m}$. But then $x^2\mathfrak{m} \subseteq x\mathfrak{m}$, and in this way we obtain the chain

$$A \supseteq \mathfrak{m} \supseteq x\mathfrak{m} \supseteq x^2\mathfrak{m} \supseteq \dots$$

Hence $x^n \in d^{-1}A$ for each n.

Look at $A[x] \subseteq K$; evidently it is in $d^{-1}A$. Thus $A[x]$ is a finitely generated A-module (**here we use the fact that A is a Dedekind domain**). So x is integral over A, but since A is integrally closed and $x \in A$. Thus $\mathfrak{m}' \subseteq A$; hence $\mathfrak{m}' = A$.

We now state two lemmas.

Lemma 14.3

If $\mathfrak{p} \subseteq R$ is prime (for R any commutative ring) and $\mathfrak{a}_1 \dots \mathfrak{a}_n \subseteq \mathfrak{p}$ (for some ideals $\mathfrak{a}_i$) then some $\mathfrak{a}_i$ is actually contained in $\mathfrak{p}$.

Proof. Trivial. If not not; pick $a_i \in \mathfrak{a}_i \setminus \mathfrak{p}$ but then $\prod a_i \in \mathfrak{p}$, impossible. ■

Lemma 14.4

Let R be a Noetherian integral domain and $\mathfrak{a}$ a nonzero ideal. Then $\mathfrak{a}$ contains a product of nonzero prime ideals.

(If we drop the "nonzero on the prime ideals" condition, then this is true for any R, and vacuously so for any R. Note that R being an integral domain means (0) is prime.)

Proof. Let Φ be the set of ideals which do not contain a product of nonzero prime ideals, and assume that Φ is not empty.

Since A is Noetherian[2], Φ has a maximal element $\mathfrak{b}$.

Since $\mathfrak{b}$ is not itself prime, there exists $x, y \in A$, $x, y \notin \mathfrak{b}$ and $xy \in \mathfrak{b}$. Then $\mathfrak{b} \subsetneq \mathfrak{b} + (x), \mathfrak{b} + (y)$. By maximality, $\mathfrak{b} + (x), \mathfrak{b} + (y)$ contain products of prime ideals and hence so does

$$(\mathfrak{b} + (x))(\mathfrak{b} + (y)) \subseteq \mathfrak{b} + (xy) = \mathfrak{b}$$

which is a contradiction. ■

To get a contradiction, we will exhibit an element $b \in \mathfrak{m}'$ not in A. Pick any $0 \neq a \in \mathfrak{m}$ and consider the ideal $(a) = A \cdot a$. It contains a product of nonzero prime ideals by the latter lemma. Take a minimal decomposition of primes *viz*

$$\mathfrak{m} \supseteq A \cdot a \supseteq \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_n.$$

Since $\mathfrak{m}$ is prime (it's maximal), there is some prime $\mathfrak{p}_i$ contained inside it. **Since we're in a Dedekind domain,** $\mathfrak{m} = \mathfrak{p}_1$, as prime ideals are maximal! Let $\mathfrak{b} = \mathfrak{p}_2 \dots \mathfrak{p}_n$; by minimality of n, there exists $b \in \mathfrak{b}$ such that $b \notin a \cdot A$. Then

$$\mathfrak{m} \cdot b \subseteq \mathfrak{m} \cdot \mathfrak{b} = \mathfrak{p}_1 \dots \mathfrak{p}_n \subseteq A \cdot a$$

and thus $ba^{-1} \in \mathfrak{m}'$. But by construction, $b \notin a \cdot A \implies ba^{-1} \notin A$. This gives the required contradiction. □

[2]Zorn's Lemma is not sufficient here, because the union of a chain need not be an upper bound for it.

§15 March 6, 2015

Let A be a Dedekind domain. Last time we showed that if $\mathfrak{m} \subseteq A$ is a maximal ideal, then $\exists \mathfrak{m}' \subseteq K$ a fractional ideal such that $\mathfrak{m} \cdot \mathfrak{m}' = A$. We got down to two lemmas; I've retroactively added their proofs to the previous lecture.

Now we proceed to prove the main theorem on unique factorization for II.

§15.1 Uniqueness of factorization

Cancelling common primes, suppose that

$$\mathfrak{p}_1^{\alpha_1} \dots \mathfrak{p}_r^{\alpha_r} = \mathfrak{q}_1^{\beta_1} \dots \mathfrak{q}_s^{\beta_s}$$

where $\alpha, \beta_i > 0$ are integers and the $\mathfrak{p}_i$, $\mathfrak{q}_i$ are pairwise distinct prime ideals. We'll show $r = s = 0$. Assume not, so that

$$\mathfrak{p}_i \supseteq \mathfrak{q}_1^{\beta_1} \dots \mathfrak{q}_r^{\beta_r}.$$

But this implies that some $\mathfrak{q}_i$ is a subset of $\mathfrak{p}_1$. But since we're in a Dedekind domain, we have $\mathfrak{q}_1$ is maximal, so $\mathfrak{p}_1 = \mathfrak{q}_i$ for some i, which is impossible.

§15.2 Existence of Factorization For Ideals

First we solve the case where $\mathfrak{b} \subseteq A$ is in fact an ideal (rather than a general fractional ideal). Let Φ be the set of nonzero ideals which are not such a product. Then Φ has a maximal element $\mathfrak{a} \subseteq A$ since A is Noetherian.

Let $\mathfrak{p}$ be a prime ideal containing $\mathfrak{a}$. By the proposition, there is an inverse ideal $\mathfrak{p}'$ such that $\mathfrak{p}\mathfrak{p}' = A$. Since $a \subseteq \mathfrak{p}$, we have

$$\mathfrak{a} \supseteq \mathfrak{a}\mathfrak{p}' \subseteq \mathfrak{p}\mathfrak{p}' = A.$$

Claim 15.1. $\mathfrak{a}\mathfrak{p}' \supsetneq \mathfrak{a}$.

Proof. Otherwise, for all $x \in \mathfrak{p}'$, $x\mathfrak{a} \subseteq \mathfrak{a}$. Hence $x^n\mathfrak{a} \subseteq \mathfrak{a}$ for all n, and thus x is integral over A. Since A is integrally closed, $x \in A$.

But $x \in \mathfrak{p}'$ was arbitrary. Hence $A = \mathfrak{p}'$. Multiplying both sides by $\mathfrak{p}$ gives that $\mathfrak{p} = \mathfrak{p}\mathfrak{p}' = A$. □

By maximality of $\mathfrak{a} \in \Phi$, it follows that $\mathfrak{a}\mathfrak{p}'$ factors as a product of prime ideals $\prod \mathfrak{q}$. Thus $\mathfrak{a} = \mathfrak{p} \prod_{\mathfrak{q}}$, contradiction.

§15.3 Complete Existence

First, we wish to reduce to the case where $\mathfrak{b}$ is in fact an ideal. Let $\mathfrak{b} \in K$ be a fractional ideal, so $d\mathfrak{b} \subseteq A$ for $0 \neq d \in A$. Thus

$$\mathfrak{b} = (d\mathfrak{b})(d^{-1}A).$$

Observe

$$(d) = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})}$$

and hence

$$(d) \cdot \prod_{\mathfrak{p}} \mathfrak{p}^{-n(\mathfrak{p})} = A$$

so $d^{-1}A = (d)^{-1} = \prod_{pp} \mathfrak{p}^{-n(\mathfrak{p})}$. Hence we're through.

§16 March 9, 2015

§16.1 Loose Ends on Unique Factorization

Let A be a Dedekind domain and K its field of fractions. Recall that we now have unique factorization into prime ideals.

Lemma 16.1
Let $I = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})}$ be a fractional ideal and suppose that in fact $I \subseteq A$. Then $n(\mathfrak{p}) \geq 0$ for each $\mathfrak{p}$.

This lemma is pretty intuitive; it would be really bizzare if it was false.

Proof. Assume not. We can rewrite this into

$$\mathfrak{p}_1^{\alpha_1} \dots \mathfrak{p}_s^{\alpha_s} \subseteq \mathfrak{q}_1^{\beta_1} \dots \mathfrak{q}_t^{\beta_t}$$

where $\alpha_i, \beta_i > 0$ and $s \geq 0$, $t > 0$. Then $\mathfrak{q}_1$ divides some $\mathfrak{p}_i$ which is impossible. □

Corollary 16.2
Suppose I and J are fractional ideals in K. Let $I = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})}$ and and $J = \prod_{\mathfrak{p}} \mathfrak{p}^{m(\mathfrak{p})}$. Then $I \subseteq J$ if and only if $n(\mathfrak{p}) \geq m(\mathfrak{p})$ for each $\mathfrak{p}$.

Proof. Consider $IJ^{-1} = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})-m(\mathfrak{p})}$. □

Also, we can now formalize the process we used before to factor 6 in $\mathbb{Z}[\sqrt{-5}]$ earlier.

Corollary 16.3 (Factoring Primes in $\mathcal{O}_K$)
Let p be a rational prime number, and K a number field. Suppose we're lucky enough that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$ with minimal polynomial f. For a polynomial ψ let $\overline{\psi}$ be its image in $\mathbb{Z}/p\mathbb{Z}[x]$. Suppose $\overline{f}$ factors as

$$\overline{f} = \prod_{i=1}^{r} (\overline{f}_i)^{e_i}.$$

Then $\mathfrak{p}_i = (f_i(\alpha), p)$ is prime for each i (note that this ideal doesn't depend on the pre-image f_i chosen) and we have

$$\mathcal{O}_K \supseteq (p) = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}.$$

Note that earlier, we could check the factorization worked for any particular case. The corollary guarantees us that this process will work.

Proof. First, note that the $\mathfrak{p}_i$ are prime just because

$$\mathcal{O}_K/\mathfrak{p}_i \cong (\mathbb{Z}[x]/f)/(p, f_i) \cong \mathbb{Z}_p[x]/f_i$$

is a field.

Let $I = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$. Modulo p it is equal to

$$\prod_{i=1}^{r} (f_i(\alpha))^{e_i} \equiv (f(\alpha)) \equiv 0 \pmod{p}$$

id est, I is in the kernel of the projection map

$$\mathcal{O}_K \to \mathcal{O}_K / p\mathcal{O}_K.$$

Thus $I \subseteq (p)$. Actually, we can even write

$$(p) = \prod_i \mathfrak{p}_i^{e_i'}$$

where $e_i' \le e_i$ for each i.

We want this equality to be tight. If not, then the image $p\mathcal{O}_K = \prod_i \mathfrak{p}_i^{e_i'}$ in $\mathcal{O}_K/p\mathcal{O}_K$ is not zero, which is impossible. □

Example 16.4 (Factoring p in the pth cyclotomic field)

Let $K = \mathbb{Q}(\zeta_p)$, meaning $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$. We seek the factorization of p.

First, we wish to factor the minimal polynomial of ζ_p, namely $\Phi_p(x) = x^{p-1} + \cdots + 1 = \frac{x^p-1}{x-1}$, modulo p. Observe that

$$\Phi_p(x+1) = \frac{1}{x}\left(x^p + \binom{p}{1} x^{p-1} + \cdots + \binom{p}{p-1} x + 1 - 1 \right) \equiv x^{p-1} \pmod{p}.$$

Consequently $\Phi_p = (x-1)^{p-1} \pmod{p}$.

Thus, the factorization is

$$(p) = (p, \zeta_p - 1)^{p-1}.$$

§16.2 Requested homework solutions

> In a problem like this, the solution is always part science and part art. The science part is like computing the trace or something... The art part is eyeballing an element of $\mathcal{O}_K$. Even the art part, if you know enough, has a science to it, but...
>
> – Mark Kisin

Example 16.5

Let $K = \mathbb{Q}(\sqrt{23}, \sqrt{3})$. Compute $\mathcal{O}_K$.

Proof. Observe that $\mathcal{O}_K \subseteq \frac{1}{4}\mathbb{Z}[\sqrt{23}, \sqrt{3}]$ by the lemma on linearly disjoint fields. Hence any element $x \in \mathcal{O}_K$ has the form

$$x = \frac{A + B\sqrt{3} + C\sqrt{23} + D\sqrt{69}}{4}.$$

Consider $\operatorname{Tr}_{K/L}(x)$, for the fields $L = \mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{23})$, $\mathbb{Q}(\sqrt{69})$, with associated $\mathcal{O}_L$ as $\mathbb{Z}[\sqrt{3}]$, $\mathbb{Z}[\sqrt{23}]$, $\mathbb{Z}[\frac{1}{2}(1+\sqrt{69}]$. The calculation gives

- $\frac{1}{2}(A + B\sqrt{3}) \in \mathbb{Z}[\sqrt{3}]$, so A, B are even.
- $\frac{1}{2}(A + C\sqrt{23}) \in \mathbb{Z}[\sqrt{23}]$, so A, C are even.
- $\frac{1}{2}(A + D\sqrt{69}) \in \mathbb{Z}[\frac{1}{2}(1+\sqrt{69})]$ from which we can show A and D are even.

Hence any element $x \in \mathcal{O}_K$ has the form

$$x = \frac{A' + B'\sqrt{3} + C'\sqrt{23} + D'\sqrt{69}}{4}.$$

Next, we observe that $\frac{1}{2}$, $\frac{1}{2}\sqrt{3}$, $\frac{1}{2}\sqrt{23}$, $\frac{1}{2}\sqrt{69}$ are not in $\mathcal{O}_K$ by considering their minimal polynomials and noticing that they are not monic. On the other hand, $\frac{1}{2}(\sqrt{23} - \sqrt{3})$ and $\frac{1}{2}(1+\sqrt{69})$ are. From this one can deduce that the answer is

$$\mathcal{O}_K = \left\{ \frac{1}{2}(A' + B'\sqrt{3} + C'\sqrt{23} + D'\sqrt{69}) \mid A' + D', B' + C' \in 2\mathbb{Z} \right\}. \qquad \square$$

Another solution proceeds by using the fact that $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{69})$ are linearly disjoint to get a bound

$$\mathcal{O}_K \subseteq \frac{1}{3}\left(\mathbb{Z}[\sqrt{3}, \frac{1}{2}(1+\sqrt{69})] \right)$$

where we recall that $K = \mathbb{Q}(\sqrt{3}, \sqrt{69}) \cong \mathbb{Q}(\sqrt{3}, \sqrt{23})$. Combined with the other lemma, we get bounds with factors of $\frac{1}{3}$ and $\frac{1}{4}$ which together eradicate the problem.

Example 16.6

Let $K = \mathbb{Q}(\zeta_p, \zeta_q)$ for distinct odd primes p and q. Show that $\mathcal{O}_K = \mathbb{Z}[\zeta_p, \zeta_q]$.

Proof. The hard part is to show that they are linearly disjoint; after that it's trivialized by the fact that the discriminants are $\pm p^{p-2}$ and $\pm q^{q-2}$.

We claim that

$$\mathbb{Z}[\zeta_p]/q \cdot \mathbb{Z}[\zeta_p]$$

is a finite field. Note that $\mathbb{Z}[x]/\Phi_p(x) \cong \mathcal{O}_K$ (where Φ_p is the cyclotomic polynomial) so

$$\mathcal{O}_K/q\mathcal{O}_K \cong (\mathbb{Z}/q\mathbb{Z})[x]/\overline{\Phi_p(x)}.$$

So the point is to show that $\overline{\Phi_p(x)}$ is separable. In fact, more strongly $x^p - 1$ is separable, just by taking the derivative.

Now we have to show $\Phi_q(x)$ is irreducible over $\mathbb{Z}[\zeta_p]$. We can repeat the proof with irreducibility over $\mathbb{Z}$ via Eisenstein; the argument still works because of the preceding claim. (Instead of $\mathbb{Z}/q\mathbb{Z}$ we use $\mathbb{Z}[\zeta_p]/q\mathbb{Z}[\zeta_p]$.) $\square$

§17 March 11, 2015

Midterm.

What is a class group?

§18 March 13, 2015

Today we prove that $\mathbb{C}$ is algebraically closed. This will actually get used: let K be a number field, and consider all embedding $\iota : K \hookrightarrow \mathbb{C}$. Then the image of $\mathcal{O}_K$ yields a lattice in the product.

§18.1 First proof of Fundamental Theorem of Algebra

First, a standard complex analysis proof. We need the fact that the following is true.

Theorem 18.1 (Louiville's Theorem)
If $f : \mathbb{C} \to \mathbb{C}$ is holomorphic and bounded then f is constant.

Assume that $P(z)$ is monic and nonconstant. If it is not monic, then $\frac{1}{P(z)}$ is holomorphic and bounded and hence constant.

§18.2 Second proof of Fundamental Theorem of Algebra

Observe that any polynomial over $\mathbb{R}$ of odd degree has a solution (by considering its limits to $\pm\infty$). Also, the property is true for polynomials of degree 2 by the quadratic formula.

> "If you wrote this on the exam I would give you two out of ten points." – Kisin
>
> "The rest of this is left as an exercise to the reader." – Aaron
>
> "Then I would two points to you and eight points to the reader." – Kisin

Now let $E/\mathbb{C}$ be a finite extension which is Galois over $\mathbb{R}$ and let $G = \text{Gal}(E/\mathbb{R})$ and $H \subseteq G$ a 2-Sylow subgroup.

Let $F = E^H$, and note that

$$[F : \mathbb{R}] = [G : H] \equiv 1 \pmod 2.$$

Take $\alpha \in F$ a primitive element. Then the minimal polynomial $P_\alpha(x)$ of α has degree $[F : \mathbb{R}]$ which is odd.

Evidently $P_\alpha(x)$ has a zero since it has odd degree, so $\deg P_\alpha = 1$ and therefore $F = \mathbb{R}$. Consequently $H = G$, meaning $|G|$ is a power of two.

Lemma 18.2
If p is a prime, then a group H of order p^k is **solvable**, meaning there is a sequence of extensions

$$H_1 \triangleright H_1 \triangleright \cdots \triangleright H_m = \{0\}$$

such that H_i/H_{i+1} is abelian.

Proof. Standard group theory lemma. □

Assuming the lemma, let $H_1 \subseteq H$ be the stabilizer of $\mathbb{C}$. Let $H = \mathrm{Gal}(E/\mathbb{R})$, so $[H : H_1] = 2$. Since H_1 is a 2-group, there exists a normal $H_2 \triangleleft H_1$ such that H_1/H_2 is abelian and nontrivial, so we get a map

$$\theta : H_1 \to H_1/H_2 \twoheadrightarrow \mathbb{Z}/2\mathbb{Z}.$$

Consider $F = E^{\ker\theta}$. Let $[H_1 : \ker\theta] = 2$. Since

$$H \underset{2}{\supset} H_1 \underset{2}{\supset} \ker\theta,$$

or

$$E^H \underset{2}{\subset} E^{H_1} \underset{2}{\subset} E^{\ker\theta}$$

which is

$$\mathbb{R} \underset{2}{-} \mathbb{C} \underset{2}{-} E^{\ker\theta}$$

which contradicts the fact that there are no degree two extensions of $\mathbb{C}$ (quadratic formula).

§19 March 23, 2015

We are going to start the geometry of numbers. Our main aim is to show that if K is a number field, then then its class group Cl_K is finite.

Recall that the class group is defined as the set of fractional ideals modulo the set of principal fractional ideals.

Example 19.1
If $K = \mathbb{Q}$ or more generally if $\mathcal{O}_K$ is a principal ideal domain, then the class group of K is trivial.

§19.1 Signatures and Embeddings

Look at the n embeddings of K into $\mathbb{C}$. We will number them as follows:

- $\sigma_1, \dots, \sigma_{r_1}$ are the real embeddings.
- $\sigma_{r_1+1}, \dots, \sigma_{r_1+r_2}$ are the first half of the non-real embeddings (meaning the image of these embeddings is not contained in $\mathbb{R}$), and
- $\overline{\sigma_{r_1+1}}, \dots, \overline{\sigma_{r_1+r_2}}$ are the conjugates of the nonreal embeddings.

Hence $n = r_1 + 2r_2$. The pair (r_1, r_2) is called the **signature** of K.

Observe that any map $\sigma_i : K \hookrightarrow \mathbb{C}$ extends to a map $K \otimes \mathbb{R} \hookrightarrow \mathbb{C}$. The image of this extended map must be a real vector space sitting inside $\mathbb{C}$, which forces it to be either $\mathbb{R}$ or $\mathbb{C}$, meaning we have

$$\mathcal{O}_K \hookrightarrow K \otimes_{\mathbb{Q}} \mathbb{R} \simeq \prod_{i=1}^{r_1} \mathbb{R} \times \prod_{i=r_1+1}^{r_1+r_2} \mathbb{C}.$$

This arises from

$$K \xrightarrow{\prod \sigma_i} \prod_{i=1}^{r_1} \mathbb{R} \times \prod_{i=r_1+1}^{r_1+r_2} \mathbb{C}$$

and doing a tensor product. The fact that we had an isomorphism follows for degree reasons.

§19.2 Overview

The image of $\mathcal{O}_K$ with this embedding is thus a "lattice" in

$$\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}.$$

So it looks kind of like embedding $\mathbb{Z}^n$ into $\mathbb{R}^n$. In fact, we will show $\sigma(\mathcal{O}_K)$ is "discrete".

As a result, we'll show that if $\mathfrak{a} \subseteq \mathcal{O}_K$ is an ideal, then there exists $x \in \mathfrak{a}^{-1}$ with

$$\mathrm{N}_{K/\mathbb{Q}}(x) \le c \, \mathrm{N}\,\mathfrak{a}$$

where c is a constant depending only on K. Here $\mathrm{N}(\mathfrak{a}) \stackrel{\text{def}}{=} |\mathcal{O}_K/\mathfrak{a}\mathcal{O}_K|$ as usual. That's the same as $\mathrm{N}(\mathfrak{b}) \le c$ fro $\mathfrak{b} = \mathfrak{a}(x)$. (Here $\mathfrak{b} \sim \mathfrak{a}$ in the class group, since x is a single element.)

This will imply the conclusion, there are only finitely many ideals whose norm are at most c.

§19.3 Geometry

Recall that an additive subgroup $H \subseteq \mathbb{R}^n$ is **discrete** if there exists some open subset $U \subseteq \mathbb{R}^n$ at the origin such that $U \cap h$ contains just the point $\{0\}$. (This implies such neighborhoods at all points, because H is an additive subgroup.) For example, $\mathbb{Z}^n \subseteq \mathbb{R}^n$ is discrete.

Lemma 19.2

$H \subseteq \mathbb{R}^n$ discrete if and only if for every compact set $K \subseteq \mathbb{R}^n$, the set $H \cap K$ is finite.

Proof. Suppose H is discrete. Suppose $h_1, h_2, \dots$ is a Cauchy sequence in H. Then $h_i - h_j \to 0$, and from discreteness, we in fact have h_i is eventually constant Hence $\lim h_i \in H$. Thus H is closed.

From the fact that K is compact, notice that $H \cap K$ is closed, and hence compact. But $H \cap K$ has the discrete topology on it, from which $H \cap K$ is finite.[3]

Conversely, suppose $H \cap K$ is compact. Let K denote the closed ball B_r of radius r for $r > 0$. From $H \cap K$ finite we get that $H \cap B_r = \{0\}$ for r small enough. □

Lemma 19.3

The image of

$$\mathcal{O}_K \overset{\sigma}{\hookrightarrow} \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$$

is discrete.

Proof. We want to exhibit an open ball whose intersection with the lattice above is just the point 0.

If $x \in \mathcal{O}_K$, we can consider its norm $N_{K/\mathbb{Q}}(x)$. If $x \neq 0$ then

$$0 \neq \mathrm{N}_{K/\mathbb{Q}}(x) \in \mathbb{Z}.$$

Now recall that the norm is the product of the Galois conjugates:

$$\prod_{i=1}^{r_1} \sigma_i(x) \prod_{i=r_1+1}^{r_2} \sigma_i(x)\overline{\sigma_i(x)}.$$

It is also an integer, and hence has absolute value at least 1.

Hence, if we take the box

$$B = \left\{ (z_1, \dots, z_{r_1+r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid |z_i| < \frac{1}{2} \right\}$$

then for any $\alpha \in \mathcal{O}_K$, we cannot possibly have $\sigma(\alpha) \in B$. □

[3]Trick: compact discrete sets are finite.

§20 March 25, 2015

Didn't attend class.

Definition 20.1. A subgroup $H \subseteq \mathbb{R}^n$ is **discrete** if $H \cap K$ is finite for any set K.

Example 20.2

$\mathbb{Z}^r$ is the standard example of a discrete subgroup of $\mathbb{R}^r$.

Theorem 20.3

Let H be a discrete subgroup of $\mathbb{R}^n$. Then H is generated as a $\mathbb{Z}$-module by r linearly independent vectors (here $r \le n$).

Definition 20.4. A discrete subgroup of $\mathbb{R}^n$ with rank n is called a **lattice**.

§21 March 27, 2015

Last time we had an embedding

$$\sigma : \mathcal{O}_K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \simeq K \otimes \mathbb{R}$$

and we showed that it was a lattice. We showed that it is discrete.

§21.1 Discrete Things and Lattices

Corollary 21.1

Let $H \subseteq \mathbb{R}^n$ denote a discrete subgroup. The following are equivalent.

- H is a lattice, meaning it has maximal rank.
- H spans $\mathbb{R}^n$, meaning $H \otimes \mathbb{R} \twoheadrightarrow \mathbb{R}^n$.
- H is an isomorphism $H \otimes \mathbb{R} \simeq \mathbb{R}^n$.
- $\mathbb{R}^n/H$ has finite volume.

Proof. (1) $\iff$ (2) $\iff$ (3) already happened last time.

Let's see (4). First, assume H is not a lattice. Then the $\mathbb{Z}$-rank of H is strictly less than n, so the map $H \otimes \mathbb{R} \to \mathbb{R}^n$ fails to be surjective and hence $\operatorname{vol}(\mathbb{R}^n/H) = \infty$.

Conversely, assume its a lattice. Set $H = \bigoplus_{i=1}^n \mathbb{Z} \cdot e_i$. Then, as we show in a moment,

$$\operatorname{vol}(\mathbb{R}^n/H) = |\det(e_1, \dots, e_n)|. \qquad \square$$

§21.2 Fundamental Domains

Let $H \subseteq \mathbb{R}^n$ be a lattice with basis $e = (e_1, \dots, e_n)$ be a basis. We define

$$P_e = \left\{ x \in \mathbb{R}^n \mid x = \sum_{i=1}^n \alpha_i e_i \; 0 \le \alpha_i < 1 \right\}.$$

This is called the **fundamental domain** of $H \subseteq \mathbb{R}^n$; we tautologically have an isomorphism $P_e \leftrightarrow \mathbb{R}^n/H$ as a continuous bijection. For example, if $n = 1$ this gives a bijection from $[0, 1)$ to $\mathbb{R}/\mathbb{Z} \simeq S^1$; in general $\mathbb{R}^n/H$ looks like an n-torus.

Let μ denote the Lebesgue measure (a very fancy area); we won't need any tricky stuff since all the sets we will be measuring our simple (e.g. parallelpipeds).

Lemma 21.2

The Lebesgue measaure of P_e is given by

$$\mu(P_e) = \operatorname{vol}(\mathbb{R}^n/H) = |\det(e_1, \dots, e_n)|.$$

In particular, $\mu(P_e)$ depends only on H and not on e.

Proof. The fact that $\mu(P_e) = \operatorname{vol}(\mathbb{R}^n/H)$ follows from the fact that $P_e \xrightarrow{\sim} \mathbb{R}^n/H$ in a continuous bijection. Do some stuff. Blah. $\square$

Remark 21.3. If $f = (f_1, \dots, f_n)$ is another $\mathbb{Z}$-basis of H, then $f = Ae$ where $\det A = \pm 1$. Thus the independence can also be seen from here.

§21.3 Minkowski

Define $\text{vol}(H) \stackrel{\text{def}}{=} \text{vol}(\mathbb{R}^n/H) = \mu(P_e)$.

Theorem 21.4

Let $H \subseteq \mathbb{R}^n$ be a lattice and $S \subseteq \mathbb{R}^n$ a measurable set. Assume $\mu(S) > \text{vol}(H)$. Then there exists distinct $x, y \in S$ such that $x - y \in \text{vol}(H)$.

Proof. Pigeonhole with volumes. □

Corollary 21.5

Let $H \subseteq \mathbb{R}^n$ be a lattice and $S \subseteq \mathbb{R}^n$ a symmetric measurable convex set containing 0. If either

(a) $\mu(S) > 2^n \text{vol}(H)$, or

(b) $\mu(S) \geq 2^n \text{vol}(H)$ and S is compact,

then some nonzero point of H is in S.

§22 March 30, 2015

Didn't attend class. Here's the next few results

§23 April 1, 2015

Didn't attend class.

Recall that the class group $\mathrm{Cl}(K)$ consists of the fractional ideals modulo the principal ideals.

§23.1 The Minkowski Bonud

Recall that the **norm of an (integral) ideal** $\mathfrak{a} \subseteq \mathcal{O}_K$ is defined as

$$\mathrm{N}(\alpha) \stackrel{\text{def}}{=} |\mathcal{O}_K/\mathfrak{a}|$$

which is finite, as proved earlier when we showed $\mathcal{O}_K$ was Dedekind. Observe that if $\mathfrak{a} = (x)$, then this gives $\left|\mathrm{N}_{K/\mathbb{Q}}(x)\right|$. It is completely multiplicative and thus extends as well to fractional ideals of $\mathcal{O}_K$.

Proposition 23.1 (Minkowski Bound)

Let K be a number field of degree n, with signature (r_1, r_2). Let D_K denote its discriminant. For any nonzero integral ideal $\mathfrak{a}$ of K, we have the bound

$$\left|\mathrm{N}_{K/\mathbb{Q}}(x)\right| \le \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|D_K|}\, \mathrm{N}(\mathfrak{a})$$

for some $x \in \mathfrak{a}$.

Proof. Greasy geometry. □

§23.2 Consequences of the Minkowski Bound

Corollary 23.2

Every ideal class of K (that is, an element of the class group $\mathrm{Cl}(K)$) contains an integral ideal $\mathfrak{b}$ such that

$$\mathrm{N}(\mathfrak{b}) \le \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|D_K|}.$$

Proof. Let $\mathfrak{a}'$ be an ideal class, and set $\mathfrak{a} = \mathfrak{a}^{-1}$. By scaling $\mathfrak{a}'$ appropriately we assume $\mathfrak{a}$ is integral. Take $x \in \mathfrak{a}$ as prescribed in the proposition; then set $\mathfrak{b} = x\mathfrak{a}^{-1}$. □

§23.3 Finiteness of the Class Group

Theorem 23.3 (Dirichlet)

The class group $\mathrm{Cl}(K)$ of any number field is finite.

Proof. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. If you go through the proof that $\mathcal{O}_K$ is Dedekind, you'll discover that $\mathfrak{p} \cap \mathbb{Z} = (p)$. In particular, $\mathfrak{p}$ divides (p), and moreover $\mathbb{N}(\mathfrak{p}) = p^d$ for some d.

Fixing a rational prime p, we see that there are only finitely many $\mathfrak{p}$ whose norm is a power of p; thus each prime power can only be contributed in a finite number of ways. Moreover for a general ideal $\mathfrak{a} = \prod \mathfrak{p}_i^{v_i}$ we have

$$\mathrm{N}(\mathfrak{a}) = \mathrm{N}(\mathfrak{p}_1)^{v_1} \dots \mathrm{N}(\mathfrak{p}_r)^{v_r}$$

and hence is a product of prime powers in the same way.

From all this we deduce that for any given integer M, there are at most finitely many ideals which can have norm exceeding M.

But every ideal class can be represented by an ideal of finite size according to the corollary. This completes the proof. □

§24 April 3, 2015

Last time, we proved that if K is a number field, we had $|\text{Cl}_K| < \infty$ by showing that every class has a representative with a bounded norm. We will now do an example.

§24.1 Class Group of $K = \mathbb{Q}(i)$

We have $D_K = -4$, and Minkowski's Bound tells us that every class has an integral ideal of norm at most

$$\text{N}(\mathfrak{b}) \left(\frac{4}{\pi}\right)^1 \cdot \frac{2!}{2^2} \cdot \sqrt{4} = \frac{4}{\pi} < 2.$$

Consequently, the class group is trivial, as $\text{N}(\mathfrak{b}) = 1$; any nontrivial ideal has norm exceeding 1.

§24.2 Class Group of $K = \mathbb{Q}(\sqrt{-5})$

Let $K = \mathbb{Q}(\sqrt{-5})$. The Minkowski Bound gives $\text{N}(\mathfrak{b}) < 3$, or $\text{N}(\mathfrak{b}) \le 2$. Assume $\text{N}(\mathfrak{b}) = 2$; then $\mathfrak{b}$ divides (2).

We do the standard trick

$$\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}] = \mathbb{Z}[x]/(x^2+5)$$

and hence $\mathcal{O}_K/(2) = \mathbb{F}_2[x]/(x+1)^2$. Thus in the same way as before we have

$$(2) = \mathfrak{p}^2 \quad \text{where } \mathfrak{p} = (2, 1+\sqrt{-5}).$$

Also, $\mathfrak{p}$ is nonprincipal.

I had better state the following lemma now.

Lemma 24.1

Let $\mathfrak{b}$ be an integral ideal with $\text{N}(\mathfrak{b}) = 2015$. Then $\mathfrak{b}$ divides the ideal (2015).

Proof. By definition, $2015 = |\mathcal{O}_K/\mathfrak{b}|$. Then every element of this quotient group has order dividing 2015; that is, for any $\alpha \in \mathcal{O}_K$ we have

$$2015\alpha \equiv 0 \pmod{\mathfrak{b}} \iff 2015\alpha \in \mathfrak{b} \quad \forall \alpha \in \mathcal{O}_K.$$

In other words, $\mathfrak{b}$ divides (2015). □

§24.3 Trivial Class Groups

In full detail, here is the proof that $\mathbb{Q}[\sqrt{-n}]$ has trivial class group (and hence is a PID) for $n = 11, 19, 43, 67, 163$.

Imaginary quadratic fields have signature $(0, 2)$, and all fields in question are of the form $\mathbb{Q}[\sqrt{-n}]$ for $-n \equiv 1 \pmod 4$; hence the discriminant is $-n$, and the ring of integers is just

$$\mathbb{Z}\left[\frac{1}{2}(-1+\sqrt{-n})\right] \cong \mathbb{Z}[x]/\left(x^2 + x + \frac{1}{4}(n+1)\right).$$

The Minkowski bound for these imaginary quadratic fields is

$$M \stackrel{\text{def}}{=} \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{2}{2^2}\sqrt{|-n|} = \frac{2}{\pi}\sqrt{n}$$

For each of the quadratic fields, the class group is generated by (ideal classes of) *prime ideals* with norm not exceeding this bound.

Moreover, recall that for prime ideals $\mathfrak{p}$, $\mathbb{N}(\mathfrak{p}) = p^d$ for some rational prime p, and actually $\mathfrak{p}$ divides (p).

So the algorithm for each of these is: consider the primes p at most the Minkowski bound M, and show in each case that (p) is in fact prime. The factorization of (p) is induced by the factorization of $4x^2 + n - 1$ modulo p.

- $\mathbb{Q}[\sqrt{-11}]$: here $M \approx 2.11$. Since $x^2 + x + 3 \equiv x^2 + x + 1 \pmod 2$ is irreducible, it follows that (2) is prime, irreducible, and principal; consequently the class group is trivial.
- $\mathbb{Q}[\sqrt{-19}]$: here $M \approx 2.77$. Now $x^2 + x + 5 \equiv x^2 + x + 1 \pmod 2$ is again irreducible.
- $\mathbb{Q}[\sqrt{-43}]$: here $M \approx 4.17$. Again $x^2 + x + 11 \equiv x^2 + x + 1 \pmod 2$ is irreducible and $x^2 + x + 11 \equiv x^2 + x - 1 \pmod 3$ is irreducible (no roots).
- $\mathbb{Q}[\sqrt{-67}]$: here $M \approx 5.2$. The polynomial $x^2 + x + 17$ is $x^2 + x + 1$, $x^2 + x - 1$, and $x^2 + x + 2$ mod 2, 3, 5. The former two are irreducible already; the last one again has no roots.
- $\mathbb{Q}[\sqrt{-163}]$: now $M \approx 8.12$. The polynomial $x^2 + x + 41$ is quite famous: it is prime for all values $1 \le x \le 40$, and greater than 7 for each of them, which immediately implies it has no roots for each of 2, 3, 5, 7.

§24.4 Class Group of $\mathbb{Q}(\sqrt{-17})$

Since $D_K = -68$, we compute the Minkowsi bound

$$\frac{4}{\pi}\sqrt{17} < 6.$$

We then proceed to spend five minutes discussing the difficulty of doing an arithmetic calculation. Remarks exchanged:

- Will we be allowed to bring a small calculator on the exam? – Aaron
- What does the size of the calculator have to do with anything? You could have like an Apple Watch. – Kisin
- Just use the fact that $\pi \ge 3$. – me
- Even Gaitsgory doesn't know that, how are we supposed to? – Wyatt
- You have to do this yourself! – Kisin
- This is an outrage.

Now, it suffices to factor with (2), (3), (5). The minimal polynomial of $\sqrt{-17}$ is $x^2 + 17$, so we can for example factor

$$\begin{aligned}(2) &= (2, \sqrt{-17} + 1)^2 \\ (3) &= (3, \sqrt{-17} - 1)(3, \sqrt{-17} + 1) \\ (5) &= (5)\end{aligned}$$

corresponding to the factorizations of x^2+17 modulo each of 2, 3, 5. Set $\mathfrak{p} = (2, \sqrt{-17}+1)$ and $\mathfrak{q}_1 = (3, \sqrt{-17}-1)$, $\mathfrak{q}_2 = (3, \sqrt{-17}+1)$.

Hence for any $c \in \mathrm{Cl}_K$, we have

$$c \in \left\{ [(1)], [\mathfrak{p}], [\mathfrak{q}_1], [\mathfrak{q}_2], [\mathfrak{p}]^2 \right\}$$

where $[(1)] = [\mathfrak{p}^2] = [(2)]$ are trivial. (I'm being pedantic and using $[-]$ to denote classes.) In particular, the class group has order at most 4.

Since $[\mathfrak{p}]$ has order two, and $\mathfrak{p}$ is not principal (hence $[\mathfrak{p}] \neq [(1)]$), it follows that the class group has even order, hence either 2 or 4.

Now we claim $[\mathfrak{q}_1]^2 \neq [(1)]$, meaning $\mathfrak{q}_1$ has order greater than 2. If not, $\mathfrak{q}_1^2$ is principal. We can $\mathrm{N}(\mathfrak{q}) = 3$, so this can only occur if $\mathfrak{q}_1^2 = (3)$; this would force $\mathfrak{q}_1 = \mathfrak{q}_2$.

This is impossible since

$$\mathfrak{q}_1 + \mathfrak{q}_2 = (1).$$

Thus, $\mathfrak{q}_1$ has even order greater than 2. So it has to have order 4. Hence $\mathrm{Cl}_K = \mathbb{Z}/4\mathbb{Z}$.

§24.5 A Real Quadratic Example, $K = \mathbb{Q}(\sqrt{7})$

Let $K = \mathbb{Q}(\sqrt{7})$, with signature $(2, 0)$. The discriminant is 28, and the Minkowski bound this time is

$$M = \frac{1}{2}\sqrt{28} < 3.$$

By the same calculations as usual,

$$(2) = (2, \sqrt{7}-1)^2 = \mathfrak{p}^2.$$

But in fact, in this case $\mathfrak{p}$ isn't trivial! We have

$$\mathfrak{p} = (3 - \sqrt{7}).$$

In fact, this comes from the fact that

$$2 = (3-\sqrt{7})(3+\sqrt{7}).$$

Hence the class group is trivial.

§25 April 6, 2015

§25.1 Number Fields with Bounded Discriminant

Corollary 25.1
For a number field K of degree $n \geq 2$ (that is, $K \neq \mathbb{Q}$), we have

$$|D_K| \geq \frac{\pi}{3} \cdot \left(\frac{3\pi}{4}\right)^{n-1}.$$

Proof. Take a $\mathfrak{b}$ and use $\mathrm{N}(\mathfrak{b}) \geq 1$. Hence $\sqrt{D_K} \geq \left(\frac{\pi}{4}\right)^{r_2} \cdot \frac{n^n}{n!}$. The rest is computation, with the trivial bounds $r_2 \geq 2n$ and $\frac{\pi}{4} < 1$. □

In particular,

$$\frac{n}{\log |D_K|}$$

is bounded by some constant (again some bloody calculations).

Corollary 25.2
If $K \neq \mathbb{Q}$, then $|D_K| \geq 1$.

This will be important later. In fact, we will later see that a rational prime p "ramifies" if and only if it divides $|D_K|$. So in an extension, some positive number of primes ramify but only finitely many of them do.

> "What do you do if the prime ramifies?" – Aaron
>
> "What do you mean, what do you do? ... You go to Disney World." – Kisin

Theorem 25.3
Fix a positive integer M. Then there are finitely many number fields $K \subseteq \mathbb{C}$ such that $D_K \leq M$.

Proof. We will show the result for a fixed degree n (bounded by previous corollary) and a fixed signature (r_1, r_2), (as $r_1 + 2r_2 = n$).

Let $\sigma_1, \dots, \sigma_{r_1}$ and $\sigma_{r_1+1}, \dots, \sigma_{r_1+2r_2}$ be the real and complex embeddings with the complex embeddings in conjugate pairs (as $\sigma_{r_1+k} = \overline{\sigma_{r_1+r_2+k}}$).

We now wish to use Minkowski again. We need to pick a region B suitably large, which will let us find an $x \in B \cap \sigma$"$(\mathcal{O}_K)$.

- If $r_1 > 0$ (there is a real embedding), we pick the box carved out by

$$|y_1| \leq 2^{n-1} \left(\frac{\pi}{2}\right)^{-r_2} \sqrt{M}.$$

Then set $|y_i| \le \frac{1}{2}$ for $i \ge 2$ and $|z_j| \le \frac{1}{2}$ for all j. In that case the volume of B is given by

$$\begin{aligned}\operatorname{vol}(B) &= 2^n \left(\frac{\pi}{2}\right)^{-r_2} \sqrt{M} 1^{r_1-1} \left(\frac{\pi}{4}\right)^{r_2} \\ &= 2^{n+r_2-2r_2}\sqrt{M} \\ &= 2^{n-r_2}\sqrt{M} \\ &\ge 2^{n-r_2}\sqrt{D_K} \\ &= 2^n \operatorname{vol}(\sigma(\mathcal{O}_K))\end{aligned}$$

- If $r_1 = 0$, we hack this as follows Put

$$|2\Im(z_1)| = |z_1 - \overline{z_1}| \le 2^n \left(\frac{\pi}{2}\right)^{1-r_2} \sqrt{M}.$$

and $|2\Re(z)| = |z_1 + \overline{z_1}| \le \frac{1}{2}$. Then set $|z_j| \le \frac{1}{2}$ for all $j \ge 2$.

Here, the volume is

$$\begin{aligned}\operatorname{vol}(B) &= 2^n \left(\frac{\pi}{2}\right)^{1-r_2} \frac{1}{2} \left(\frac{\pi}{4}\right)^{r_2-1} \sqrt{M} \\ &= 2^{n-1} \cdot 2^{-r_2+1}\sqrt{M} \\ &\ge 2^n \operatorname{vol}(\sigma(\mathcal{O}_K)).\end{aligned}$$

Thus in both cases there is a $0 \neq x \in \mathcal{O}_K$ for which $\sigma(x) \in B$.

We claim that $K = \mathbb{Q}(x)$ now. This will complete the proof, since then x has minimal polynomial

$$P(X) = \prod_{i=1}^{r_1+2r_2} (X - \sigma_i(x)) \in \mathbb{Z}[X].$$

Now the roots are bounded by some constant because of the construction of B. Thus the coefficients of $P(X)$ are bounded by some constant depending on r_1, r_2, d; there are thus only finitely many possible P and the claim would thus imply that there are only finitely many possible x.

Now we prove the claim. Note that

$$1 \le \left| \prod_{i=1}^{r_1+2r_2} \sigma_i(x) \right| = \left|\mathrm{N}_{K/Q}(x)\right|$$

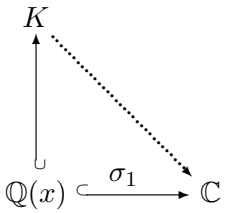
and the narrow-ness of the box implies that $|\sigma_i(x)| < 1$ for each $i = 2, \dots, r_1 + r_2$; thus $\sigma_1(x) > 1$.

- In the first case, where the embedding $\sigma_1(x) \in \mathbb{R}$, we thus have $\sigma_1(x) \neq \sigma_i(x)$ for $i \ge 2$.
- In the second case $r_1 = 0$, we still have $\sigma_1(x) \neq \sigma_i(x)$, except possibly $i = r_2 + 1$, *id est* $\sigma_i = \overline{\sigma_1}$ But

$$\Re(\sigma_1(x)) < 1 \implies |\sigma_1(x)| > 1$$

hence $\sigma_1(x) \notin \mathbb{R}$ and this is not an issue.

Hence in either case $\sigma_1(x) \neq \sigma_i(x)$.



That's enough to imply that there is no intermediate field, as desired. Meaning, $[K : \mathbb{Q}(x)] = 1$, and we're done. □

§26 April 8, 2015

Didn't attend class.

§27 April 10, 2015

Today we finish the proof of the unit theorem, which states the following.

§27.1 Review of Unit Theorem

Theorem 27.1 (Dirichlet's Unit Theorem)
Let K be a number field of signature (r_1, r_2).

> "I can see at least one person is taking the unit theorem appropriately seriously by wearing a tie. . .
>
> Well, I guess I'm not wearing a tie." – Mark Kisin

Last time, we defined a map

$$L : K^* \mapsto \mathbb{R}^{r_1+r_2}$$

by

$$x \mapsto (\log|\sigma_1(x)|, \log|\sigma_{r_1+r_2}(x)|).$$

We restrict it to $\mathcal{O}_K^*$. We proved last time through the box

$$L\text{“}(\mathcal{O}_K^*) \subseteq \left\{ (w_i) \mid \sum_{i=1}^{r_1} w_i + \sum_{i=r_1+1}^{r_1+r_2} 2w_i = 0 \right\}$$

that $\mathcal{O}_K^*$ has rank at most $r_1 + r_2 - 1$.

§27.2 Quadratic Example

We prove the unit theorem in the special case of $K = \mathbb{Q}(\sqrt{d})$ with signature $(2, 0)$ for concretenesses (say $d > 0$). It suffices to exhibit a unit of infinite order, since the above result tells us we have at most $2 + 0 - 1 = 1$ such generators.

We consider the embedding $\sigma : \mathcal{O}_K \hookrightarrow \mathbb{R}^2$. Fix $\alpha \in \mathbb{R}^+$, and consider the box

$$B_\lambda = \left\{ (x_1, x_2) \in \mathbb{R}^2 \mid |x_1| \le \lambda, |x_2| \le \frac{\alpha}{\lambda} \right\}.$$

Clearly its volume is α, so for any point in the box $\mathrm{N}_{K/\mathbb{Q}}(x\lambda) \le \alpha$. Now pick α so that the Minkowski bound works. Then there exists $x_\lambda \in \sigma\text{“}\mathcal{O}_K \cap B_\lambda$.

Now by increasing λ drastically, we can get a $B_{\lambda'}$ which omits x_λ, and hence has some nontrivial point $x_{\lambda'} \neq x_\lambda$. (Note that x_λ is not on the x-axis because the y-coordinate is σ_2(something).) So we can get an *infinite* sequence of distinct points. (Rephrasing: $a - b\sqrt{d}$ can be made arbitrarily close to zero).

But the norm is an integer bounded by α, so there are finitely many values. Also, we've seen that there are finitely many ideal for a given norm. Since we can get an infinite sequence, we realize that there exists $\lambda' > \lambda > 0$ such that $x_{\lambda'} \neq \pm x_\lambda$ but the ideals (x_λ) and $(x_{\lambda'})$ are equal.

Remark 27.2. Note that here we've done a lot of abuse by identifying a point in $\sigma\text{“}\mathcal{O}_K \subset \mathbb{R}^2$ with the original guy in $\mathcal{O}_K$.

Then $u = x_\lambda x_\lambda^{-1} \in \mathcal{O}_K$, and $u \in \mathcal{O}_K^*$. Moreover, $u \neq \pm 1$. Now since $K \subseteq \mathbb{R}$, it follows that u has infinite order (any non-infinite unit is a root of unity).

Example 27.3
If $K = \mathbb{Q}(\sqrt{3})$, then $\mathcal{O}_K^* \simeq (2 + \sqrt{3})^{\mathbb{Z}}$.

§27.3 General Case

We will continue to abuse notation by identifying an integer in $\mathcal{O}_K$ with its image under σ.

It is enough to show that for any $f : W \to \mathbb{R}$ a nonzero linear form, there exists a unit u such that

$$f(L(u)) \neq 0.$$

This will give a surjection

$$L(\mathcal{O}_K^*) \otimes \mathbb{R} \twoheadrightarrow W$$

and hence implies that

$$\operatorname{rank} L(\mathcal{O}_K^*) \geq \dim W = r_1 + r_2 - 1$$

which is what we want. This approach has the advantage that we only need to find a single unit, rather than juggle around with multiple units and try to show linearly independence.

Let $\alpha \in \mathbb{R}^+$ and $r = r_1 + r_2 - 1$. If $\lambda = (\lambda_1, \dots, \lambda_r) \in (\mathbb{R}^+)^r$ we can choose $\lambda_{r+1} \in \mathbb{R}^+$ such that

$$\prod_{i=1}^{r_1} \lambda_i \prod_{i=r_1+1}^{r_1+r_2} \lambda_i^2 = \alpha$$

(the last term of the product). Next let us take a compact symmetric box as before:

$$B = \left\{ (y_1, \dots, y_{r_1}, z_1, \dots, z_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid |y_i| \leq \lambda_i, |z_i| \leq \lambda_{i+r_1} \right\}.$$

One can compute its volume, which will only depend on α by contrivation:

$$\operatorname{vol}(B) = \prod_{i=1}^{r_1} 2\lambda_i \cdot \prod_{i=r_1+1}^{r_1+r_2} \pi\lambda_i^2 = 2^{r_1}\pi^{r_2}\alpha.$$

So if we choose an α so Minkowski works, and we can thus exhibit a $0 \neq x_\lambda \in B \cap \sigma\text{“}(\mathcal{O}_K)$. By construction, $|\sigma_i(x_\lambda)| \leq \lambda_i$ for all i. Thus

$$1 \leq \left|\mathrm{N}_{K/\mathbb{Q}}(x_\lambda)\right| \leq \prod_i |\sigma_i(x_\lambda)| \leq \alpha.$$

From this we deduce that

$$|\sigma_i(x_\lambda)| \geq \lambda_i/\alpha$$

for every i. Thus we have

$$\frac{\sigma_i}{\alpha} \leq |\sigma_i(x_\lambda)| \leq \lambda_i$$

which rearranges to

$$0 \leq \log \lambda_i - \log |\sigma_i(x_\lambda)| \leq \log \alpha \quad \forall i \tag{$\dagger$}$$

OK... no we actually bring in our function f. Let $(y_1, \dots, y_{r_1+r_2}) = y \in W \subseteq \mathbb{R}^{r_1+r_2}$. By using the condition that $y_1 + \cdots + y_{r_1+r_2} = 0$, we can think of f as a function

$$f(y) = \sum_{i=1}^{r_1+r_2-1} c_i y_i \quad c_i \in \mathbb{R}.$$

Now weight ($\dagger$) by $|c_i|$ and summing, we obtain

$$0 \leq \sum_{i=1}^{r_1+r_2} |c_i \log \lambda_i - c_i \log |\sigma_i(x_\lambda)|| \leq \sum_{i=1}^{r_1+r_2} |c_i| \log \alpha.$$

By applying the triangle inequality, we actually can strengthen the lower bound of zero to

$$\left| \sum_i c_i \log |\sigma_i(x_\lambda)| - c_i \log \lambda_i \right| = \left| f(L(x)) - \sum_i c_i \log \lambda_i \right|.$$

Now, choose $\beta > (\sum |c_i|) \log \alpha$, and choose $\lambda_h = (\lambda_{1,h}, \dots, \lambda_{r,h})$ such that

$$\sum_{i=1}^{r} c_i \log \lambda_{i,h} = 2\beta h$$

which implies

$$|f(L(x_{\lambda_h})) - 2\beta h| < \beta.$$

Then

$$(2h-1)\beta < f(L(x_{\lambda_h})) < (2h+1)\beta$$

and hence the $f(L(x_{\lambda_h}))$ are distinct as $h = 1, 2, \dots$.

§28 April 22, 2015

§28.1 Review of finite fields

Let p be a rational prime, and set $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Fix an algebraic closure $\overline{\mathbb{F}_p}$ of $\mathbb{F}_p$. For $q = p^r$ we set

$$\mathbb{F}_q = \left\{ x \in \overline{\mathbb{F}_p} \mid x^q = x \right\}.$$

Proposition 28.1

We have

(1) $\mathbb{F}_q$ is a subfield of $\overline{\mathbb{F}_p}$

(2) If $q' = p^{r'}$ then $\mathbb{F}_q \subseteq \mathbb{F}_{q'}$ if and only if $r \le r'$.

(3) $\bigcup_{r \ge 1} \mathbb{F}_q = \overline{\mathbb{F}_p}$.

(4) $\operatorname{Gal}(\mathbb{F}_q/\mathbb{F}_p) = \langle x \mapsto x^p \rangle \simeq \mathbb{Z}/r\mathbb{Z}$.

(5) If $F \subseteq \overline{\mathbb{F}_p}$ is a subfield with $[F : \mathbb{F}_p] < \infty$ then $F = \mathbb{F}_q$, where $q = |F|$.

Remark 28.2. For (5) there are infinite proper subfields of $\overline{\mathbb{F}_p}$. Actually we have an inverse limit

$$\operatorname{Gal}(\overline{F_p}/F_p) \simeq \varprojlim_r \mathbb{Z}/r\mathbb{Z}.$$

Corollary 28.3

We have

- $\mathbb{F}_q^*$ is cyclic of order $q-1$.
- $\mathbb{F}_q = \mathbb{F}_p[\zeta_{q-1}]$, where ζ_{q-1} is a $(q-1)$th root of unity.
- $\mathbb{F}_q \xrightarrow{\text{Tr}} \mathbb{F}_p$ is surjective.

Actually,

$$\operatorname{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x) = \sum_{i=1}^{r-1} x^{p^i}$$

is a polynomial of degree p^{r-1}.

§28.2 Lemma on Total Ramification

Theorem 28.4

Let L/K be a Galois extension of number fields, and let $\mathfrak{p} \subseteq \mathcal{O}_K$ be prime. Then

$$\mathfrak{p} \cdot \mathcal{O}_L = (\mathfrak{q}_1 \dots \mathfrak{q}_m)^e$$

for some $e \in \mathbb{Z}$ and distinct primes $\mathfrak{q}_i$.

This is since $\operatorname{Gal}(L/K)$ permutes the prime factors.

Proposition 28.5

In the notation above, let $\mathfrak{q} = \mathfrak{q}_i$ for some i.

- $\mathcal{O}_L/\mathfrak{q}$ is a Galois extension of $\mathcal{O}_K/\mathfrak{p}$.
- There is a natural map
$$\theta : G_{\mathfrak{q}} \twoheadrightarrow \operatorname{Gal}\left((\mathcal{O}_L/\mathfrak{q})/(\mathcal{O}_K/\mathfrak{p})\right)$$
which is surjective. Here
$$G_{\mathfrak{q}} = \{\sigma \in \operatorname{Gal}(L/K) : \sigma(\mathfrak{q}) = \mathfrak{q}\}.$$
- $\ker\theta$ has order e.

Note that if $e = 1$ (which is "almost always true") then $G_{\mathfrak{q}} \simeq \operatorname{Gal}(\mathcal{O}_L/\mathfrak{q}/\mathcal{O}_K/\mathfrak{p})$ via θ.

§29 April 24, 2015

> It's a curse now that those two things are equal.... I'm never sure which one to write, so I have to write both.

Goal: we're going to use the results we obtained in order to show the existence of Frobenius elements, in order to get quadratic reciprocity.

§29.1 Frobenius Elements

Observe the corollary from last time that

Corollary 29.1

Let L/K be a Galois extension of number fields. If $\mathfrak{p} \supseteq \mathcal{O}_K$ is unramified in L and $\mathfrak{q}$ is a prime factor of $\mathfrak{p}$, then

$$\operatorname{Gal}(L/K) \supseteq G_{\mathfrak{q}} = \operatorname{Gal}\left((\mathcal{O}_L/\mathfrak{q})/(\mathcal{O}_K/\mathfrak{p})\right).$$

In any case, we know that the right-hand side is generated by the Frobenius map $\langle x \mapsto x^q \rangle$, where $q = |\mathcal{O}_K/\mathfrak{p}|$. Denote the corresponding element by $\operatorname{Frob}_{\mathfrak{q}} \in \operatorname{Gal}(L/K)$.

Note that if $\mathfrak{q}'$ is any other prime of $\mathfrak{q}$, there is a $\sigma \in \operatorname{Gal}(L/K)$ such that $\sigma\mathfrak{q} = \mathfrak{q}'$. From this it follows that

$$G_{\mathfrak{q}'} = \sigma G_{\mathfrak{q}} \sigma^{-1} \implies \operatorname{Frob}_{\mathfrak{q}'} = \sigma \operatorname{Frob}_{\mathfrak{q}} \sigma^{-1}.$$

Thus the conjugacy class depends only $\mathfrak{p}$, not on $\mathfrak{q}$. Moreover if $\operatorname{Gal}(L/K)$ is abelian then $\operatorname{Frob}_{\mathfrak{q}}$ depends only on $\mathfrak{p}$.

§29.2 Example: Cyclotomic Fields

Lemma 29.2

If $\ell \neq p$ is a rational prime, then ζ is unramified in $K = \mathbb{Q}(\zeta_p)$.

Proof 1. The discriminant of K is $\pm p^{p-2}$ which isn't divisible by ℓ. □

Proof 2. Let f be be the minimal polynomial of ζ_p. We want $f(x)$ to have distinct roots in $\overline{\mathbb{F}_\ell}$, and we do so by bashing derivatives. (Blah about separable polynomials.) □

§30 April 27, 2015

§30.1 From last time

Let's take $L = \mathbb{Q}(\zeta_\ell)$ for some rational prime ℓ. Then for any rational prime $p \neq \ell$, p is unramified in L and we have an element

$$\text{Frob}_p \in \text{Gal}(L/\mathbb{Q}) \simeq (\mathbb{Z}/\ell\mathbb{Z})^*$$

distinguished as follows: let $p = \prod_i \mathfrak{p}_i^e$. Then the Frob_p is the element which fixes $\mathcal{O}_L/\mathfrak{p}_i$.

Note that

$$\text{Frob}_p(\zeta_\ell) = \zeta_\ell^p.$$

Indeed, by hypothesis $\text{Frob}_p(\zeta_\ell) = \zeta_\ell^a$ for some $a \in (\mathbb{Z}/\ell\mathbb{Z})^*$ but modulo $\mathfrak{p}_i$ we have $\zeta_\ell^a \equiv \eta_\ell^p \pmod{p}_i$; this actually implies $\zeta_\ell^a = \zeta_\ell^p$ or $a \equiv \ell \pmod p$.

In fact, all elements of $\text{Gal}(L/\mathbb{Q})$ are of the form Frob_p. This follows from Dirichlet's Theorem: there exists a prime $\equiv a \pmod \ell$ (in fact infinitely many) for any $a \not\equiv 0 \pmod \ell$.

§30.2 Quadratic Reciprocity

Let $L = \mathbb{Q}(\zeta_\ell)$, so $\Delta_L = \pm\ell^{\ell-2}$. There is a unique quadratic subgroup of L by Galois theory, say $K = \mathbb{Q}(\sqrt{\ell^*})$. Since Δ_K must divide Δ_L, it follows that ℓ^* has to be $\pm\ell$ so that $\ell \equiv 1 \pmod 4$. (One can also do this just by considering ramifications.)

It comes in this way: let H be the unique subgroup of order two of $\text{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/\ell\mathbb{Z})^*$. Note that we can extract it as follows: there is a surjection

$$\left(\frac{\bullet}{\ell}\right) : (\mathbb{Z}/\ell\mathbb{Z})^* \twoheadrightarrow \{\pm 1\}$$

with kernel H, corresponding to the quadratic residues. The quadratic subfield is then

$$K = (\text{fixed field of } \mathbb{Q}(\zeta_\ell) \text{ under } H) = \mathbb{Q}(\sqrt{\ell^*}).$$

Lemma 30.1

Let $\text{Frob}_p \in \text{Gal}(K/\mathbb{Q})$. Then $\text{Frob}_p \in H$ if and only if p splits in K.

Proof. Let $\mathfrak{p}$ divide $\mathcal{O}_K$. Then $\text{Frob}_p \in H$ is equivalent to Frob_p fixing $\mathcal{O}_K$.

Claim 30.2. Frob_p fixes $\mathcal{O}_K$ if and only if it fixes $\mathcal{O}_K/\mathfrak{p}_1$.

Proof. One direction is immediate. For the other direction, take $\mathfrak{q}$ a prime factor of $\mathfrak{p}_1 \cdot \mathcal{O}_L$. Blah. ■

□

Theorem 30.3 (Quadratic Reciprocity for Odd Primes)

For distinct odd primes p and ℓ we have

$$\left(\frac{p}{\ell}\right)\left(\frac{\ell}{p}\right) = (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(\ell-1)}.$$

Proof. Assume p, ℓ odd. We have

$$1 = \left(\frac{p}{\ell}\right) \iff \text{Frob}_p \in H \iff p \text{ splits in } K.$$

We have

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{1}{2}(1+\sqrt{\ell^*})\right].$$

So p splits in K exactly when $x^2 + x + \frac{1-\ell^*}{4}$ has roots mod p, which is $\left(\frac{\ell^*}{p}\right) = 1$. In summary

$$\left(\frac{p}{\ell}\right) = \left(\frac{\ell^*}{p}\right)$$

which is secretly quadratic reciprocity. □

The proof with $p = 2$ is analogous, just that dealing with $x^2 + x + \frac{1-\ell^*}{4}$ is a little weirder because it's not just $\left(\frac{\ell^*}{p}\right)$. Instead, it's whether $\frac{1-\ell^*}{4}$ is even or odd, which amounts to $\ell \equiv \pm 1 \pmod 8$ in the good case.

§31 May 1, 2015

§31.1 The $\mathfrak{p}$-adic numbers

Let $p \subseteq \mathcal{O}_K$ be a prime. If $x \in K$, we can consider the fractional ideal $x \cdot \mathcal{O}_K$, and let

$$\nu_{\mathfrak{p}}(x) = \text{exponent of } \mathfrak{p} \text{ in } x$$

if $x \neq 0$, and ∞ otherwise.

Then for any q we may set

$$|x|_{\mathfrak{p}} \stackrel{\text{def}}{=} q^{\nu_p(x)}.$$

For convenience, we may let $q = \mathbb{N}(\mathfrak{p})$. This induces an *ultrametric* on K with

$$|x+y|_{\mathfrak{p}} \le \max\left\{|x|_{\mathfrak{p}}, |y|_{\mathfrak{p}}\right\}.$$

We can thus complete it (in the topological sense) to $K_{\mathfrak{p}}$. We can think of it as the limit

$$K_{\mathfrak{p}} = \lim_{\leftarrow i} \mathcal{O}_K/\mathfrak{p}^i.$$

We can also think of it concretely as the set of Cauchy sequences in K.

Lemma 31.1

$K_{\mathfrak{p}}$ is a field.

Proof. The metric is continuous with respect to the ring operation on K, so it follows that $K_{\mathfrak{p}}$ is a ring. Thus all that remains is to get that all nonzero elements are invertible. Blah. □

Example 31.2

Letting $K = \mathbb{Q}$, $\mathfrak{p} = (p)$ we obtain the **p-adic integers** $\mathbb{Q}_p$.

Proposition 31.3

If $\mathfrak{p} \mid p \cdot \mathcal{O}_K$, then

$$K_{\mathfrak{p}}/\mathbb{Q}_p$$

is a finite extension of degree $e_p f_{\mathfrak{p}}$. Here e_p is the power of $\mathfrak{p}$ dividing $p \cdot \mathcal{O}_K$, and $f_p = [\mathcal{O}_K/\mathfrak{p} : \mathbb{F}_p]$.

(The fact that $\mathbb{Q}_p \subseteq K_{\mathfrak{p}}$ can be checked directly.)

§31.2 Classification of Norms

Definition 31.4. A **norm** $|\bullet| : K \to \mathbb{R}$ is a map with

(1) $|x| = 0 \iff x = 0$.

(2) $|xy| = |x|\,|y|$

(3) $|x+y| \le |x| + |y|$

(4) For some nonzero $x \in K$, $|x| \neq 1$. (This disallows the norm sending all nonzero elements to 1, which would induce the discrete topology.)

Two norms are **equivalent** if they induce the same topology on K.

Theorem 31.5 (Classification of Norms on Number Fields)
Any norm on K is equivalent to one of

(i) $|\bullet|_{\mathfrak{p}}$ for some prime $\mathfrak{p}$.

(ii) A map $|x|_\sigma = \|\sigma(x)\|$, where $\sigma : K \hookrightarrow \mathbb{C}$ is an embedding and $\|-\|$ is complex absolute value.

Remark 31.6. Using the Chinese Remainder Theorem, we can show that two norms of the first type are all non-equivalent. No two norms of the first and second type are equivalent, and the only time when distinct embeddings give the same topology is when they are conjugates.

§31.3 Adeles

"Now you can play the music"
(Adele starts playing)

Convention: an infinite prime $\mathfrak{p}$ of K is a norm induced by some embedding $K \hookrightarrow \mathbb{C}$. Then we denote by $K_{\mathfrak{p}}$ the completion of K; it will be *isomorphic* to either $\mathbb{R}$ or $\mathbb{C}$ (although the topology on K itself is not one of them).

§31.4 Adeles

Definition 31.7. An **adele** of K, the set of which is denoted $\mathbb{A}_K \subseteq \prod_{\mathfrak{p}} K_{\mathfrak{p}}$, (where the product runs over infinite primes as well), is defined as

$$\mathbb{A}_K \prod_{\mathfrak{p}}{}' K_{\mathfrak{p}} = \left\{ (x_{\mathfrak{p}}) \mid x_{\mathfrak{p}} \in \mathcal{O}_{K_{\mathfrak{p}}} \text{ for almost all } \mathfrak{p} \right\}.$$

(Remark that $x_{\mathfrak{p}} \in \mathcal{O}_{K_{\mathfrak{p}}} \iff |x|_{\mathfrak{p}} \leq 1$ for almost all $\mathfrak{p}$).

Here "almost all" means cofinitely many.
This is a topological ring, whose basis of neighborhoods is given by open sets

$$\prod_{\mathfrak{p}} U_{\mathfrak{p}}$$

where $U_{\mathfrak{p}} \subseteq \mathcal{O}_{K_{\mathfrak{p}}}$ and for almost all $\mathfrak{p}$, $U_{\mathfrak{p}} = \mathcal{O}_{K_{\mathfrak{p}}}$.

Definition 31.8. An **idele** is an element of $I_K \subseteq \prod_p \mathfrak{p} K_{\mathfrak{p}}^\times$ given by

$$\left\{ (\alpha_{\mathfrak{p}})_{\mathfrak{p}} \mid \alpha_{\mathfrak{p}} \in \mathcal{O}_{K_{\mathfrak{p}}}^\times \text{ for almost all } \mathfrak{p} \right\}$$

Here $K_{\mathfrak{p}}^\times$ is the units of $K_{\mathfrak{p}}$, i.e. everything not zero. We can put a topology on it, with basis given by $1 + U_{\mathfrak{p}}$, where $U_{\mathfrak{p}} \subseteq \mathcal{O}_{K_{\mathfrak{p}}}$ is open.

Remark 31.9. The topology of $K_{\mathfrak{p}}^{\times}$ is *not* the subspace topology on $K_{\mathfrak{p}}$. Assume not. Indeed, consider the sequence

$$\{p^m \mid m = 1, 2, \dots\} \to 0$$

in $\mathbb{Q}_{\mathfrak{p}}$. Then the sequence is Cauchy in $\mathbb{Q}_{\mathfrak{p}}^{\times}$. Next

$$\mathbb{Q}_p^{\times} \to \mathbb{Q}_p^{\times} \quad \text{by} \quad x \mapsto x^{-1}.$$

Thus $\{p^{-m}\}$ would be Cauchy too, which is impossible.

§31.5 Idele Class Group

Observe that $K^{\times}$ can be thought of as a subset of I_K by mapping $x \in K^{\times}$ to the constant sequence (x). We can then define the **idele class group** as

$$C_K \stackrel{\text{def}}{=} I_K / K^{\times}.$$

Moreover, we can define a group homomorphism

$$\mathrm{N} : I_K \to \mathbb{R}^+$$

by

$$(\alpha_{\mathfrak{p}})_{\mathfrak{p}} \mapsto \prod_{\mathfrak{p}} |\alpha_{\mathfrak{p}}|_{\mathfrak{p}}.$$

(Note that positive real numbers form an abelian group under multiplication.) In the real places $\mathfrak{p}$, we use the norm as the standard absolute value; for the complex places $\mathfrak{p}$ we use the square of this.

Proposition 31.10

We have $K^* \subseteq \ker(\mathrm{N})$.

Example 31.11

Let $K = \mathbb{Q}$. Enough to check that if $\mathrm{N}(x) = 1$ for $x = p$ and $x = -1$.

For $x = -1$, we have $|x|_p = 1$ for all p. For $x = p$, we have $|p|_{\infty} = p$, $|p|_q = 1$ for any $q \neq 4$, and $|p|_p = p^{-\nu_p(p)} = p^{-1}$. Multiplying, we see $\mathrm{N}(p) = 1$, which implies the conclusion.

Proposition 31.12

The subspace $K^* \subseteq I_K$ is discrete and hence closed.

Sketch of Proof. Lt $I_K^0 = \ker N$. Let $C_K^0 = I_K^0 / K^{\times}$. It's a topological group.

The fact that C_K^0 is compact is equivalent to the finiteness of the class groups and the unit theorem. Indeed, the proofs are not substantially different; in proving C_K^0 directly, one sees much the same techniques. □

Note: there is a map

$$C_K^0 \twoheadrightarrow \mathrm{Cl}_K$$

by

$$(\alpha_{\mathfrak{p}})_{\mathfrak{p}} \mapsto \prod_{\mathfrak{p}} p^{\nu_p(\alpha_p)}.$$

The compactness of C_K^0 forces Cl_K to be finite.