Math 2530: Number Theory

Uthsav Chitra

March 15, 2017

Contents

1 Sept. 7, 2016

This day's notes aren't very organized, since the professor was mostly showing cool results in algebraic number theory.

In the beginning of class we went over some logistical things. Then Professor Silverman motivated the course by talking about Pythagorean triples and then Fermat's Last Theorem. I didn't take notes on this stuff but it was interesting– basically, we talked about how you can solve for all solutions of the Pythagorean formula in the following way. First, we have

$$a^2 + b^2 = c^2 \Rightarrow a^2 = (c+b)(c-b). \tag{1}$$

Using some parity arguments, we can assume that both b and c aren't even. Thus $\gcd(b+c, b-c) = 1$, so we can write

$$\begin{aligned} c + b &= m^2, \\ c - b &= n^2 \end{aligned} \tag{2}$$

and solve for a, b, c. Now if we want to solve $a^p + b^p = c^p$, we can try the same thing. This leads us to the following rearrangement:

$$a^p = \prod_{i=0}^{n-1} (c - \zeta^i b) \tag{3}$$

where ζ is a primitive pth root of unity. But now, we have two problems. One, how do we formalize that each factor on the right is relatively prime? And how do we formalize that each factor on the right is a prime power? Of course, this won't work, but this motivates a lot of algebraic number theory.

Definition 1.1

A **number field** is a finite extension of $\mathbb{Q}$.

Definition 1.2

The **ring of integers** of a number field K is

$$R_K = \{\alpha \in K : \alpha \text{ is the root of a monic polynomial in } \mathbb{Z}[x]\} \tag{4}$$

This gives us the followng diagram.

$$\begin{tikzcd} R_K \arrow[r, hook] \arrow[d, dash] & K \arrow[d, dash] \\ \mathbb{Z} \arrow[r, hook] & \mathbb{Q} \end{tikzcd}$$

However, it is not obvious (and we need to show) that R_K is a ring. Algebraic number theory is essentially the study of R_K.

1.1 Things we'll look at

Topics and results we will look at in the semester include:

- R_K is a ring (though often not a PID or UFD).
- Every (nonzero) ideal uniquely factors as a product of prime ideals.
- The set of fractional ideals forms a group under multiplication.
- Motivated by the going-up and going-down theorems, take $p \in \mathbb{Z}$, and consider the ideal $pR_K = \zeta_1\zeta_2\cdots$ which uniquely factors into prime ideals. If $K/\mathbb{Q}$ is Galois, then $\mathrm{Gal}(K/\mathbb{Q})$ acts on the prime ideals ζ_1 and permutes them. We will look at this in more depth.

We also look at two **finiteness theorems**.

Theorem 1.3

Given a number field K, the **ideal class group** of K (really of R_K, but people incorrectly say K) is

$$H_K = \frac{\text{group of ideals in } K}{\text{group of principal ideals in } K}. \tag{5}$$

Then H_K is finite.

One famous conjecture is that there are infinitely many $d > 0$ such that $H_{\mathbb{Q}(\sqrt{d})} = (0)$, that is, $\mathbb{Q}(\sqrt{d})$ is a PID.

For the second finiteness theorem, we look at the units, rather than ideals, since studying ideals tells us nothing about the units.

Theorem 1.4

Let K be a number field. Then R_K^* is a finitely generated abelian group.

By the fundamental theorem of finitely generated abelian groups,

$$R_K^* = (\text{finite group}) \times \mathbb{Z}^r. \tag{6}$$

This leads us to the main result.

Theorem 1.5 (Dirichlet's Unit Theorem)

Define

$$r_1 = \#(\text{embeddings } K \hookrightarrow \mathbb{R}) \tag{7}$$

$$r_2 = \frac{1}{2} \cdot \#(\text{embeddings } K \hookrightarrow \mathbb{C} \text{ with } K \not\hookrightarrow \mathbb{R}). \tag{8}$$

Then, we have

$$R_K^* \cong (\text{finite cyclic group}) \times \mathbb{Z}^{r_1+r_2-1}. \tag{9}$$

The $\frac{1}{2}$ is there because we don't want to consider both an embedding of $K \hookrightarrow \mathbb{C}$ and its complex conjugate as different maps.

For example, $\mathbb{Z}^* = \{\pm 1\}$, $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$, $\mathbb{Z}[\sqrt{2}] = \pm(1+\sqrt{2})^k$.

1.2 Analytic Theory

Define the zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}. \tag{10}$$

It converges for $\Re(s) > 1$, and $\zeta(1)$ diverges. We also have, by unique factorization,

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}. \tag{11}$$

In fact, the fact that $\zeta(1)$ diverges, together with the above factorization, can be used to show that there are infinitely many primes. This fact is attributed to Euclid, though he probably didn't prove it this way.

It also can be used to show that $\sum_p \frac{1}{p}$ diverges. The rate of convergence is

$$\sum_{p<x} \frac{1}{p} \approx \log\log x \tag{12}$$

which is very, very slow.

We can also write

$$\zeta(s) = \frac{1}{s-1} + (\text{analytic function}). \tag{13}$$

This lets us use complex analysis to get information about the primes via equation 11.

Now, how can we generalize these facts to generic number fields? We need the following definition.

Definition 1.6

The **norm** of I is $NI = \#(R_K/I)$.

Then we define the zeta function over K as $\zeta_K(s) = \sum_{0 \neq I \subset R_K} \frac{1}{(NI)^s}$. We in fact have a similar factorization as before, namely

$$\zeta_K(s) = \prod_{\mathfrak{p} \subset R_K \text{ prime}} \left(1 - \frac{1}{(NP)^s}\right)^{-1}. \tag{14}$$

Similarly, we can write

$$\zeta_K(s) = \frac{c_K}{s-1} + (\text{analytic function}). \tag{15}$$

for some constant c_K. It turns out that c_K contains lots of information about K.

2 Sept. 9, 2016

We'll first finish going over the introduction. Last time we talked about factorization, but there's also **localization**. This is akin to reduction mod p or mod m.

2.1 Localization

Example 2.1

Let's try to solve $x^2+y^2 = 7z^2$ for integers x, y, z not all 0. We can also assume that $\gcd(x, y, z) = 1$ because of the 7. (write out later).

If there is a solution, then $x^2 + y^2 = 0 \pmod 7$, which implies -1 is a square mod 7. But this is not true, so there are no other solutions. More generally, we can reduce equations mod p^2, p^3, and so on, which motivates looking for p-adic solutions in $\mathbb{Z}_p$.

To find solutions in the integers, one strategy is to look for solutions in $\mathbb{Z}_p$ for all p, and then fit to a solution in $\mathbb{Z}$. This works if there is no solution for some prime p, because then the equation does not have any solutions, but can fail otherwise.

Theorem 2.2 (Legendre)

Let $a, b, c \in \mathbb{Z}$ be nonzero. Then $ax^2 + by^2 + cz^2 = 0$ has a (nontrivial) solution in $\mathbb{Z}$ iff it has a solution mod m for all m and a solution in $\mathbb{R}$.

It actually turns out that you can show there is a solution to the above equation if m is relatively prime to a, b, c. Thus you only need to check a finite number of m, not infinitely many. However, as the following example shows, this example of the local-global principle fails for cubics.

Example 2.3 (Selmer)

$3x^3 + 4x^3 + 5x^3 = 0$ has a solution mod m for all m, and solutions in $\mathbb{R}$, but no solution in $\mathbb{Z}$.

2.2 Algebraic Integers

Recall the definition of an algebraic number.

Definition 2.4

$\alpha \in \mathbb{C}$ is an **algebraic number** if any of the following hold:

- α is the root of some non-zero $f(x) \in \mathbb{Q}[x]$.
- $\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$.
- $\mathbb{Q}[\alpha]$ is a finite-dimensional $\mathbb{Q}$-vector space.

All of the above characterizations are equivalent.

The bottom characterization is the most useful because it reduces the problem to one in linear algebra.

Definition 2.5

$\alpha \in \mathbb{C}$ is an **algebraic integer** if any of the following hold: α is the root of some non-zero *monic* $f(x) \in \mathbb{Z}[x]$, We want to prove characterizations of algebraic integers that are similar to our ones for algebraic numbers.

Theorem 2.6

The following are equivalent:

(a) α is an algebraic integer.

(b) The minimal polynomial of α in $\mathbb{Z}[x]$ is monic. (This is not the same as our definition since our definition only requires *some* polynomial to be monic, not the minimal one).

(c) $\mathbb{Z}[\alpha]$ is a finite $\mathbb{Z}$-module (that is, it has a finite generating set).

(d) There is a finite $\mathbb{Z}$-module $M \subset \mathbb{C}$ satisfying $\alpha M \subset M$.

Proof. First we show that a implies b. Let $f \in \mathbb{Z}[x]$ be a monic polynomial with $f(\alpha) = 0$. Let $g(x) \in \mathbb{Z}[x]$ be the minimal polynomial of α, with the coefficients of g relatively prime. By definition, $g(x) \mid f(x)$ in $\mathbb{Q}[x]$ (since $\mathbb{Q}[x]$ is a PID, we can do the division algorithm). Thus,

$$f(x) = g(x) \cdot h(x). \tag{16}$$

We know that $f(x) \in \mathbb{Z}[x]$ and is monic; $g(x) \in \mathbb{Z}[x]$; and $h(x) \in \mathbb{Q}[x]$. We want to use that the coefficients of g are relatively prime, which motivates the following definition.

Definition 2.7

If $f \in \mathbb{Z}[x]$ is nonzero, then content(f) is the gcd of the coefficients of f.

We also have Gauss' Lemma, which is proved in the homework.

Lemma 2.8 (Gauss' Lemma)

Content is multiplicative. That is, for $f, g \in \mathbb{Z}[x]$,

$$\text{content}(fg) = \text{content}(f)\,\text{content}(g) \tag{17}$$

We want to use Gauss' lemma somehow. So choose d such that $d \cdot h(x) = H(x)$ for $H \in \mathbb{Z}[x]$. Multiplying 16 by d on both sides and plugging in, we get

$$d \cdot f(x) = g(x) \cdot H(x). \tag{18}$$

Since $f(x)$ is monic, content$(f) = 1$. Thus content$(d \cdot f) = d$. For the RHS, by Gauss' lemma we have

$$\text{content}(gH) = \text{content}(g)\,\text{content}(H) = \text{content}(H), \tag{19}$$

since content$(g) = 1$. Thus, content$(H) = d$, so this implies

$$\frac{1}{d} \cdot H(x) = h(x) \in \mathbb{Z}[x]. \tag{20}$$

Thus, $f(x) = g(x) \cdot h(x)$ with $f, g, h \in \mathbb{Z}[x]$. This tells us that

$$x^m + \ldots = (ax^n + \ldots)(bx^l + \ldots) \tag{21}$$

since f is monic. Equating coefficients, we get $1 = ab$ for intgers a, b. Thus, $a = 1$ (or $a = -1$, but then we can just multiply g by -1), so g is monic.

Next we show b implies c. Let $g(x)$ be the minimal polynomial of α in $\mathbb{Z}[x]$, and set $d = \deg g(x)$. Let $\beta \in \mathbb{Z}[\alpha]$. We claim

$$\beta = b_0 + b_1\alpha + \ldots + b_{d-1}\alpha^{d-1} \tag{22}$$

for some $b_i \in \mathbb{Z}$.

To prove this, we can write $\beta = f(\alpha)$ for some $f(x) \in \mathbb{Z}[x]$. By the division algorithm, we have

$$f(x) = g(x)q(x) + r(x) \tag{23}$$

with some $q, r \in \mathbb{Z}[x]$ with $\deg r < \deg g = d$. Note that q, r have integer coefficients because g is monic; think long division.

Plugging in α into the above equation yields

$$f(\alpha) = g(\alpha)q(\alpha) + r(\alpha) \Rightarrow \beta = r(\alpha) \tag{24}$$

since $g(\alpha) = 0$. Thus β is the root of a polynomial with degree less than $\deg g = d$, so we are done.

To show c implies d, take $M = \mathbb{Z}[\alpha]$.

Finally, we show d implies a. Let $m_1, \ldots, m_d \in M$ be generators. By assumption, $\alpha m_1, \ldots, \alpha m_d \in M$. Since the m_i are generators, we have

$$\alpha m_i = \sum_{j-1}^{d} a_{ij} m_j \tag{25}$$

for some $a_{ij} \in \mathbb{Z}$. (Note that a_{ij} depends on α as well, although we suppress this from the notation for convenience). Writing this in matrix form, we have

$$\alpha \begin{pmatrix} m_1 \\ \vdots \\ m_d \end{pmatrix} = \begin{pmatrix} a_{11} & \cdots & a_{1d} \\ \vdots & & \vdots \\ a_{d1} & \cdots & a_{dd} \end{pmatrix} \begin{pmatrix} m_1 \\ \vdots \\ m_d \end{pmatrix}. \tag{26}$$

Let A be the $d \times d$ matrix on the RHS. Rearranging the above equation yields

$$(\alpha I - A) \begin{pmatrix} m_1 \\ \vdots \\ m_d \end{pmatrix} = 0. \tag{27}$$

Since $\begin{pmatrix} m_1 \\ \vdots \\ m_d \end{pmatrix}$ is not the zero vector, $\det(\alpha I - A) = 0$. Note that $\det(xI - A)$ is a monic polynomial with coefficients in $\mathbb{Z}$. Since this polynomial has α as a root, it follows that α is an algebraic integer. □

We can now show the following important result.

Corollary 2.9

Let $\alpha, \beta \in \overline{\mathbb{Z}}$, where $\overline{\mathbb{Z}}$ is the algebraic integers. Then $\alpha + \beta, \alpha\beta \in \overline{\mathbb{Z}}$.

Proof. Let $M = \mathbb{Z}[\alpha, \beta]$. We claim that M is finitely generated. To prove this, we note that by the above theorem, $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are finitely generated. So we can write

$$\mathbb{Z}[\alpha] = \mathbb{Z} + \cdots + \mathbb{Z}\alpha^{d-1} \tag{28}$$
$$\mathbb{Z}[\beta] = \mathbb{Z} + \cdots + \mathbb{Z}\alpha^{e-1}. \tag{29}$$

It's not hard to check that M is generated by the $\alpha^i\beta^j$, for $0 \leq i \leq d$ and $0 \leq j \leq e$. Furthermore, we have

$$(\alpha + \beta)\mathbb{Z}[\alpha, \beta] \subset \mathbb{Z}[\alpha, \beta] \tag{30}$$
$$\alpha\beta\mathbb{Z}[\alpha, \beta] \subset \mathbb{Z}[\alpha, \beta]. \tag{31}$$

Thus by the lemma, $\alpha + \beta$ and $\alpha\beta$ are algebraic integers. □

The next corollary is proved in the exact same way, so we omit its proof.

Corollary 2.10

Let K be a number field. Let $R_K = \{\alpha \in K : \alpha \text{ is integral over } \mathbb{Z}\}$ be the ring of integers. Then R_K is a ring.

3 Sept. 12, 2016

3.1 Integrality

More generally, we can define integrality for any two rings.

Definition 3.1

Let $A \subset B$ be rings. Then $\beta \in B$ is **integral over** A if β is a root of a monic (nonzero) $f(x) \in A[x]$.

Essentially the same proof as before will show that the above definition is equivalent to:

- $A[\beta]$ is a finitely generated A-module.
- There is a finitely generated A-module $M \subset B$ with $\beta M \subset M$.

Definition 3.2

The **integral closure of** A **in** B is $\{\beta \in B : \beta \text{ is integral over } A\}$.

There isn't really any good notation for the integral closure. Using the same proof as last time, we have the following theorem.

Theorem 3.3

The integral closure of A in B is a ring.

This motivates the following definition.

Definition 3.4

A is **integrally closed in** B if the integral closure of A in B is itself A.

One special case is when A is an integral domain and B is its fraction field. If A is integrally closed in B, we say A is **integrally closed**.

Example 3.5

$\mathbb{Z}$ is integrally closed. To see why, let $\beta \in \mathbb{Q}$ be integal over $\mathbb{Z}$. Write $\beta = \frac{a}{b}$ with $a, b \in \mathbb{Z}, \gcd(a, b) = 1$. By definition, there exists a monic polynomial

$$f(x) = x^d + c_1x^{d-1} + \ldots + c_d \in \mathbb{Z}[x] \tag{32}$$

such that $f(\beta) = 0$. Plugging in β and clearing denominators yields

$$a^d + c_1a^{d-1}b + \ldots + c_{d-1}ab^{d-1} + c_db^d = 0. \tag{33}$$

Since every term except the first has a factor of b, it follows that $b \mid a^d$. Combining this with the assumption that $\gcd(a, b) = 1$ implies that $b = \pm 1$, so $\beta \in \mathbb{Z}$.

Example 3.6

$\mathbb{Z}[\sqrt{5}]$ is not integrally closed. Let $\beta = \frac{1+\sqrt{5}}{2} \in \mathbb{Q}(\sqrt{5})$. It's not hard to see that β is a root of $x^2 - x - 1$, so it is integral over $\mathbb{Z}[\sqrt{5}]$, but β is clearly not in $\mathbb{Z}[\sqrt{5}]$. In fact, the integral closure of $\mathbb{Z}[\sqrt{5}]$ in $\mathbb{Q}[\sqrt{5}]$ is $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$.

Proposition 3.7

Let $A \subset B \subset C$ be rings. If B is integral over A, and C is integral over B, then C is integral over A.

Proof. Let $\alpha \in C$. By definition, there exist $b_i \in B$ such that

$$\alpha^n + b_1\alpha^{n-1} + \ldots + b_n = 0. \tag{34}$$

Each b_i is integral over A, so $B' := A[b_1, \ldots, b_n]$ is a finitely generated A-module. From the above polynomial, α is integral over B', so $B'[\alpha]$ is a finitely generated B'-module. Since B' is a finitely generated A-module, it follows that $B'[\alpha]$ is a finitely generated A-module. Finally, since

$$\alpha B'[\alpha] \subset B'[\alpha], \tag{35}$$

it follows that α is integral over C. □

Proposition 3.8

Say B/A integral, and A, B are domains. Then B is a field iff A is a field.

Proof. First, assume B is a field. Let $\alpha \in A$ be nonzero. Let $\beta \in B$ satisfy $\alpha\beta = 1$. Then, by definition we have

$$\beta^d + a_1\beta^{d-1} + \ldots + a_d = 0 \tag{36}$$

for $a_i \in A$. Multiplying by α^{d-1} and using that $\alpha\beta = 1$:

$$\beta + a_1 + a_2\alpha + \ldots + a_d\alpha^{d-1} = 0. \tag{37}$$

$a_1 + a_2\alpha + \ldots + a_d\alpha^{d-1} \in A$, so it follows that $\beta \in A$.

Next, assume A is a field. Let $\beta \in B$ be nonzero. Again, we have

$$\beta^d + a_1\beta^{d-1} + \ldots + a_d = 0 \tag{38}$$

for $a_i \in A$. We can assume WLOG that $a_d \neq 0$, since if $a_d = 0$, then our polynomial would look like

$$\beta \cdot (\beta^{d-1} + \ldots + a_{d-1}) = 0. \tag{39}$$

Using that B is a domain and $\beta \neq 0$, we get $\beta^{d-1} + \ldots + a_{d-1} = 0$, and we can repeat this argument until the constant term is non-zero.

Now in equation 38, moving a_d to the RHS and dividing by a_d (which we can do since A is a field), we get

$$\beta \cdot \left(\frac{\beta^{d-1} + a_1\beta^{d-2} + \ldots + a_{d-1}}{-a_d} \right) = 1. \tag{40}$$

Thus β has an inverse, so B is a field. □

3.2 Quadratic Fields

Consider fields $K/\mathbb{Q}$, with $[K : \mathbb{Q}] = 2$. Then we can write $K = \mathbb{Q}(\sqrt{d})$, with $d \in \mathbb{Z}$. Furthermore, we can assume d is square-free; that is, we can write $d = \pm p_1 \ldots p_r$ for some distinct primes p_r. We say K is **real** if $d > 0$, and K is **imaginary** if $d < 0$.

It turns out that, for different primes p_i, the above quadratic fields K are not isomorphic. For example, $\mathbb{Q}(\sqrt{2})$ is not isomorphic to $\mathbb{Q}(\sqrt{3})$. This may seem obvious, but consider the fields $\mathbb{F}_p(\sqrt{2})$ and $\mathbb{F}_p(\sqrt{3})$. If 2, 3 are QNRs mod p, then these fields are isomorphic!

$K/\mathbb{Q}$ is Galois if $\mathrm{Gal}(K/\mathbb{Q}) = \{1, \sigma\}$, where $\sigma(a + b\sqrt{d}) = a - b\sqrt{d}$.

Proposition 3.9

$\alpha \in R_K \Rightarrow \sigma(\alpha) \in R_K$.

Proof. Apply σ to $\alpha^d + a_1\alpha^{d-1} + \ldots + a_d = 0$, where $a_i \in \mathbb{Z}$, using that σ is a field isomorphism that fixes $\mathbb{Q}$ and therefore $\mathbb{Z}$. □

If $\alpha \in R_K$ and $\alpha \in \mathbb{Q}$, then $\alpha \in \mathbb{Z}$. This is something we proved earlier. But more interestingly, suppose $\alpha \notin \mathbb{Z}$, with $\alpha = a + b\sqrt{d}$ for some $a, b \in \mathbb{Q}$. When is $\alpha \in R_K$?

By the claim, $\alpha, \sigma(\alpha) \in R_K$. Thus, $\alpha + \sigma(\alpha) \in R_K$ and $\alpha \cdot \sigma(\alpha) \in R_K$. Both of these quantities are fixed by σ, so they are in $\mathbb{Q}$ as well. Thus, $\alpha + \sigma(\alpha), \alpha \cdot \sigma(\alpha) \in R_K \cap \mathbb{Q}$, so by a previous result, they are in $\mathbb{Z}$. Writing it out, we have

$$\alpha + \sigma(\alpha) = 2a \in \mathbb{Z}, \tag{41}$$
$$\alpha \cdot \sigma(\alpha) = a^2 - db^2 \in \mathbb{Z}. \tag{42}$$

The first condition is especially useful, as either a is an integer or $\frac{1}{2}$ plus an integer. We look at each case separately.

Case 1. Assume $a \in \mathbb{Z}$. Then, $b^2 d \in \mathbb{Z}$. Since d is squarefree, we must have $b \in \mathbb{Z}$ (as if $b = \frac{e}{f}$, then this implies $f^2 \mid d$).

Case 2. Write $a = \frac{1}{2} + A$ for some $A \in \mathbb{Z}$. Then, using the second condition:

$$\begin{aligned}\left(\frac{1}{2}+A\right)^2 - db^2 \in \mathbb{Z} &\Rightarrow \frac{1}{4} + A + A^2 - b^2 d \in \mathbb{Z} \\ &\Rightarrow \frac{1}{4} - b^2 d \in \mathbb{Z} \\ &\Rightarrow b^2 d = \frac{1}{4} + B \text{ for some } B \in \mathbb{Z}\end{aligned} \tag{43}$$

Now, the above equation implies that $b = \frac{1}{2} + B'$ for some $B' \in \mathbb{Z}$. This is a necessary condition, but it might not be sufficient. So, plugging this back in to equation 43, we get:

$$\left(\frac{1}{4} + B' + B'^2\right) \cdot d = \frac{1}{4} + B \Rightarrow B - B'd - B'^2 d = \frac{d-1}{4} \tag{44}$$

Since the LHS is an integer, we must have $d \equiv 1 \pmod 4$.

Putting both cases together gives us the following theorem.

Theorem 3.10
$$R_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \equiv 2, 3 \pmod 4, \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & d \equiv 1 \pmod 4. \end{cases}.$$

3.3 Cyclotomic Fields

Another example to keep in mind is the cyclotomic fields, $K = \mathbb{Q}(\zeta)$, where ζ is a primitive nth root of unity. Consider the homomorphism from $\mathrm{Gal}(K/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$ defined by $\sigma \mapsto a(\sigma)$, where $\sigma(\zeta) = \zeta^{a(\sigma)}$. This map turns out to be an isomorphism. We will later prove this when n is prime, but we might not get to the general proof.

More relevant to our studies is the following theorem. Maybe we'll prove this later?

Theorem 3.11
$R_{\mathbb{Q}(\zeta)} = \mathbb{Z}[\zeta]$.

Note that $G(\mathbb{Q}(\zeta)/\mathbb{Q})$ is really nice since it is abelian. The following theorem (which is really hard so we won't prove it) says that, in some way, these are all the Galois extensions of $\mathbb{Q}$ with an abelian Galois group.

Theorem 3.12 (Kronecker-Weber)
Let $K/\mathbb{Q}$ be Galois with $G(K/\mathbb{Q})$ abelian. Then there exists n such that $K \subset \mathbb{Q}(\zeta_n)$, where ζ_n is a primitive nth root of unity.

In the above theorem, if you replace $\mathbb{Q}$ with $\mathbb{Q}(\sqrt{d})$ and $d < 0$, then there's an analogue of this theorem. There's no analogue so far if $d > 0$ though.

4 Sept. 14, 2016

Today we'll talk about three useful tools for studying number fields.

4.1 Norms and Traces

Let L/K be a finite extension of fields. One way to study this extension is to consider L as a finite-dimensional vector space over K and see what multiplication in L does in this viewpoint. For any $\beta \in L$, define $M_\beta : L \to L$ by $M_\beta(\alpha) = \beta\alpha$. This is a K-linear transformation of L.

Definition 4.1

The **norm** of β, denoted $N_{L/K}\beta$, is $\det(M_\beta)$. The **trace** of β, denoted $T_{L/K}\beta$, is $\mathrm{Tr}(M_\beta)$. We sometimes omit the subscript L/K when it is not needed.

Consider the polynomial $\det(xI - M_\beta)$. We have

$$\det(xI - M_\beta) = x^{[L:K]} - (T_{L/K}\beta)x^{[L:K]-1} + \ldots \pm (N_{L/K}\beta). \tag{45}$$

This gives another way to define the norm and the trace. Note that the norm and trace are independent of the choice of basis of L over K.

Here are some facts about norms and traces.

1. $T(\beta_1 + \beta_2) = T(\beta_1) + T(\beta_2)$, since the trace of a matrix is additive;
2. $T(a\beta) = a \cdot T(\beta)$ for all $a \in K$;
3. $N(\beta_1\beta_2) = (N\beta_1)(N\beta_2)$, since the determinant of a matrix is additive.

Note that $T : L \to K$, since the elements of M_β are in K. Thus, the first and second facts tell us that T is a K-linear map.

Proposition 4.2

Suppose β is algebraic and separable over K (that is, $K(\beta)/K$ is a finite extension, and the minimal polynomial of β has distinct roots). Let $\beta_1, \ldots, \beta_d$ be the roots of the minimal polynomial of β over K. [Equivalently, these are the images of β for all possible embeddings $\sigma_i : K(\beta) \hookrightarrow \overline{K}$.] Then,

$$T(\beta) = \beta_1 + \ldots + \beta_d \tag{46}$$

$$N(\beta) = \beta_1 \ldots \beta_d. \tag{47}$$

Proof. Since the minimal polynomial has d roots, $K(\beta)/K$ is degree d. Thus $1, \beta, \ldots, \beta^{d-1}$ is a K-basis for $L := K(\beta)$. Let $x^d - a_1x^{d-1} - \ldots - a_d = 0$ be the minimal polynomial of β over K.

Now consider the map $M_\beta : L \to L$, which sends $\alpha \mapsto \beta\alpha$. We have

$$M_\beta 1 = \beta \tag{48}$$

$$M_\beta \beta = \beta^2 \tag{49}$$

$$\vdots \tag{50}$$

$$M_\beta \beta^{d-1} = a_1\beta^{d-1} + \ldots + a_d. \tag{51}$$

Thus, the matrix of M_β looks like

$$\begin{pmatrix} 0 & & & & a_d \\ 1 & 0 & & & a_{d-1} \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & a_2 \\ & & & 1 & a_1 \end{pmatrix} \tag{52}$$

Looking at the matrix, we see that $T(\beta) = a_1$ and $N(\beta) = \pm a_d$. To evaluate these in terms of the β_i, note that

$$x^d - a_1 x^{d-1} - \ldots - a_d = (x - \beta_1) \cdots (x - \beta_n) \tag{53}$$

From Viete's formulas, we thus have that $a_1 = \beta_1 + \cdots + \beta_n$ and $a_d = \pm\beta_1 \cdots \beta_n$. Equating these with the norm and trace gives us the desired result. □

Now we proved our formulas for $K(\beta)/K$. But what if we have an extension L on top of $K(\beta)$? Then we have

$$T_{L/K}(\beta) = [L : K(\beta)] \cdot T_{K(\beta)/K}(\beta) \tag{54}$$

$$N_{L/K}(\beta) = (N_{K(\beta)/K}(\beta))^{[L:K(\beta)]}. \tag{55}$$

The proof of the above two formulas is easy, but if you've never seen it before you should work it out.

Proposition 4.3

Let A be an integral domain, K its fraction field. Suppose we have an extension L/K, with $\beta \in L$ and β integral over A. Then $N(\beta), T(\beta)$, both of which are in K, are integral over A. If A is integrally closed, this implies that $N(\beta), T(\beta) \in A$.

Proof. Let $\beta_1, \ldots, \beta_d$ be the roots of $F_\beta(x)$, the minimal monic polynomial of β over K. We showed that $F_\beta(x) \in A[x]$. Thus, $\beta_1, \ldots, \beta_d$ are integral over A, since they are the roots of a monic polynomial in $A[x]$, so it follows that their sum and product are integral over A as well. □

Example 4.4

Let $K = \mathbb{Q}, L = \mathbb{Q}(\sqrt{d}), \beta = a + b\sqrt{d} \in L$. To compute M_β, choose $1, \sqrt{d}$ as a basis for L over K. Then:

$$M_\beta(1) = a + b\sqrt{d} \tag{56}$$

$$M_\beta(\sqrt{d}) = bd + a\sqrt{d}. \tag{57}$$

Thus, the matrix of M_β is

$$\begin{pmatrix} a & bd \\ b & a \end{pmatrix}. \tag{58}$$

Then, $T\beta = 2a$ and $N\beta = a^2 - db^2$. Furthermore, note that there are two embeddings of $L = \mathbb{Q}(\sqrt{d})$ into $\overline{\mathbb{Q}}$: one that sends $\sqrt{d}$ to itself, and one that sends $\sqrt{d}$ to $-\sqrt{d}$. Then the trace is the some of β's conjugates, $a + b\sqrt{d}$ and $a - b\sqrt{d}$, and the norm is the product of the conjugates.

Example 4.5

Let $K = \mathbb{Q}, L = \mathbb{Q}(\zeta_m)$, where ζ_m is a primitive mth root of unity. Then

$$N_{L/K}(\zeta_m) = \prod_{k=1,(k,m)=1}^{m-1} \zeta_m^k. \tag{59}$$

This product looks hard, but note that k is relatively prime to m iff $m-k$ is relatively prime to m. If m is odd, then every term cancels and the norm is 1. If m is even and $m/2$ is relatively prime to m, then the $k = m/2$ term does not get cancelled, and you end up with $\zeta_m^{m/2} = -1$.

4.2 Discriminants

Let B/A be an extension of rings. Assume B is a free, finitely-generated A-module. (Here, free means that B has a basis over A).

Example 4.6

Consider $K/\mathbb{Q}$. Then the ring of integers, R_K, is a finitely generated $\mathbb{Z}$-module. Because R_K has no torsion (it can't be killed by any $z \in \mathbb{Z}$ since $1 \in R_K$), by the fundamental theorem of finitely generated abelian groups, R_K is a free module.

Definition 4.7

Let $\beta_1, \ldots, \beta_n \in B$. The **discriminant of $\beta_1, \ldots, \beta_n$ over A** is

$$D_{B/A}(\beta_1, \ldots, \beta_n) := \det\left(T_{B/A}(\beta_i\beta_j)\right) \tag{60}$$

where $T_{B/A}(\beta_i\beta_j)$ is (bad notation for) a matrix whose i, j-th entry is $T_{B/A}(\beta_i\beta_j)$.

This looks really weird, but here's some motivation. We have a map

$$\begin{aligned} B \times B &\to A && (61)\\ (\beta, \beta') &\mapsto T_{B/A}(\beta\beta'). && (62) \end{aligned}$$

This map is A-bilinear, so we see that the discriminant is a way of studying this bilinear map. In fact, if $B = R_K$ and $A = \mathbb{Z}$, we'll see that the above bilinear map is positive-definite and non-degenerate. This then lets you use geometry to study A and B; we can define an inner product $\langle v, w\rangle$ using this map, then the norm $\|v\| = \sqrt{\langle v, v\rangle}$, etc. In this setting, the determinant is the (signed) volume of the parallelpiped spanned by the basis elements.

4.3 Change of Variables

Proposition 4.8

Suppose $\beta_1, \ldots, \beta_n \in B$ and $\gamma_1, \ldots, \gamma_n \in B$. Suppose

$$\gamma_i = \sum_{j=1}^{n} a_{ij}\beta_j \tag{63}$$

for some $a_{ij} \in A$. Then,

$$D(\gamma) = (\det(a_{ij}))^2 D(\beta). \tag{64}$$

Proof. We have

$$\begin{aligned} T(\gamma_i\gamma_j) &= T\left(\sum_k a_{ik}\beta_k \sum_l a_{jl}\beta_l\right) \\ &= \sum_{k,l} a_{ik} T(\beta_k\beta_l) a_{jl} \end{aligned} \tag{65}$$

by the linearity of the trace map. Note the above formula's similarity to matrix multiplication. In terms of matrices (and really bad notation), we can write this as:

$$(T(\gamma_i\gamma_j)) = (a_{ij}) \cdot (T(\beta_i\beta_j)) \cdot (a_{ij})^t. \tag{66}$$

Taking the determinant of both sides, we get

$$D(\gamma) = (\det(a_{ij})) \cdot D(\beta) \cdot (\det(a_{ij}))^t = (\det(a_{ij}))^2 \cdot D(\beta), \tag{67}$$

as desired. □

5 Sept. 16, 2016

5.1 Discriminant Review

Last time we defined the norm, trace, and discriminant. Say B/A is an extension of rings, B free and finitely-generated. Let $\beta_1, \ldots, \beta_n \in B$. Then

$$D_{B/A}(\beta_1, \ldots, \beta_n) := \det(T(\beta_i\beta_j)). \tag{68}$$

We also have the following corollary to our change of basis theorem.

Corollary 5.1

Suppose $\beta_1, \ldots, \beta_n$ is a basis for B/A, and $\beta_1', \ldots, \beta_n'$ is another basis for B/A. Then,

$$D(\beta) = u^2 D(\beta') \tag{69}$$

for some unit $u \in A^*$.

Proof. By definition, we can write

$$\beta_i' = \sum a_{ij}\beta_j \tag{70}$$

$$\beta_i = \sum a_{ij}'\beta_j'. \tag{71}$$

Then, $\beta' = M\beta$, and $\beta = M'\beta'$. It follows that $MM' = I$, so $\det(M)$ is a unit. By last time,

$$D(\beta') = (\det(M))^2 \cdot D(\beta) \tag{72}$$

so the result follows. □

Definition 5.2

Assume B is a free A-module. Then the **discriminant of** B/A is the ideal

$$\mathfrak{D}_{B/A} := (D_{B/A}(\beta_1, \ldots, \beta_n)) := D_{B/A}(\beta_1, \ldots, \beta_n) \cdot A \tag{73}$$

for any basis $\beta_1, \ldots, \beta_n$.

5.2 Bases and Discriminants

Our definition is well-defined because of the corollary. For the following result, we note that we don't necessarily know that $\mathfrak{D}_{B/A} \neq 0$. We will get back to show that later.

Proposition 5.3

Assume $\mathfrak{D}_{B/A} \neq 0$. Let $\gamma_1, \ldots, \gamma_n \in B$. Then $\gamma_1, \ldots, \gamma_n$ is a basis iff $D(\gamma_1, \ldots, \gamma_n) \cdot A = \mathfrak{D}_{B/A}$.

Proof. The right direction is already complete from the previous claim.

For the left direction, suppose $D(\gamma_1, \ldots, \gamma_n) \cdot A = \mathfrak{D}_{B/A}$. Let $\beta_1, \ldots, \beta_n$ be a basis for B/A. Then, by definition,

$$\mathfrak{D}_{B/A} = D(\beta) \cdot A. \tag{74}$$

Since the β_i are a basis, we can write

$$\gamma_i = \sum_j a_{ij}\beta_j \Rightarrow D(\gamma) = (\det(a_{ij}))^2 D(\beta). \tag{75}$$

for some $a_{ij} \in A$.

Looking at the ideals generated by the LHS and RHS, we have

$$D(\gamma) \cdot A = (\det(a_{ij}))^2 D(\beta) \cdot A. \tag{76}$$

Now, $D(\gamma) \cdot A = \mathfrak{D}_{B/A}$ by assumption, and $D(\beta) \cdot A = \mathfrak{D}_{B/A}$ since β is a basis. Thus, if we **add the additional assumption that** A **is a domain**, this implies $\det(a_{ij}) \in A^*$. *(need to look at later. why does $\mathfrak{a} = r^2\mathfrak{a}$ imply that r is a unit?).* Furthermore, using that

$$(a_{ij})^{-1} = (\text{adjoint of } a_{ij}) \cdot (\det(a_{ij}))^{-1}, \tag{77}$$

we see that $(a_{ij})^{-1}$ has entries in A. Thus, we can write

$$\beta_i = \sum a'_{ij}\gamma_i \tag{78}$$

for entries a'_{ij} in $(a_{ij})^{-1}$, and tt follows that γ is a basis. □

Example 5.4

Let $d \equiv 1 \pmod 4$, $K = \mathbb{Q}(\sqrt{d})$, $R_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. Then $1, \frac{1+\sqrt{d}}{2}$ is a basis for $R_K/\mathbb{Z}$, so we have

$$\mathfrak{D}_{R_K/\mathbb{Z}} = \det\left(\begin{pmatrix} T(1) & T(\frac{1+\sqrt{d}}{2}) \\ T(\frac{1+\sqrt{d}}{2}) & T(\frac{1+d}{4} + \sqrt{d}) \end{pmatrix}\right) = \det\left(\begin{pmatrix} 2 & 1 \\ 1 & \frac{1+d}{2} \end{pmatrix}\right) = 1 + d - 1 = d. \tag{79}$$

Thus, the determinant is the ideal generated by d in $\mathbb{Z}$.

Now suppose we thought that $1, \sqrt{d}$ was a basis. Then, we can compute the discriminant as

$$D(1, \sqrt{d}) = \det\left(\begin{pmatrix} T(1) & T(\sqrt{d}) \\ T(\sqrt{d}) & T(d) \end{pmatrix}\right) = \det\left(\begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix}\right) = 4d. \tag{80}$$

Since $(4d)\mathbb{Z} \neq d\mathbb{Z}$, it follows that $1, \sqrt{d}$ is not a basis.

The following theorem talks about when the discriminant is zero and nonzero.

Theorem 5.5

Let L/K be a field extension with $n = [L : K]$. Assume L/K is separable. (One definition of separable is that there are n embeddings of L into $\overline{K}$). Let $\sigma_1, \dots, \sigma_n : L \hookrightarrow \overline{K}$ be the distinct embeddings. Let $\beta_1, \dots, \beta_n \in L$. Then,

(a) $D(\beta_1, \dots, \beta_n) = \det(\sigma_i(\beta_j))^2$,

(b) $\beta_1, \dots, \beta_n$ is a basis for L/K iff $D(\beta_1, \dots, \beta_n) \neq 0$.

Proof. For the first part, $D(\beta_1, \dots, \beta_n) = \det(T(\beta_i\beta_j))$ by definition. Then

$$\begin{aligned} D(\beta_1, \dots, \beta_n) &= \det(T(\beta_i\beta_j)) \\ &= \det(\sum_{k=1}^{n} \sigma_k(\beta_i\beta_j)), \text{ by definition of trace,} \\ &= \det(\sum_{k=1}^{n} \sigma_k(\beta_i)\sigma_k(\beta_j)) \\ &= \det((\sigma_k(\beta_i))_{i,k} \times (\sigma_k(\beta_j))_{k,j}), \text{ which... might be a bit off.} \end{aligned} \tag{81}$$

Now the above matrices are transposes, and the determinant of the product is the product of the determinants. Thus the above determinant is equal to

$$(\det(\sigma_i(\beta_j)))^2. \tag{82}$$

□

We won't prove part b now, but we'll prove something we use to prove b.

Theorem 5.6 (Independence of Characters)
Let G be a group, let K be a field, and let $\chi_1, ..., \chi_n : G \to K^*$ be distinct characters (i.e. group homomorphisms). (Note that, given any set X and maps $X \to K$, the maps form a vector space over K, since you can add functions and multiply them by scalars in K). Then, $\chi_1, ..., \chi_n$ are K-linearly independent.

This theorem is pretty odd, since if χ_i were normal functions, this would definitely not be true. Somehow being group homomorphisms, which is multiplicative, gives them some additive property.

Proof. Suppose the theorem is false, and $\chi_1, ..., \chi_n$ are linearly dependent. Taking a subset, can assume n is minimal. (Note that we clearly do not need to consider $n = 1$). Since the χ_i are linearly independent, we can find $c_1, ..., c_n \in K$ with

$$c_1\chi_1 + ... + c_n\chi_n = 0. \tag{83}$$

Note that the c_i are non-zero, as otherwise this would imply n is not minimal. So for all $g \in G$,

$$c_1\chi_1(g) + c_2\chi_2(g) + \cdots + c_n\chi_n(g) = 0. \tag{84}$$

Let $h \in G$. Then,

$$c_1\chi_1(gh) + c_2\chi_2(gh) + \cdots + c_n\chi_n(gh) = 0. \tag{85}$$

Since χ_i is a group homomorphism, this implies

$$c_1\chi_1(g)\chi_1(h) + \cdots + c_n\chi_n(g)\chi_n(h) = 0. \tag{86}$$

If we do equations 86 - $\chi_1(h) \cdot$ (equation 84), we end up with

$$\sum_{i=2}^{n} c_i\chi_i(g) \cdot (\chi_i(h) - \chi_1(h)) = 0. \tag{87}$$

Note that the $i = 1$ term drops out. But now, we can write

$$\sum_{i=2}^{n} c_i(\chi_i(h) - \chi_1(h))\chi_i = 0 \tag{88}$$

as a linear combination of the functions χ_i. If $\chi_i(h) - \chi_1(h) \neq 0$ for any i, then we reached a contradiction, since we assumed n is minimal (and therefore that $\chi_2, ..., \chi_n$ are linearly independent). Thus, we must have $\chi_i(h) = \chi_1(h)$ for all $i = 1, ..., n$. But now we note that our choice of h was arbitrary. Thus, $\chi_i = \chi_1$ for all i. But since our characters are distinct, this is not possible. □

On Monday, we will finish the proof of part b.

6 Sept. 19, 2016

6.1 Discriminants

We recall the theorem we were trying to prove last time.

Theorem 6.1

Say L/K is separable, $\sigma_1, \ldots, \sigma_n : L \hookrightarrow \overline{K}$ are the distinct embeddings. Let $\beta_1, \ldots, \beta_n \in L$. Then

(a) $D(\beta_1, \ldots, \beta_n) = (\det(\sigma_i(\beta_j)))^2$.

(b) $D(\beta_1, \ldots, \beta_n) \neq 0 \Leftrightarrow \beta_1, \ldots, \beta_n$ is a basis for L/K.

Proof. We prove b now. Assume $\beta_1, \ldots, \beta_n$ is a basis. Suppose for the sake of contradiction that $D(\beta_1, \ldots, \beta_n) = 0$. By part a

$$\det(\sigma_i(\beta_j)) = 0. \tag{89}$$

Then, the columns are linearly dependent, so there exist $a_1, \ldots, a_n \in \overline{K}$ with

$$\sum_{i=1}^{n} a_i \sigma_i(\beta_j) = 0 \tag{90}$$

for all j. Now let β be an arbitrary element of L. Then we can write

$$\beta = \sum_k c_k \beta_k. \tag{91}$$

We have

$$\begin{aligned}
\sum_i a_i \sigma_i(\beta) &= \sum_i a_i \sigma_i \left(\sum_k c_k \beta_k \right) \\
&= \sum_i \sum_k a_i c_k \sigma_i(\beta_k) \\
&= \sum_k \sum_i a_i c_k \sigma_i(\beta_k) \\
&= \sum_k c_k \left(\sum_i a_i \sigma_i(\beta_k) \right) \\
&= \sum_k c_k \cdot 0, \text{ by equation 90} \\
&= 0.
\end{aligned} \tag{92}$$

Thus, $\sum_i a_i \sigma_i : L \to \overline{K}$ is the 0 function. Now, we note that if we restrict the σ_i to L^*, then we have

$$\sigma_i : L^* \hookrightarrow \overline{K}^* \tag{93}$$

so the σ_i are characters. Furthermore, they are distinct since each σ_i was a distinct embedding. Thus, by independence of characters, we have a contradiction.

The other direction of b is simpler, so we can work this out on our own. □

Proposition 6.2

Let L/K separable, $n = [L : K]$, and $\beta \in L$. Let

$$F_\beta(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in K[x] \tag{94}$$

be the minimal polynomial of β over K. (So $L = K(\beta)$). Then

$$D(1, \beta, ..., \beta^{n-1}) = (-1)^{\text{something}} N_{L/K}(F'_\beta(\beta)). \tag{95}$$

(We'll figure out the exponent of (-1) in the proof).

Proof. Write $F_\beta(x) = \prod_i (x - \beta_i)$, for some $\beta_i \in \overline{K}$. Then

$$D(1, \beta, ..., \beta^{n-1}) = (\det(\sigma_i(\beta^j))^2 = (\det(\beta_i^j))^2. \tag{96}$$

The RHS looks like a Vandermonde matrix!

$$(\beta_i^j) = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \beta_1 & \beta_2 & \cdots & \beta_2 \\ \vdots & \vdots & \ddots & \vdots \\ \beta_1^{n-1} & \beta_2^{n-1} & \cdots & \beta_n^{n-1} \end{pmatrix}. \tag{97}$$

Thus, we have

$$\begin{aligned} D(1, \beta, ..., \beta^{n-1}) &= \prod_{i<j} (\beta_i - \beta_j)^2 \\ &= (-1)^{\text{ number of } i,j \text{ with } i<j} \prod_{i \neq j} (\beta_i - \beta_j). \end{aligned} \tag{98}$$

We can compute the exponent of (-1) as $\binom{n}{2}$. Expanding the rest of the RHS above, we get

$$\begin{aligned} \prod_{i \neq j} (\beta_i - \beta_j) &= \prod_{i=1}^n \left(\prod_{\substack{j=1 \\ j \neq i}}^n (\beta_i - \beta_j) \right) \\ &= \prod_{i=1}^n F'_\beta(\beta_i). \end{aligned} \tag{99}$$

To see how we went from the top equation to the bottom one, note that

$$F_\beta(x) = \prod_{k=1}^n (x - \beta_i), \tag{100}$$

which implies

$$F'_\beta(x) = \sum_{l=1}^n \prod_{k=1, k \neq l}^n (x - \beta_k). \tag{101}$$

Plugging in $x = \beta_i$, every addend in the above sum with a $x - \beta_i$ term will go to 0. There is only one addend without such a term, namely when $l = i$. Thus,

$$F'_\beta(\beta_i) = \prod_{k=1, k \neq i}^n (\beta_i - \beta_k). \tag{102}$$

Now going back to equation 99, we have

$$\begin{aligned}\prod_{i\neq j}(\beta_i-\beta_j) &= \prod_{i=1}^{n} F'_\beta(\beta_i)\\ &= \prod F'_\beta(\sigma_i(\beta))\\ &= \prod \sigma_i(F'_\beta(\beta))\\ &= N(F'_\beta(\beta))\end{aligned} \tag{103}$$

as desired. □

Example 6.3

β is a root of x^n+a, where $a\in K$ and x^n+a is irreducible in $K[x]$. Now,

$$\begin{aligned}D(1,\beta,\ldots,\beta^{n-1}) &= (-1)^{\binom{n}{2}}N_{K(\beta)/K}(n\beta^{n-1})\\ &= (-1)^{\text{something}}n^n(N_{K(\beta)/K}(\beta))^{n-1}.\end{aligned} \tag{104}$$

Using Viete's formulas, $N(\beta)=(-1)^{\text{something else}}\cdot a$. Thus, the discriminant is n^na^{n-1} with some (-1) factor in the beginning.

Example 6.4

Let β be a root of x^3+ax+b. Then $D(1,\beta,\beta^2)=4a^3+27b^2$. Probably with a (-1) factor in the beginning.

6.2 Cyclotomic Fields

Let p be prime. We want to compute the ring of integers of $\mathbb{Q}(\zeta)$, where $\zeta=\zeta_p=e^{2\pi i/p}$. The answer ends up being $R_{\mathbb{Q}\beta}=\mathbb{Z}[\zeta]$.

Our first task is to find the minimal polynomial of ζ in $\mathbb{Q}$. Let $f(x)=x^{p-1}+x^{p-2}\cdots+1$.

Proposition 6.5

f is irreducible.

Proof. Consider $f(x+1)$. We have

$$f(x+1)=\frac{(x+1)^p-1}{(x+1)-1}=\sum_{k=0}^{p-1}\binom{p}{k+1}x^k=x^{p-1}+px^{p-2}+\cdots+\binom{p}{k}x^k+\cdots+p. \tag{105}$$

By Eisenstein's, $f(x+1)$ is irreducible. Additionally, we note that if p were composite, this proof could fail because one of the binomial coefficients may not be divisible by a prime that divides the constant term (say if $p=p_1p_2$). □

Also, $\mathbb{Q}(\zeta)$ is Galois because it is the splitting field of $f(x)$. So we have

$$\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \{\sigma_k : \sigma_k(\zeta) = \zeta^k \text{ for } 1 \leq k \leq p-1\}. \tag{106}$$

Now let's compute the trace and norm of ζ. (We omit the subscripts, but it's clear that $T = T_{\mathbb{Q}(\zeta)/\mathbb{Q}}$ and likewise for the norm). We have

$$T(\zeta) = T(\zeta^j) = -1, \text{ by Viete's} \tag{107}$$
$$T(1) = p-1, \text{ since } 1 + \zeta + \cdots + \zeta^{p-1} = 0. \tag{108}$$

By linearity of the trace, we have

$$T(1-\zeta) = T(1) - T(\zeta) = (p-1) - (-1) = p \tag{109}$$
$$N(\zeta - 1) = (-1)^{\text{blah}} \cdot \text{constant term of the min poly of } (\zeta - 1) = (-1)^{p-1}p, \tag{110}$$

since the minimal polynomial of $\zeta - 1$ is $f(x+1)$. Since p is odd, $N(1-\zeta) = p$ as well, because $N(-1) = (-1)^{p-1} = 1$.

7 Sept. 21, 2016

7.1 Cyclotomic Fields, continued

Recall that our goal is to show that $R_{\mathbb{Q}(\zeta)} = \mathbb{Z}[\zeta]$. (We write $R = R_{\mathbb{Q}(\zeta)}$ for ease). We computed

$$T(\zeta^j) = -1 \text{ for } \leq j \leq p-1 \tag{111}$$
$$T(1) = p-1 \tag{112}$$
$$T(1-\zeta^j) = p \text{ for } 1 \leq j \leq p-1 \tag{113}$$
$$N(1-\zeta) = p. \tag{114}$$

Using the last line and the fact that the norm is the product of conjugates gives

$$p = N(1-\zeta) = \prod_{j=1}^{p-1}(1-\zeta^j). \tag{115}$$

Step 1: Compute $(1-\zeta)R \cap \mathbb{Z}$. We have $1 - \zeta^j \in \mathbb{Z}[\zeta] \subset R$ for $j > 1$. Thus,

$$p = \prod_{j=1}^{p-1}(1-\zeta^j) \in (1-\zeta)R. \tag{116}$$

Thus, $p \in (1-\zeta)R \cap \mathbb{Z}$. Since this is an ideal in $\mathbb{Z}$, we must have that it equals either $p\mathbb{Z}$ or $\mathbb{Z}$. We want to show that it equals $p\mathbb{Z}$, so assume for the sake of contradiction that

$$(1-\zeta)R \cap \mathbb{Z} = \mathbb{Z}. \tag{117}$$

This implies that $1 \in (1-\zeta)R$, which further implies $1 - \zeta \in R^*$. Similarly, all the conjugates of $1-\zeta$ are units, since we can apply some $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Thus,

$$1 - \zeta^j \in R^* \tag{118}$$

for $j = 1, \ldots, p-1$.

But now we use that $p = \prod_{j=1}^{p-1}(1-\zeta^j)$. Since p is the product of units, we must have $p \in R^*$. Thus $p \cdot u = 1$ for some $u \in R$. But this implies that $u = \frac{1}{p}$, so $u \in \mathbb{Q}$ and u is integral over $\mathbb{Z}$. But this is not possible, so we have a contradiction. Thus, $(1-\zeta)R \cap \mathbb{Z} = p\mathbb{Z}$.

(We won't prove this, but if we try to go the other way— pushing $p\mathbb{Z}$ up to R instead of going down from an ideal of R— then we'll see that $pR = (1-\zeta)^{p-1}R$).

Step 2: Let $\beta \in R$. We want to show that $\beta \in \mathbb{Z}[\zeta]$. We know that $\beta \in \mathbb{Q}[\zeta]$, so we can write

$$\beta = b_0 + b_1\zeta + \cdots + b_{p-2}\zeta^{p-2} \tag{119}$$

for some $b_i \in \mathbb{Q}$. We want to show that $b_i \in \mathbb{Z}$.

The trick here is to look at $T_{R/\mathbb{Z}}((1-\zeta)\beta)$. Since this is the trace of R down to $\mathbb{Z}$, this element is in $\mathbb{Z}$. We can write

$$T((1-\zeta)\beta) = \sum_{j=0}^{p-2}(1-\zeta^j)\beta_j. \tag{120}$$

where β_j are the conjugates of β. Now, $\beta_j \in R$, and $1-\zeta^j \in (1-\zeta)R$. Thus, the above expression is in $(1-\zeta)R \cap \mathbb{Z}$. Therefore

$$T((1-\zeta)\beta) \in p\mathbb{Z}. \tag{121}$$

We have

$$\begin{aligned} T((1-\zeta)\beta) &= T\left((1-\zeta)\cdot\sum_{j=0}^{p-2} b_j\zeta^j\right) \\ &= \sum_{j=0}^{p-2} b_j(T(\zeta^j) - T(\zeta^{j+1})) \\ &= pb_0 \end{aligned} \tag{122}$$

This is because $T(\zeta^j) = -1$ if $p \nmid j$ and $T(\zeta^j) = p-1$ if $p \mid j$. Since $T((1-\zeta)\beta) \in p\mathbb{Z}$, this implies $b_0 \in \mathbb{Z}$.

To show that the other coefficients are integers, we can replace β with

$$(\beta - b_0)\zeta^{-1} = b_1 + b_2\zeta + \cdots + b_{p-2}\zeta^{p-3} \tag{123}$$

and repeat the same argument to show $b_1 \in \mathbb{Z}$. Repeating this argument again shows that $b_2, b_3, ..., b_{p-2} \in \mathbb{Z}$, as desired.

7.2 Facts about R_K

Proposition 7.1

Consider $K/\mathbb{Q}$ with $n = [K : \mathbb{Q}]$. Then R_K is a free $\mathbb{Z}$-module of rank n. That is,

$$R_K \cong \mathbb{Z}^n \tag{124}$$

as $\mathbb{Z}$-modules.

Proof. R_K is a finitely-generated free $\mathbb{Z}$-module. Thus, by the fundamental theorem of finitely generated abelian groups

$$R_K = (\text{finite group}) \times \mathbb{Z}^r. \tag{125}$$

However, there can be nothing in the finite group, as otherwise it would have to be killed off by some $z \in \mathbb{Z}$. Thus, the question now is what is r.

Certainly $r \le n$ due to some argument about vector spaces I missed (this link is a good explanation for why R_K is finitely generated). For the other direction, let $\beta_1, \ldots, \beta_n \in K$ be generators for K over $\mathbb{Q}$. By a homework problem, there exists $d \in R, d \neq 0$ such that

$$d\beta_1, \ldots, d\beta_n \in R_K. \tag{126}$$

If $r < n$, then

$$\sum_{i=1}^{n} (c_i d)\beta_i = 0 \tag{127}$$

with $c_i \in R_k$. Since the β_i are K-linearly independent, $c_i d = 0 \Rightarrow c_i = 0$. □

Proposition 7.2

Let $K/\mathbb{Q}$. Then R_K is integrally closed.

Proof. Let $\beta \in K$ be integral over R_K. We want to show that $\beta \in K$ is integral over R_K. We have the following tower.

$$\begin{tikzcd}
R_K[\beta] \arrow[d, dash] \\
R_K \arrow[d, dash] \\
\mathbb{Z}.
\end{tikzcd}$$

$R_K[\beta]$ is integral over R by definition. Also, R_K is integral over $\mathbb{Z}$, again by definition. Thus $R_K[\beta]$ is integral over $\mathbb{Z}$, so β is integral over $\mathbb{Z}$. But by definition, R_K is the set of elements in K that are integral over $\mathbb{Z}$. Thus, $\beta \in R_K$. □

Goal: Given $K/\mathbb{Q}$, we want to describe the ideals in R_K. For example, if $K = \mathbb{Q}$, we would want to describe all the ideals in $\mathbb{Z}$. Let $\mathfrak{a} \in R_K$ be an ideal. Assume $\mathfrak{a} \neq 0$. Here are some facts:

1. $\mathfrak{a} \cap \mathbb{Z} \neq 0$. This is a HW problem.

2. $\mathfrak{a}$ is a finitely-generated, free $\mathbb{Z}$-module, since it is a $\mathbb{Z}$-submodule of R_K.

3. $R_K/\mathfrak{a}$ is finite.

   Proof. Let $0 \neq d \in \mathfrak{a} \cap \mathbb{Z}$, by property 1. Then,

   $$dR_K \subset \mathfrak{a}, \tag{128}$$

   so $R_K/dR_K \supset R_K/\mathfrak{a}$. As a $\mathbb{Z}$-module, we have

   $$R_K/dR_K \cong \mathbb{Z}^n/d\mathbb{Z}^n \cong (\mathbb{Z}/d\mathbb{Z})^n. \tag{129}$$

   Thus, R_K/dR_K is finite, so $R_K/\mathfrak{a}$ is as well. □

Definition 7.3

The **norm of** $\mathfrak{a}$, where $\mathfrak{a} \neq (0)$, is

$$N\mathfrak{a} = N_{K/\mathbb{Q}}\mathfrak{a} = \#(R_K/\mathfrak{a}). \tag{130}$$

By convention, set $N(0) = 0$.

Suppose $\mathfrak{a} = \alpha R_K$. Then $N_{K/\mathbb{Q}}(\alpha) = \prod_{\sigma:K \hookrightarrow \overline{K}} \sigma(\alpha)$. This does not look very similar to our definition above, but later we will show that

$$|N_{K/\mathbb{Q}}\alpha| = N(\mathfrak{a}). \tag{131}$$

Continuining on with our facts:

4. Let $\mathfrak{p} \subset R_K$ be a (non-zero) prime ideal. Then

   (a) $\mathfrak{p}$ is maximal,

   (b) $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ for some prime $p \in p\mathbb{Z}$.

   Proof. Note that $R_K/\mathfrak{p}$ is finite and an integral domain, since $\mathfrak{p}$ is prime. These two facts imply that $R_K/\mathfrak{p}$ is a field, so $\mathfrak{p}$ is maximal. □

Hinting at the connection between R_K and Dedekind domains, we see that

- R_K is integrally closed.
- Every non-zero prime ideal is maximal.
- R_K is Noetherian.

Okay, we didn't actually prove the last one. So let's do that.

Proof. If $\mathfrak{a} \subset \mathfrak{b}$, then $R/\mathfrak{a} \xrightarrow{onto} R/\mathfrak{b}$, so that $\#(R/\mathfrak{a}) \geq \#(R/\mathfrak{b})$ and $N\alpha \geq N\beta$. Further, if our inclusion is strict, then $N\alpha > N\beta$.

So suppose $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots$ is an infinite strictly increasing chain. Then $N\mathfrak{a}_1 > N\mathfrak{a}_2 > N\mathfrak{a}_3 > \cdots$. But norms are positive integers, so well-ordering principle. BAM. □

8 Sept. 23, 2016

I ended up writing these notes in my notebook. I'll copy them over at some point. We proved things about Dedekind domains, and are very close to unique factorization of ideals.

9 Sept. 26, 2016

9.1 Unique Factorization of Ideals

Recall that if $\mathfrak{a} \subset K$ is a fractional ideal (an R-submodule of K), then

$$\mathfrak{a}^{-1} := \{\beta \in K : \beta\mathfrak{a} \subset R\}. \tag{132}$$

Last time, we proved the following:

Proposition 9.1

If $\mathfrak{p}$ is prime, then $\mathfrak{p}\mathfrak{p}^{-1} = R$.

This is the key for the big theorem about Dedekind domains.

Theorem 9.2

If $\mathfrak{a} \subset R$ is a nonzero proper ideal, then you can uniquely write $\mathfrak{a}$ as a product of prime ideals.

Note that, if R is a PID, then this is not too hard to show (very similar to $\mathbb{Z}$).

Proof. First we show existence. We use an argument very common when talking about Noetherian rings. Let

$$S = \{\mathfrak{a} \subset R : \mathfrak{a} \text{ is not a product of primes}\}. \tag{133}$$

If $S = \emptyset$, we are done. Otherwise, since R is Noetherian, S has a maximal element, say $\mathfrak{b}$. By Zorn's lemma, let $\mathfrak{p}$ be a maximal ideal with $\mathfrak{b} \subset \mathfrak{p}$. If $\mathfrak{b} = \mathfrak{p}$, we have a contradiction. Multiplying by $\mathfrak{p}^{-1}$ on both sides gives us

$$\mathfrak{b} \subsetneq \mathfrak{p} \Rightarrow \mathfrak{b}\mathfrak{p}^{-1} \subsetneq \mathfrak{p}\mathfrak{p}^{-1} = R. \tag{134}$$

We also know that $R \subsetneq \mathfrak{p}^{-1}$. This implies that $\mathfrak{b} \subsetneq \mathfrak{p}^{-1}\mathfrak{b}$, so

$$\mathfrak{b} \subsetneq \mathfrak{p}^{-1}\mathfrak{b} \subsetneq R, \tag{135}$$

Thus, since $\mathfrak{b}$ is a maximal element of S, and $\mathfrak{p}^{-1}\mathfrak{b}$ is a proper ideal, we can write $\mathfrak{p}^{-1}\mathfrak{b}$ as a product of primes:

$$\mathfrak{p}^{-1}\mathfrak{b} = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_n \tag{136}$$

Multiplying by $\mathfrak{p}$ on both sides gives

$$\mathfrak{b} = \mathfrak{p}\mathfrak{p}_1 \cdots \mathfrak{p}_n. \tag{137}$$

Thus, $\mathfrak{b}$ is a product of ideals, which is a contradiction.

Next, we show uniqueness. Suppose it's false, and write

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s \tag{138}$$

for unequal prime ideals, with r minimal. From this, we get

$$\mathfrak{p}_1 \mid \mathfrak{q}_1 \cdots \mathfrak{q}_s. \tag{139}$$

Since $\mathfrak{p}_1$ is prime, $\mathfrak{p}_1 \mid \mathfrak{q}_1$ after relabeling, or $\mathfrak{q}_1 \subset \mathfrak{p}_1$. Since these are both proper maximal ideals, $\mathfrak{q}_1 = \mathfrak{p}_1$, so we can write

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{p}_1\mathfrak{q}_2 \cdots \mathfrak{q}_s. \tag{140}$$

Multiplying both sides by $\mathfrak{p}_1^{-1}$ and using that $\mathfrak{p}_1\mathfrak{p}_1^{-1} = R$ gives us

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s \tag{141}$$

This is another counterexample, but we chose r to be minimal, which is a contradiction. □

9.2 Application to Riemann-Zeta Functions

Recall the Riemann-Zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \left(1 - \frac{1}{p^s}\right)^{-1}. \tag{142}$$

The RHS is essentially unique factorization. We can also define the Riemann-Zeta function for a number field $K/\mathbb{Q}$.

$$\zeta_K(s) = \sum_{0 \neq \mathfrak{a} \subset R} \frac{1}{(N\mathfrak{a})^s}, \tag{143}$$

where $N\mathfrak{a} = \#(R/\mathfrak{a})$. It turns out we can write

$$\zeta_K(s) = \sum_{0 \neq \mathfrak{a} \subset R} \frac{1}{(N\mathfrak{a})^s} = \prod_{\mathfrak{p}} \left(1 - \frac{1}{(N\mathfrak{a})^s}\right)^{-1}. \tag{144}$$

This uses unique factorization of ideals, plus the fact that $N(\mathfrak{a}\mathfrak{b}) = N\mathfrak{a} \cdot N\mathfrak{b}$.

9.3 Chinese Remainder Theorem

Let R be a ring, and let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be ideals. Assume that for all $i \neq j$, $\mathfrak{a}_i + \mathfrak{a}_j = R$. We say that $\mathfrak{a}_i$ and $\mathfrak{a}_j$ are **relatively prime** if this holds. We can map

$$R \to R/\mathfrak{a}_1 \times R\mathfrak{a}_2 \times \cdots \times R/\mathfrak{a}_n \tag{145}$$

in the obvious way.

Theorem 9.3 (Chinese Remainder Theorem)
This is an onto map, and its kernel is $\cap_{i=1}^n \mathfrak{a}_i$.

Proof. The idea of this proof is that, if we can show that $(1, 0, \ldots, 0), (0, 1, \ldots, 0)$, etc. are in the image of this map, then we can take a linear combination to get anything in the range.

We have

$$\begin{aligned} 1 \in R &= (\mathfrak{a}_1 + \mathfrak{a}_2)(\mathfrak{a}_1 + \mathfrak{a}_3) \cdots (\mathfrak{a}_1 + \mathfrak{a}_n) \\ &\subset \mathfrak{a}_1 + (\mathfrak{a}_2\mathfrak{a}_3 \cdots \mathfrak{a}_n) \end{aligned} \tag{146}$$

Thus, we can write $1 = \alpha_1 + \beta_1$, where $\alpha_1 \in \mathfrak{a}_1$ and $\beta_1 \in \mathfrak{a}_2 \cdots \mathfrak{a}_n$. Now what is the image of β_1? Since β_1 is in $\mathfrak{a}_i$, $\beta_1 + \mathfrak{a}_i = 0$ for $i > 2$. For $i = 1$, $\beta_1 + \mathfrak{a}_i = 1$. Thus,

$$\beta_1 \mapsto (1, 0, \ldots, 0). \tag{147}$$

Repeating this for $i = 2, \ldots, n$, we get $1 = \alpha_i + \beta_i$, where $\alpha_i \in \mathfrak{a}_i$ and $\beta_i \in \mathfrak{a}_1 \cdots \mathfrak{a}_{i-1}\mathfrak{a}_{i+1} \cdots \mathfrak{a}_n$. Then, for $j \neq i$,

$$\beta_i \equiv 0 \pmod{\mathfrak{a}_j} \tag{148}$$

$$\beta_i \equiv 1 \pmod{\mathfrak{a}_i} \tag{149}$$

so $\beta_i \mapsto (0, \ldots, 1, \ldots, 0)$. Finally, if $c_1, \ldots, c_n \in R$, then

$$\sum_{i=1}^{n} c_i\beta_i \mapsto (\overline{c_1}, \ldots, \overline{c_n}) \in R/\mathfrak{a}_1 \times \cdots \times R/\mathfrak{a}_n. \tag{150}$$

Thus, our map is surjective. It's clear that the kernel is $\cap_{i=1}^n \mathfrak{a}_i$. □

Proposition 9.4

If R is a Dedekind domain, and $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are distinct primes, then by linearity,

$$\cap_{i=1}^{r} \mathfrak{p}_i^{e_i} = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i} \tag{151}$$

Proof. We will sketch the proof for $r = 2$. Let $\mathfrak{p}, \mathfrak{q}$ be the two primes. It's clear that

$$\mathfrak{p}\mathfrak{q} \subset \mathfrak{p} \cap \mathfrak{q}. \tag{152}$$

For the other direction, since R is Dedekind, we can write

$$\mathfrak{p} \cap \mathfrak{q} = \mathfrak{p}^e \cdot \mathfrak{q}^f \cdot \mathfrak{a} \tag{153}$$

where $\mathfrak{a}$ is some ideal with no $\mathfrak{p}$'s or $\mathfrak{q}$'s in its prime factorization. We want to show that $e = f = 1$ and $\mathfrak{a} = R$.

Suppose $e > 2$. Then $\mathfrak{p} \cap \mathfrak{q} \subset \mathfrak{p}^2$. Now let $\beta \in \mathfrak{q}$. Then,

$$\beta\mathfrak{p} \subset \mathfrak{p} \cap \mathfrak{q} \subset \mathfrak{p}^2. \tag{154}$$

Multiplying by $\mathfrak{p}^{-1}$ on both sides (which we can do since $\mathfrak{p}\mathfrak{p}^{-1} = R$), we get

$$\beta R \subset \mathfrak{p} \Rightarrow \beta \in \mathfrak{p} \tag{155}$$

This implies that $\mathfrak{q} \subset \mathfrak{p}$. Since prime ideals are maximal, $\mathfrak{q} = \mathfrak{p}$, which is a contradiction. Thus, $e \leq 1$. Similarly, $f \leq 1$. A similar argument shows that no other prime ideals can factor $\mathfrak{a}$. This implies

$$\mathfrak{p} \cap \mathfrak{q} = R, \mathfrak{p}, \mathfrak{q}, \text{or } \mathfrak{p}\mathfrak{q}. \tag{156}$$

$\mathfrak{p} \cap \mathfrak{q}$ is certainly not equal to R. It also isn't equal to $\mathfrak{p}$ or $\mathfrak{q}$, since otherwise this implies $\mathfrak{p} = \mathfrak{q}$. Thus, $\mathfrak{p} \cap \mathfrak{q} = \mathfrak{p}\mathfrak{q}$. □

Corollary 9.5

$N(\mathfrak{a}\mathfrak{b}) = N\mathfrak{a} \cdot N\mathfrak{b}$.

Proof. It suffices to show

1. $N(\prod \mathfrak{p}_i^{e_i}) = \prod N(\mathfrak{p}_i^{e_i})$, and
2. $N(\mathfrak{p}^e) = N(\mathfrak{p})^e$.

Not enough time, so we'll only show the first one. We know that $\mathfrak{p}_i + \mathfrak{p}_j = R$ for $i \neq j$, since $\mathfrak{p}_i + \mathfrak{p}_j$ strictly contains $\mathfrak{p}_i$ and $\mathfrak{p}_j$. I claim that

$$\mathfrak{p}_i^{e_i} + \mathfrak{p}_j^{e_j} = R. \tag{157}$$

The proof is pretty simple: show that $R = (\mathfrak{p}_i + \mathfrak{p}_j)^{e_i + e_j - 1} \subset \mathfrak{p}_i^{e_i} + \mathfrak{p}_j^{e_j}$.

Now by the Chinese Remainder Theorem and our proposition,

$$R/\prod \mathfrak{p}_i^{e_i} = R/\cap \mathfrak{p}_i^{e_i} \to \prod R/\mathfrak{p}_i^{e_i} \tag{158}$$

is a bijection. Looking at the number of elements on each side yields

$$N(\prod \mathfrak{p}_i^{e_i}) = \prod N(\mathfrak{p}_i^{e_i}), \tag{159}$$

as desired. □

10 Sept. 28, 2016

10.1 Finishing up the proof

Last time, we were halfway through proving $N(\mathfrak{a}\mathfrak{b}) = N\mathfrak{a} \cdot N\mathfrak{b}$. We now need to show that $N(\mathfrak{p}^e) = N(\mathfrak{p})^e$. To do this, we need the following lemma.

Lemma 10.1

Consider $\mathfrak{p}^e/\mathfrak{p}^{e+1}$ as a $R/\mathfrak{p}$-vector space. Then, its dimension as a $R/\mathfrak{p}$ vector space is 1.

Proof. Since $\mathfrak{p}$ is strictly contained in R, then $\mathfrak{p}^{e+1}$ is strictly contained in $\mathfrak{p}^e$. Thus, $\dim(\mathfrak{p}^e/\mathfrak{p}^{e+1}) \geq 1$.

Now choose some $\alpha \in \mathfrak{p}^e \setminus \mathfrak{p}^{e+1}$. We want to show that every element is a multiple of α. Consider the ideal $\mathfrak{p}^{e+1} + \alpha R$. We have

$$\mathfrak{p}^{e+1} \subsetneq \mathfrak{p}^{e+1} + \alpha R \subset \mathfrak{p}^e \tag{160}$$

"Now we hit it with a big hammer." Unique factorization tells us that $\mathfrak{p}^{e+1} + \alpha R$ is a power of $\mathfrak{p}$. Since the above inclusion is strict, it is not a multiple of $\mathfrak{p}^{e+1}$. Thus,

$$\mathfrak{p}^{e+1} + \alpha R = \mathfrak{p}^e \tag{161}$$

which implies that α generates $\mathfrak{p}^e/\mathfrak{p}^{e+1}$ as an $R/\mathfrak{p}$-module. Thus, $\dim(\mathfrak{p}^e/\mathfrak{p}^{e+1}) = 1$ as an $R/\mathfrak{p}$-module. □

We now finish our proof that $N(\mathfrak{a}\mathfrak{b}) = N\mathfrak{a} \cdot N\mathfrak{b}$.

Proof. Now we will prove our claim by induction on e. The base case is clear, so assume it holds for e. Consider the map

$$R/\mathfrak{p}^{e+1} \to R/\mathfrak{p}^e \to 0. \tag{162}$$

What is the kernel of the left map? $\mathfrak{p}^e/\mathfrak{p}^{e+1}$. This gives us an exact sequence of finite R-modules

$$0 \to \mathfrak{p}^e/\mathfrak{p}^{e+1} \to R/\mathfrak{p}^{e+1} \to R/\mathfrak{p}^e \to 0. \tag{163}$$

Since this is an exact sequence of finite R-modules, the size of the middle is equal to the product of the sizes of the left and the right, i.e.

$$\#(R/\mathfrak{p}^{e+1}) = \#(\mathfrak{p}^e/\mathfrak{p}^{e+1}) \cdot \#(R/\mathfrak{p}^e). \tag{164}$$

Now by our lemma, $\mathfrak{p}^e/\mathfrak{p}^{e+1}$ has dimension 1 as a $R/\mathfrak{p}$-module. Thus, it has $\#(R/\mathfrak{p}) = N\mathfrak{p}$ elements. By induction, $(\#(R/\mathfrak{p}^e)) = N(\mathfrak{p})^e$. Thus,

$$\#(R/\mathfrak{p}^{e+1}) = N(\mathfrak{p})^{e+1} \tag{165}$$

and we are done. □

10.2 Fractional Ideals

Let $I_K = \{$(non-zero) fractional ideals of $K\}$. Every $C \in I_K$ is uniquely written as

$$C = \prod \mathfrak{p}^{e_{\mathfrak{p}}(C)} \tag{166}$$

with $e_{\mathfrak{p}}(C) \in \mathbb{Z}$. Why? We can find an $\alpha \in R$ with $\alpha C \subset R$ by just clearing all denominators of a generating set. So we can write

$$\alpha C = \prod \mathfrak{p}^{e_{\mathfrak{p}}(\alpha C)}. \tag{167}$$

We also have

$$\alpha R = \prod \mathfrak{p}^{e_\mathfrak{p}(\alpha R)}. \tag{168}$$

Thus,

$$C = (\alpha C)(\alpha^{-1}R) = \prod \mathfrak{p}^{e_\mathfrak{p}(\alpha C) - e_\mathfrak{p}(\alpha R)}. \tag{169}$$

This immediately gives us the following.

Corollary 10.2

For all $\mathfrak{p} \in I_K$, there exists a unique $\mathfrak{p} \in I_K$ with $\mathfrak{a}\mathfrak{b} = R$.

Proof. If $\mathfrak{a} = \prod \mathfrak{p}^{e_\mathfrak{p}(\mathfrak{a})}$, then let $\mathfrak{b} = \prod \mathfrak{p}^{e_\mathfrak{p}(\mathfrak{b})}$. □

Note that, by the above result, I_K is a group. One important subgroup of I_K is those generated by one element, the principal (fractional) ideals.

$$\{\alpha R : \alpha \in K^*\}. \tag{170}$$

This is clearly a subgroup, since $(\alpha R)(\beta R) = (\alpha\beta)R$. Another way to define this is the image of the map

$$\begin{aligned} K^* &\to I_K && (171) \\ \alpha &\mapsto \alpha R. && (172) \end{aligned}$$

Let the quotient of this map be C_K, the **ideal class group**. C_K = fractional ideals/principal ideals. Then we get the exact sequence

$$K^* \to I_K \to C_K \to 1 \tag{173}$$

Now how do we make the left of this equation exact? That is, what $\alpha \in K^*$ satisfy $\alpha R = R$? These are the units of R. Thus, we have the full exact sequence

$$1 \to R_K^* \to K^* \to I_K \to C_K \to 1 \tag{174}$$

where R_K^* are the units of R_K. Both the unit group and the ideal class group are heavily studied in algebraic number theory. Here are two theorems we want to prove this semester.

Theorem 10.3

C_K is finite.

Then, we can define $h_K = \#C_K$, the class number of K.

Theorem 10.4

R_K^* is finitely-generated.

Then, as we saw in the beginning of class, $\mathrm{rank}(R_K^*) = r_1 + r_2 - 1$, where r_1 is the number of real embeddings and $2r_2$ the number of complex embeddings.

10.3 Factorization in Extension Fields

Let R_K be a Dedekind domain, K be its fraction field, and let L/K be a finite extension. Let R_L be the integral closure of R_K in L.

Proposition 10.5

R_L is a Dedekind domain.

Proof. Same as our proof for when $K = \mathbb{Q}, R_K = \mathbb{Z}$. (need to look back in notes, I'm not sure what he's referring to). □

Here's a picture.

$$\begin{tikzcd}
R_L \arrow[r, phantom, "\subset"] \arrow[d, dash] & L \arrow[d, dash] \\
R_K \arrow[r, phantom, "\subset"] & K
\end{tikzcd}$$

Let $\mathfrak{p} \subset R_K$ be prime. Then $\mathfrak{p}R_L$ is an ideal of R_L. Is it prime? ... Probably not. For example, consider

$$\begin{tikzcd}
Z[i] \arrow[r, phantom, "\subset"] \arrow[d, dash] & \mathbb{Q}(i) \arrow[d, dash] \\
\mathbb{Z} \arrow[r, phantom, "\subset"] & \mathbb{Q}
\end{tikzcd}$$

Then $p\mathbb{Z}[i]$ is not always prime. For instance, $5 \cdot \mathbb{Z}[i]$ is not prime, since $5 = (2+i)(2-i)$ and neither factor is in the ideal.

Let $\mathcal{P} \subset R_L$ be a prime of R_L with $\mathcal{P} \mid \mathfrak{p}R_L$. (Note that this is equivalent to $\mathfrak{p}R_L \subset \mathcal{P}$). This induces a well-defined map

$$R_K/\mathfrak{p} \hookrightarrow R_L/\mathcal{P} \tag{175}$$

Now $R_K/\mathfrak{p}$ and $R_L/\mathcal{P}$ are finite fields. So one important question to ask is: what is the field extension?

Definition 10.6

The **residue field degree** of $\mathcal{P}/\mathfrak{p}$ is

$$f(\mathcal{P}/\mathfrak{p}) = [R_L/\mathcal{P} : R_K/\mathfrak{p}]. \tag{176}$$

What if $\mathcal{P}$ divides $\mathfrak{p}$ multiple times? For example, with $\mathbb{Z}[i]$, we have $2\mathbb{Z}[i] = ((1+i)\mathbb{Z}[i])^2$.

Definition 10.7

The **ramification degree of** $\mathcal{P}/\mathfrak{p}$, denoted $e(\mathcal{P}/\mathfrak{p})$, is the largest $e \geq 1$ with $\mathcal{P}^e \mid \mathfrak{p}R_L$. If $e \geq 2$, we say $\mathfrak{p}$ is **ramified**.

We have the following fact, due to Dedekind, which will be proven later.

Fact 10.8. The set

$$\{\mathfrak{p} \subset R_K : e(\mathcal{P}/\mathfrak{p}) \geq 2 \text{ for some } \mathcal{P} \mid \mathfrak{p}R_L\} \tag{177}$$

is finite.

For example, 2 ramifies in $\mathbb{Z}[i]$ while 5 does not. Below, we prove a useful formula.

10.4 ref formula

Theorem 10.9

Let $\mathfrak{p} \subset R_K$ be prime, $n = [L : K]$. We can write

$$\mathfrak{p}R_L = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_r}. \tag{178}$$

(Note that $e_i = e(\mathcal{P}_i/\mathfrak{p})$). Then,

$$\sum_{i=1}^{r} e(\mathcal{P}_i/\mathfrak{p}) f(\mathcal{P}_i/\mathfrak{p}) = n. \tag{179}$$

Proof. Taking the norm of both sides of equation 178 and using multiplicativity, we get

$$\begin{aligned} N(\mathfrak{p}R_L) &= \prod_{i=1}^{r} (N\mathcal{P}_i)^{e_i} \\ &= \prod_{i=1}^{r} \#(R_L/\mathcal{P}_i)^{e_i}. \end{aligned} \tag{180}$$

Since $(R_L/\mathcal{P}_i)^{e_i}$ is a $R_K/\mathfrak{p}$-vector space of dimension $f(\mathcal{P}_i/\mathfrak{p})$, which we abbreviate to f_i, we get

$$\begin{aligned} N(\mathfrak{p}R_L) &= \prod_{i=1}^{r} \#(R_L/\mathcal{P}_i)^{e_i} \\ &= \prod_{i=1}^{r} (\#(R_K/\mathfrak{p})^{f_i})^{e_i} \\ &= \prod_{i=1}^{r} (\#(R_K/\mathfrak{p}))^{f_i e_i} \\ &= (N\mathfrak{p})^{\sum_{i=1}^{r} e_i f_i}. \end{aligned} \tag{181}$$

To deal with the other side of equation 180, we note that

$$(R_L/\mathfrak{p}R_L) = (R_K/\mathfrak{p}R_K)^n. \tag{182}$$

Thus,

$$\#(R_L/\mathfrak{p}R_L) = \#(R_K/\mathfrak{p}R_K)^n = (N\mathfrak{p})^n. \tag{183}$$

Putting both sides together, we have

$$(N\mathfrak{p})^{\sum_{i=1}^{r} e_i f_i} = (N\mathfrak{p})^n. \tag{184}$$

Since $\mathfrak{p}$ is a proper ideal, $N\mathfrak{p} > 1$. Thus,

$$n = \sum_{i=1}^{r} e_i f_i \tag{185}$$

as desired. □

11 Sept. 30, 2016

11.1 Dedekind's Theorem on Ramification

Consider the usual picture

$$\begin{tikzcd}
R_L \arrow[r, phantom, "\subset"] \arrow[d, no head] & L \arrow[d, no head] \\
\mathbb{Z} \arrow[r, phantom, "\subset"] & \mathbb{Q}.
\end{tikzcd}$$

Recall the following definition.

Definition 11.1

Say $pR_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_i^{e_i}$. Then p **ramifies** in K if any $e_i \geq 1$.

It turns out that ramification is not common.

Theorem 11.2 (Dedekind)

p ramifies in K iff $p \mid D_{K/\mathbb{Q}}$.

Thus, there are only finitely primes that ramify in any extension $K/\mathbb{Q}$.

We'll prove the left-to-right direction, and the other direction will be homework. The proof will go through the construction of something called the different.

11.2 Constructing the Different

Lemma 11.3

Consider the set $\mathfrak{a} = \{\alpha \in L : \mathrm{Tr}(\alpha R_K) \subset \mathbb{Z}\}$, where $\mathrm{Tr}(\alpha R_K) = \{\mathrm{Tr}(\alpha\beta) : \beta \in R_K\}$. Then $\mathfrak{a}$ is a fractional ideal.

Proof. Note that $R_K \subset \mathfrak{a}$. To show that $\mathfrak{a}$ is a fractional ideal, we need to show that it's a finitely-generated R_K-module.

First we check that $\mathfrak{a}$ is an R_K-module. Let $\beta \in R_K, \alpha \in \mathfrak{a}$. Then we want $\beta\alpha \in \mathfrak{a}$. We have

$$\mathrm{Tr}(\beta\alpha R_K) = \mathrm{Tr}(\alpha(\beta R_K)) \subset \mathrm{Tr}(\alpha R_K) \subset \mathbb{Z} \tag{186}$$

since $\beta \in R_K$. Thus, $\mathfrak{a}$ is an R_K-module.

Next, we check that $\mathfrak{a}$ is finitely-generated. Let $\omega_1, \ldots, \omega_n$ be a $\mathbb{Z}$-basis for R_K. Then the ω_i are also a $\mathbb{Q}$-basis for K. Consider the map

$$\begin{aligned} K \times K &\to \mathbb{Q} \\ (x, y) &\mapsto \mathrm{Tr}(x, y) \end{aligned}$$

We showed that this map is $\mathbb{Q}$-bilinear, and non-degenerate (we used independence of characters to show this). Let $\omega_1^*, \ldots, \omega_n^*$ (all in K) be a dual $\mathbb{Q}$-basis for K. That is,

$$(\omega_i, \omega_j^*) \mapsto \mathrm{Tr}(\omega_i\omega_j) = \delta_{i,j}. \tag{187}$$

This implies that $\mathrm{Tr}(\beta\omega_k^*) \in \mathbb{Z}$ for all $\beta \in R_K$, since $\beta = \sum b_i\omega_i$, with $b_i \in \mathbb{Z}$, and trace is $\mathbb{Q}$-linear. Thus, $\mathrm{Tr}(\omega_j^* R_K) \subset \mathbb{Z}$, so $\omega_j^* \in \mathfrak{a}$. We can write this as

$$\sum \mathbb{Z}\omega_i^* \subset \mathfrak{a}. \tag{188}$$

Now we claim that the above two sets are in fact equal. If true, this will show that $\mathfrak{a}$ is finitely-generated. Let $\alpha \in \mathfrak{a}$. Since $\alpha \in K$, we can write $\alpha = \sum_{i=1}^n a_i\omega_i^*$ for some $a_i \in \mathbb{Q}$. Then

$$\begin{aligned} \mathrm{Tr}(\alpha\omega_j) &= \sum_{i=1}^n a_i \,\mathrm{Tr}(\omega_j\omega_i^*) \\ &= \sum_{i=1}^n a_i\delta_{i,j} \\ &= a_j. \end{aligned} \tag{189}$$

Since $\alpha \in \mathfrak{a}$ and $\omega_j \in R_K$, it follows that $\mathrm{Tr}(\alpha\omega_j) \in \mathbb{Z}$, so $a_j \in \mathbb{Z}$. Thus,

$$\alpha \in \sum \mathbb{Z}\omega_i^*, \tag{190}$$

so $\mathfrak{a}$ is generated by the ω_i^*. □

This motivates the following definition.

Definition 11.4

The **different of** $K/\mathbb{Q}$ is

$$\mathfrak{D}_{K/\mathbb{Q}} = \{\alpha \in L : \mathrm{Tr}(\alpha R_K) \in \mathbb{Z}\}^{-1}. \tag{191}$$

That is, it is the inverse of the ideal we were looking at before. Since $R_K \subset \mathfrak{a}$, then $\mathfrak{D}_{K/\mathbb{Q}} = \mathfrak{a}^{-1} \subset R_K$ is an ideal of R_K.

Example 11.5

Let $K = \mathbb{Q}(\sqrt{d})$ where $d \equiv 2, 3 \pmod 4$, so $R_K = \mathbb{Z}[\sqrt{d}]$. Let $\omega_1 = 1, \omega_2 = \sqrt{d}$. We claim the dual basis is $\omega_1^* = \frac{1}{2}$ and $\omega_2^* = \frac{1}{2\sqrt{d}}$. To check

$$\operatorname{Tr}(\omega_1\omega_1^*) = \operatorname{Tr}\left(\frac{1}{2}\right) = 1 \tag{192}$$

$$\operatorname{Tr}(\omega_1\omega_2^*) = \operatorname{Tr}\left(\frac{1}{2\sqrt{d}}\right) = \frac{1}{2\sqrt{d}} - \frac{1}{2\sqrt{d}} = 0 \tag{193}$$

$$\operatorname{Tr}(\omega_2\omega_1^*) = \operatorname{Tr}\left(\frac{\sqrt{d}}{2}\right) = 0 \tag{194}$$

$$\operatorname{Tr}(\omega_2\omega_2^*) = \operatorname{Tr}\left(\frac{1}{2}\right) = 1. \tag{195}$$

Thus, from the proof of the lemma, $\mathfrak{D}_{K/\mathbb{Q}}^{-1} = \frac{1}{2}\mathbb{Z} + \frac{1}{2\sqrt{d}}\mathbb{Z}$. We can write this as

$$\mathfrak{D}_{K/\mathbb{Q}}^{-1} = \frac{1}{2\sqrt{d}}(\mathbb{Z}[\sqrt{d}] + \mathbb{Z}) = \frac{1}{2\sqrt{d}}R_K. \tag{196}$$

Thus, the different is $\mathfrak{D}_{K/\mathbb{Q}} = (2\sqrt{d})R_K$. Its norm is

$$N\mathfrak{D}_{K/\mathbb{Q}} = |4d|. \tag{197}$$

11.3 Refresher on Dual Bases

Let $B : V \times V \to \mathbb{Q}$ be bilinear. Choose a basis $v_1, \ldots, v_n$. Let $M = (B(v_i v_j))$. Then, if $x, y \in V$, writing

$$x = \sum x_i v_i \tag{198}$$

$$y = \sum y_i v_i \tag{199}$$

we can write

$$B(x, y) = \begin{pmatrix} x_1 & \cdots & x_n \end{pmatrix} M \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \tag{200}$$

Now, B is nondegenerate iff $\det M = 0$. To see this, first suppose $\det M = 0$. Then, if y is in the nontrivial kernel of M, $B(x, y) = 0$. The other direction is an exercise.

Now consider the vectors $(M^{-1})v_1, \ldots, (M^{-1})v_n$. Should write it out carefully and show that this is in fact a dual basis. This is useful, because then you can use it for computations.

11.4 Proof of Dedekind's Theorem

First we prove the following proposition.

Proposition 11.6

$N(\mathfrak{D}_{K/\mathbb{Q}}) = |D_{K/\mathbb{Q}}|$, where $D_{K/\mathbb{Q}}$ refers to the discriminant of a $\mathbb{Z}$-basis of R_K. (I think better notation would be $D_{R_K/\mathbb{Z}}$).

Proof. Write $R_K = \sum \mathbb{Z}\omega_i$ for some $\mathbb{Z}$-basis ω_i of R_K. Then,

$$\mathfrak{D}_{K/\mathbb{Q}}^{-1} = \sum \mathbb{Z}\omega_i^*. \tag{201}$$

Now, both ω_i and ω_i^* are $\mathbb{Q}$-bases for K over $\mathbb{Q}$. So we can write

$$\omega_i^* = \sum_{j=1}^{n} a_{ij}\omega_i \tag{202}$$

$$\omega_i = \sum_{j=1}^{n} b_{ij}\omega_j^*, \tag{203}$$

where $a_{ij}, b_{ij} \in \mathbb{Q}$. Clearly $(a_{ij})(b_{ij}) = I$. Now we want to relate these to the discriminant, which has entries $T(\omega_i\omega_j)$. Write

$$\begin{aligned} \mathrm{Tr}(\omega_i\omega_j) &= \mathrm{Tr}(\omega_i \sum_k b_{jk}\omega_k^*) \\ &= \sum_k b_{jk}\omega_i\omega_k^* \\ &= b_{ji}. \end{aligned} \tag{204}$$

The same reasoning says that $\mathrm{Tr}(\omega_j\omega_i) = b_{ij}$. Thus, $b_{ij} = b_{ji}$, so

$$D_{K/\mathbb{Q}} = D_{K/\mathbb{Q}}(\omega_1, \ldots, \omega_n) = \det(\mathrm{Tr}(\omega_i\omega_j)) = \det(b_{ji}) = \det(b_{ij}). \tag{205}$$

On the other hand, we have

$$\begin{aligned} D_{K/\mathbb{Q}}(\omega_1^*, \ldots, \omega_n^*) &= \det(a_{ij})^2 \cdot D_{K/\mathbb{Q}}(\omega_1, \ldots, \omega_n) \\ &= \det(a_{ij})^2 \cdot \det(b_{ij}) \\ &= \frac{1}{\det(b_{ij})} \\ &= \frac{1}{D_{K/\mathbb{Q}}} \end{aligned} \tag{206}$$

where we use that $(a_{ij})(b_{ij}) = I$. Now we need the following lemma.

Lemma 11.7

Let $\mathfrak{a} \subset R_K$, and write $\mathfrak{a} = \alpha_1\mathbb{Z} + \cdots + \alpha_n\mathbb{Z}$. Then

$$|D_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)| = (N\mathfrak{a})^2 \cdot |D_{K/\mathbb{Q}}|. \tag{207}$$

We'll prove the lemma next time. But using the lemma, we have

$$D_{K/\mathbb{Q}}(\omega_1^*, \ldots, \omega_n^*) = N(\mathfrak{D}_{K/\mathbb{Q}}^{-1})^2 \cdot D_{K/\mathbb{Q}}. \tag{208}$$

Thus,

$$N(\mathfrak{D}_{K/\mathbb{Q}}^{-1})^2 \cdot D_{K/\mathbb{Q}} = \frac{1}{D_{K/\mathbb{Q}}} \Rightarrow |D_{K/\mathbb{Q}}| = N(\mathfrak{D}_{K/\mathbb{Q}}). \tag{209}$$

□

12 Oct. 3, 2016

No class.

13 Oct. 5, 2016

13.1 Finishing the proof of Dedekind's Theorem

To recall, we were in the middle of proving that if p ramifies, then $p \mid D_{K/\mathbb{Q}}$. We were proving

$$N_{K/\mathbb{Q}}(\mathfrak{D}_{K/\mathbb{Q}}) = |D_{K/\mathbb{Q}}|. \tag{210}$$

We had gotten to the point where we needed to show that

$$D(\omega_1^*, ..., \omega_n^*) = (N\mathfrak{D}_{K/\mathbb{Q}}^{-1})^2 \cdot D_{K/\mathbb{Q}}. \tag{211}$$

This required the following lemma.

Lemma 13.1

If $\mathfrak{a} \subset R_K, \mathfrak{a} = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$. Then,

$$D(\alpha_1, ..., \alpha_n) = (N\alpha)^2 D_{K/\mathbb{Q}}. \tag{212}$$

Proof. Write $R_K = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$. By definition,

$$D_{K/\mathbb{Q}} = D(\omega_1, ..., \omega_n). \tag{213}$$

Furthermore, since $\alpha_i \in R_K$, we can write

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = M \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} \tag{214}$$

for some matrix M with entries in $\mathbb{Z}$. Using Gram-Schmidt, we can find a new basis β_i for $\mathfrak{a}$ so that M is lower-triangular.

$$\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ a_{21} & a_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} \tag{215}$$

So we can write $\mathfrak{a} = \mathbb{Z}\beta_1 + \cdots + \mathbb{Z}\beta_n$, where

$$\beta_1 = a_{11}\omega_1 \tag{216}$$

$$\beta_2 = a_{21}\omega_1 + a_{22}\omega_2 \tag{217}$$

$$\vdots \tag{218}$$

Since the α_i and β_i have the same $\mathbb{Z}$-span,

$$\begin{aligned} D(\alpha_1, \dots, \alpha_n) &= D(\beta_1, \dots, \beta_n) \\ &= (\det M)^2 \cdot D(\omega_1, \dots, \omega_n) \\ &= (a_{11} \cdots a_{nn})^2 D(\omega_1, \dots, \omega_n), \end{aligned} \tag{219}$$

where we use that the determinant of a lower-triangular matrix is the product of its diagonal entries.

Now we need to show that $a_{11} \cdots a_{nn} = N\mathfrak{a}$. We have

$$\begin{aligned} N\mathfrak{a} &= \# R_K/\mathfrak{a} \\ &= \# \frac{\mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n}{\mathbb{Z}\beta_1 + \cdots + \mathbb{Z}\beta_n} \\ &= \# \frac{\mathbb{Z}\omega_1}{\mathbb{Z}a_{11}\omega_1} \times \frac{\mathbb{Z}\omega_2}{\mathbb{Z}a_{22}\omega_2} \times \cdots \\ &= |a_{11}a_{22} \cdots a_{nn}|. \end{aligned} \tag{220}$$

□

Next, we show the following lemma.

Lemma 13.2

Let $p \in \mathbb{Z}, \mathfrak{P} \in R_K$, where $\mathfrak{P}^{e(\mathfrak{P}/p)} \mid pR_K$ and $e(\mathfrak{P}/p)$ is maximal. Then,

$$\mathfrak{P}^{e(\mathfrak{P}/p)-1} \mid \mathfrak{D}_{K/\mathbb{Q}}. \tag{221}$$

Proof. Write $e = e(\mathfrak{P}/p)$, and

$$pR_K = \mathfrak{P}^e \mathfrak{a} \tag{222}$$

where $\mathfrak{P} \nmid \mathfrak{a}$. Let $\beta \in \mathfrak{P}\mathfrak{a}$. Then, we can write

$$\beta = \sum_{i=1}^{t} \pi_i \alpha_i \tag{223}$$

where $\pi_i \in \mathfrak{P}, \alpha_i \in \mathfrak{a}$. Raising this to the pth power, we have

$$\beta^p \equiv \sum \pi_i^p \alpha_i^p \pmod{pR_K}. \tag{224}$$

In fact, we can keep raising this to the pth power, giving us

$$\beta^{p^m} \equiv \sum \pi_i^{p^m} \alpha_i^{p^m} \pmod{pR_K}. \tag{225}$$

Choose an m with $p^m > e$. Then, $\pi_i^{p^m} \in \mathfrak{P}^e$, and $\alpha_i^{p^m} \in \mathfrak{a}$, so

$$\beta^{p^m} \in \mathfrak{P}^e \mathfrak{a} = pR_K. \tag{226}$$

This implies that $\mathrm{Tr}(\beta^{p^m}) \in p\mathbb{Z}$, since we can write $\beta^{p^m} = pr$ for some $r \in R_K$, and note that $\mathrm{Tr}(r) \in \mathbb{Z}$. Let $\beta_1, \dots, \beta_n$ be the conjugates of β. Then,

$$\begin{aligned} \mathrm{Tr}(\beta^{p^m}) &= \beta_1^{p^m} + \cdots + \beta_n^{p^m} \\ &\equiv (\beta_1 + \cdots + \beta_m)^{p^m} \pmod{pR_K} \\ &\equiv \mathrm{Tr}(\beta)^{p^m} \pmod{pR_K}. \end{aligned} \tag{227}$$

Since $p \mid \operatorname{Tr}(\beta^{p^m})$, we have $p \mid \operatorname{Tr}(\beta)^{p^m}$. Thus, $p \mid \operatorname{Tr}(\beta)$, so

$$\operatorname{Tr}(\mathfrak{P}\mathfrak{a}) \subset p\mathbb{Z}. \tag{228}$$

This is equivalent to

$$\operatorname{Tr}(p^{-1}\mathfrak{P}\mathfrak{a}) \subset \mathbb{Z} \tag{229}$$

since trace is $\mathbb{Q}$-linear. Now recall

$$\mathfrak{D}_{K/\mathbb{Q}}^{-1} = \{\alpha \in K : \operatorname{Tr}(\alpha R_K) \subset \mathbb{Z}\} \supset \{\alpha \in K : \operatorname{Tr}(\alpha) \subset \mathbb{Z}\}. \tag{230}$$

Thus,

$$\begin{aligned} p^{-1}\mathfrak{P}\mathfrak{a} \subset \mathfrak{D}_{K/\mathbb{Q}}^{-1} &\Rightarrow (\mathfrak{P}^e\mathfrak{a})^{-1}\mathfrak{P}\mathfrak{a} \subset \mathfrak{D}_{K/\mathbb{Q}}^{-1} \\ &\Rightarrow \mathfrak{P}^{1-e} \subset \mathfrak{D}_{K/\mathbb{Q}}^{-1} \\ &\Rightarrow \mathfrak{D}_{K/\mathbb{Q}} \subset \mathfrak{P}^{e-1}, \end{aligned} \tag{231}$$

and we are done. □

Finally, we prove Dedekind's theorem.

Proof. Suppose p ramifies. Write

$$p = \mathfrak{P}^e\mathfrak{a} \tag{232}$$

with $e \geq 2$. By the lemma we just proved,

$$\mathfrak{P}^{e-1} \mid \mathfrak{D}_{K/\mathbb{Q}} \Rightarrow \mathfrak{P} \mid \mathfrak{D}_{K/\mathbb{Q}} \tag{233}$$

since $e \geq 2$. Taking norms of both sides,

$$N\mathfrak{P} \mid N\mathfrak{D}_{K/\mathbb{Q}}. \tag{234}$$

(As an aside,

$$\begin{aligned} \mathfrak{a} \mid \mathfrak{b} &\Rightarrow \mathfrak{b} \subset \mathfrak{a} \\ &\Rightarrow R/\mathfrak{b} \xrightarrow{onto} R/\mathfrak{a} \\ &\Rightarrow \#(R/\mathfrak{a}) \mid \#(R/\mathfrak{b}) \\ &\Rightarrow N\mathfrak{a} \mid N\mathfrak{b}. \end{aligned} \tag{235}$$

shows why taking norms of both sides holds).

Finally, by the lemma from last class, we have

$$p^{f(\mathfrak{P}/p)} \mid |D_{K/\mathbb{Q}}|. \tag{236}$$

□

13.2 Explicit Factorization Theorem

Theorem 13.3

Consider a finite extension $K/\mathbb{Q}$. Suppose $R_K = \mathbb{Z}[\theta]$ for some $\theta \in K$. Let $f(x) \in \mathbb{Z}[x]$ be the minimal polynomial of θ. Let $p \in \mathbb{Z}$ be prime. Consider $\bar{f}(x)$, the reduction of $f(x)$ mod p, and factor it into irreducible factors

$$\bar{f}(x) = \bar{f}_1(x)^{e_1}\bar{f}_2(x)^{e_2}\cdots\bar{f}_r(x)^{e_r} \pmod{p}. \tag{237}$$

Define

$$\mathfrak{P}_i = pR_K + f_i(\theta)R_K. \tag{238}$$

(Note that it doesn't matter how you lift the coefficients of $\bar{f}_i$ to $\mathbb{Z}$, since the pR_K term absorbs any multiples of p). Then,

1. $\mathfrak{P}_i$ are prime ideals in R_K;
2. $N\mathfrak{P}_i = p^{\deg f_i}$; and
3. $pR_K = \mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_n^{e_n}$.

In particular, p ramifies iff its minimal polynomial has a double root mod p, which is true iff the discriminant of its minimal polynomial vanishes.

13.3 Finiteness of the Class Number

Our next goal is to prove the following theorem.

Theorem 13.4

C_K is finite, where $C_K = I_K/P_K$, I_K is the group of fractional ideals, and P_K is the group of principal ideals.

Write $h_K = \#C_K$. This gives the following corollary, which is essentially Lagrange's theorem for groups.

Corollary 13.5

If $\mathfrak{a}$ is any ideal, then $\mathfrak{a}^{h_K}$ is a principal ideal.

We'll now start to prove the theorem. We disguise this by proving a very hard lemma, and then using that to easily prove the theorem.

Lemma 13.6

There is a $\gamma(K)$ such that, for every ideal $\mathfrak{a} \subset R_K$, there is a (non-zero) $\alpha \in \mathfrak{a}$ satisfying

$$|N_{K/\mathbb{Q}}\alpha| \leq \gamma(K) \cdot N_{K/\mathbb{Q}}\mathfrak{a}. \tag{239}$$

We not only want to prove the theorem, but we also want to compute explicitly what $\gamma(K)$ is. This will give us an algorithm to compute the class group? We'll do more next time.

14 Oct. 7, 2016

I got lazy and handwrote.

15 Oct. 10, 2016

No class, school holiday.

16 Oct. 12, 2016

No class, Yom Kippur.

17 Oct. 14, 2016

17.1 Lattices and Fundamental Domains

It's been a long break, so let's refresh. Our goal is to prove that the ideal class group, C_K, is finite. To do this, we need the following lemma.

Lemma 17.1

For all $\mathfrak{a} \subset R_K$, there exists a nonzero $\alpha \in \mathfrak{a}$ with

$$|N\alpha| \leq c_K N\mathfrak{a} \tag{240}$$

for some constant c_K, whose value only depends on K.

We proved that the above lemma implies the finiteness of the class group.

Definition 17.2

A **lattice** $L \subset \mathbb{R}^n$ is a discrete subgroup of maximal rank.

We proved last time that this is equivalent to writing $L = \mathbb{Z}\omega_1 + \ldots + \mathbb{Z}\omega_n$, with the ω_i linearly-independent.

Define the fundamental domain

$$P = \{t_1\omega_1 + \cdots + t_n\omega_n : 0 \leq t_i < 1\}. \tag{241}$$

Note that $P \to \mathbb{R}^n/L$ is a bijection. Note also that, for $n = 2$, $\mathbb{R}^2/L$ looks like a torus, since we can identify the top and bottom edges of the parallelogram, and the left and right edges.

Lemma 17.3

vol(P) does not depend on the choice of basis for L.

Proof. Let ω_i and ω_i' be two ($\mathbb{Z}$)-bases for L. Write

$$\omega_i' = \sum a_{ij}\omega_i \tag{242}$$

for some integers a_{ij}. Let $A = (a_{ij})$. Since the ω_i' are also a basis, A is invertible. Since the entries of A are integers, $\det A = \pm 1$. From basic calculus,

$$\text{vol}(P') = \text{vol}(AP) = |\det A|\,\text{vol}(P) = \text{vol}(P).$$ □

Definition 17.4

The **volume of** L is vol(P).

17.2 Minkowski's Lemma

Our goal in this section is to show that, if $S \subset \mathbb{R}^n$, with sufficient conditions, then S must contain a lattice point.

Theorem 17.5 (Minkowski)

Let $L \subset \mathbb{R}^n$ be a lattice, and $S \subset \mathbb{R}^n$ (Lebesgue-) measurable. Assume $\mu(S) > \text{vol}(L)$. Then, there exist $x, y \in S, x \neq y$ with $x - y \in L$.

Proof. We can write

$$\mathbb{R}^n = \bigcup_{\lambda \in L} P + \lambda, \tag{243}$$

the disjoint union of parallelopipeds with lower-left corners at each lattice point. So,

$$S = \bigcup_{\lambda \in L} S \cap (P + \lambda). \tag{244}$$

Then,

$$\begin{aligned} \mu(S) &= \sum_{\lambda \in L} \mu(S \cap (P + \lambda)) \\ &= \sum_{\lambda \in L} \mu((S - \lambda) \cap P), \text{ since Lebesgue measure is translation invariant.} \end{aligned} \tag{245}$$

Now suppose for the sake of contradiction that the $(S - \lambda) \cap P$ are disjoint for all λ. Then,

$$\begin{aligned} P &\supset \bigcup_{\lambda \in L} ((S - \lambda) \cap P) \\ \implies \mu(P) &\geq \sum_{\lambda \in L} \mu((S - \lambda) \cap P) = \mu(S) \end{aligned} \tag{246}$$

But we assume $\mu(P) < \mu(S)$, so this is a contradiction. Thus, the $(S - \lambda) \cap P$ are not disjoint, so there exist $\lambda_1 \neq \lambda_2$ in L and a point x with

$$x \in (S - \lambda_1) \cap P \tag{247}$$

$$x \in (S - \lambda_2) \cap P. \tag{248}$$

So we can write

$$x = s_1 - \lambda_1 \tag{249}$$

$$x = s_2 - \lambda_2, \tag{250}$$

for $s_1, s_2 \in S$. Subtracting the two, we get that

$$s_2 - s_1 = \lambda_1 - \lambda_1 \neq 0. \tag{251}$$

Thus, we have two points in S whose difference is in L. □

To show that a subset $S \subset \mathbb{R}^n$ contains a lattice point, we need some restrictions on S.

Definition 17.6

Let $S \subset \mathbb{R}^n$. Then we say S is **symmetric** if

$$x \in S \implies -x \in S. \tag{252}$$

We say S is **convex** if

$$x, y \in S \implies \{tx + (1-t)y : 0 \leq t \leq 1\} \subset S. \tag{253}$$

Theorem 17.7

Let $L \subset \mathbb{R}^n$ be a lattice, and let $S \subset \mathbb{R}^n$ be measurable, symmetric, and convex. Then,

(a) If $\mu(S) > 2^n \operatorname{vol}(L)$, then there exists $0 \neq \lambda \in S \cap L$.

(b) If $\mu(S) \geq 2^n \operatorname{vol}(L)$ and S is compact, then we have the same conclusion.

Proof. (a) Consider $S' = \frac{1}{2}S$. Note that $\operatorname{vol}(S') = \frac{1}{2^n}\operatorname{vol}(S) > \operatorname{vol}(L)$. Then, by Minkowski, there exist distinct $\frac{1}{2}x, \frac{1}{2}y$, with $x, y \in S$, and $\frac{1}{2}x - \frac{1}{2}y \in L$. We can write

$$\frac{1}{2}x - \frac{1}{2}y = \frac{1}{2}(x) + \frac{1}{2}(-y). \tag{254}$$

Since S is symmetric, $-y \in S$. Since x is convex, any point on the line between x and $-y$ is in S. Thus, $\frac{1}{2}(x) + \frac{1}{2}(-y) \in S \cap L$.

(b) Let $\epsilon > 0$. Then,

$$\mu((1+\epsilon)S) = (1+\epsilon)^n \mu(S) > 2^n \operatorname{vol}(L), \tag{255}$$

so by the previous part, $(1+\epsilon)S \cap L$ has a non-zero point. By our original definition of a lattice, since $(1+\epsilon)S$ is compact, $(1+\epsilon)S \cap L$ is finite. Consider the set

$$\cap_{\epsilon>0} \left((1+\epsilon)S \cap (L \setminus \{0\}\right). \tag{256}$$

These are finite, non-empty, nested sets (to get a sequence of sets, write $\epsilon = 1/k$). Thus, the intersection is non-empty as well.

Since S is closed, $\cap_{\epsilon>0}(1+\epsilon)S = S$. Therefore, $S \cap (L \setminus \{0\})$ is non-empty, so there exists a non-zero lattice point in S. □

17.3 Back to the class number

Let K be a number field, and let $n = [K : \mathbb{Q}]$. Then, we know there are distinct embeddings

$$\sigma_1, ..., \sigma_n : K \hookrightarrow \mathbb{C}. \tag{257}$$

If $\sigma(K) \subset \mathbb{R}$, we say σ is a **real embedding**. Otherwise, σ is a **complex embedding** ad has a conjugate embedding $\bar{\sigma}$, where $\bar{\sigma}(\alpha) = \sigma(\bar{\alpha})$. Let

$$\sigma_1, ..., \sigma_{r_1} \tag{258}$$

be the real embeddings, let

$$\sigma_{r_1+1}, ..., \sigma_{r_1+r_2} \tag{259}$$

be distinct complex embeddings, and let

$$\bar{\sigma}_{r_1+1}, ..., \bar{\sigma}_{r_1+r_2} \tag{260}$$

be the conjugates of the complex embeddings. Using $\sigma = (\sigma_1, ..., \sigma_{r_1+r_2})$, we can embed

$$K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^{r_1+2r_2} = \mathbb{R}^n. \tag{261}$$

We call σ the **canonical embedding of** K.

18 Oct. 17, 2016

18.1 Computing volumes of ideals

So say $K/\mathbb{Q}$ is an extension of degree n. Let $\sigma_1, ..., \sigma_{r_1}$ be the real embeddings, $\sigma_{r_1+1}, ..., \sigma_{r_1+r_2}$ be the distinct embeddings into $\mathbb{C}$ (i.e. not conjugates). Let

$$\sigma = (\sigma_1, ..., \sigma_{r_1+r_2}) : K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^{r_1+2r_2} = \mathbb{R}^n. \tag{262}$$

Proposition 18.1

Let $\mathfrak{a} \subset K$ be a fractional ideal. Then

(a) $\sigma(\mathfrak{a})$ is a lattice,

(b) Write $\mathfrak{a} = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$. Form the $n \times n$ matrix $(\sigma_i(\alpha_j))$. Then, $\mathrm{vol}(\sigma(\mathfrak{a})) = 2^{-r_2}|\det(\sigma_i(\alpha_j))|$.

Proof. We'll prove (a) later. (We'll in fact estimate how many points there are if we intersect with a compact set). For the second part, recall that we identify $\mathbb{C}$ with $\mathbb{R}^2$ by

$$\mathbb{C} \cong \mathbb{R}^2 \tag{263}$$
$$z \leftrightarrow (\Re(z), \Im(z)) \tag{264}$$
$$= \left(\frac{z+\bar{z}}{2}, \frac{z-\bar{z}}{2}\right). \tag{265}$$

Writing out the matrix $\sigma_i(\alpha_j)$,

$$\begin{pmatrix} \vdots \\ \sigma(\alpha_j) \\ \vdots \\ \bar{\sigma}(\alpha_j) \\ \vdots \end{pmatrix}. \tag{266}$$

Since the determinant is preserved under row operations, the following matrix has the same determinant.

$$\begin{pmatrix} \vdots \\ \sigma(\alpha_j) + \bar{\sigma}(\alpha_j) \\ \vdots \\ \bar{\sigma}(\alpha_j) - \frac{1}{2}(\sigma(\alpha_j) + \bar{\sigma}(\alpha_j)) \\ \vdots \end{pmatrix} = \begin{pmatrix} \vdots \\ \sigma(\alpha_j) + \bar{\sigma}(\alpha_j) \\ \vdots \\ -\frac{1}{2}(\sigma(\alpha_j) - \bar{\sigma}(\alpha_j)) \\ \vdots \end{pmatrix} = \begin{pmatrix} \vdots \\ 2\Re(\alpha_j) \\ \vdots \\ -i\Im(\alpha_j) \\ \vdots \end{pmatrix}. \tag{267}$$

Note that the first r_1 rows have not changed. So we have

$$\det(\sigma_i(\alpha_j)) = (-2i)^{r_2} \cdot \det \left(\begin{array}{c} \sigma_1(\alpha_j) \\ \vdots \\ \sigma_{r_1}(\alpha_j) \\ \hline \Re(\sigma_{r_1+1}(\alpha_j)) \\ \vdots \\ \Re(\sigma_{r_1+r_2}(\alpha_j)) \\ \hline \Im(\sigma_{r_1+1}(\alpha_j)) \\ \vdots \\ \Im(\sigma_{r_1+1}(\alpha_j)) \end{array} \right) \tag{268}$$

$$= (-2i)^{r_2} \cdot |\det(\sigma(\mathfrak{a}))|.$$

Thus, $\mathrm{vol}(\sigma(\mathfrak{a})) = |\det(\sigma(\mathfrak{a}))| = 2^{r_2}|\det(\sigma_i(\alpha_j))|$. □

Proposition 18.2

Let $\sigma : K \hookrightarrow \mathbb{R}^n$, $\alpha \subset R_K$ a non-zero ideal. Then,

(a) $\mathrm{vol}(\sigma(R_K)) = 2^{-r_2} \cdot |D_{K/\mathbb{Q}}|^{1/2}$. (Note that this is why the discriminant is so fundamental! It controls the volume of the fundamental domain of an ideal).

(b) $\mathrm{vol}(\sigma(\mathfrak{a})) = 2^{-r_2} \cdot |D_{K/\mathbb{Q}}|^{1/2} N\mathfrak{a}$.

Proof. Write $R_K = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$. Then,

$$\mathrm{vol}(\sigma(R_K)) = 2^{-r_2}|\det(\sigma_i(\omega_j))|. \tag{269}$$

But we proved before that $|D_{K/\mathbb{Q}}| = (\det(\sigma_i(\omega_j)))^2$, so the result follows.

For b, we note that a fundamental domain for $\mathbb{R}^n/\sigma(\mathfrak{a})$ is

$$\bigcup_{x\in R_K/\mathfrak{a}} (\text{fundamental domain for } (\mathbb{R}^n/\sigma(R_K)) + x). \tag{270}$$

Thus,

$$\operatorname{vol}(\sigma(\mathfrak{a})) = \operatorname{vol}(\sigma(R_K)) \cdot \#(R_K/\mathfrak{a}) = \operatorname{vol}(\sigma(R_K)) \cdot N\mathfrak{a}. \tag{271}$$

(Another way to think of it: the map $\mathbb{R}^n/\sigma(\mathfrak{a}) \to \mathbb{R}^n/\sigma(R_K)$ is $N\mathfrak{a}$-to-1. It is measure-preserving, so the area of the fundamental domain in $\mathbb{R}^n/\sigma(\mathfrak{a})$ is $N\mathfrak{a}$ times the area in $\mathbb{R}^n/\sigma(R_K)$). □

Theorem 18.3

Let $K/\mathbb{Q}$ be an extension of degree $n = r_1 + 2r_2$. There is a constant $C = C(r_1, r_2)$ such that, for all nonzero $\mathfrak{a} \subset R_K$, there is a (nonzero) $\alpha \in \mathfrak{a}$ satisfying

$$|N\alpha| \le C \cdot |D_{K/\mathbb{Q}}|^{1/2} N\mathfrak{a}. \tag{272}$$

As we saw before, this implies C_K is finite.

Proof. Let $\sigma : K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ be our usual map. Then $\sigma(\mathfrak{a})$ is a lattice, and $\operatorname{vol}(\sigma(\mathfrak{a})) = 2^{-r_2}|D_{K/\mathbb{Q}}|^{1/2}N\mathfrak{a}$. We want to use Minkowski's lemma here. So, for $t > 0$, define the region

$$B_t = \left\{(y,z) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} : \sum_{i=1}^{r_2} |y_i| + 2\sum_{i=1}^{r_2} |z_i| \le t\right\}. \tag{273}$$

We note that B_t is

- compact,
- convex (use triangle inequality)
- symmetric.

Its volume is

$$\mu(B_t) = t^n \mu(B_1). \tag{274}$$

Since B_t is compact, choose t such that $\mu(B_t) = t^n\mu(B_1) = 2^n \operatorname{vol}(\sigma(\mathfrak{a}))$. Thus, by Minkowski's, there exists a nonzero $\sigma(\alpha) \in \sigma(\mathfrak{a}) \cap B_t$; that is, a nonzero lattice point in B_t. Then,

$$\begin{aligned} |N\mathfrak{a}| &= \left|\prod_{i=1}^{n} \sigma_i(\alpha)\right| \\ &= \left|\prod_{i=1}^{r_1} \sigma_i(\alpha)\right| \cdot \left|\prod_{i=r_1}^{r_1+r_2} \sigma_i(\alpha)\right|^2 \\ &= |\prod y_i| \cdot |\prod z_i|^2, \end{aligned} \tag{275}$$

where, abusing notation, let $y_i = \sigma_i(\alpha)$ for $i = 1, \ldots, r_1$, and let $z_i = \sigma_i(\alpha)$ for $i > r_1$. We know

$$\sum |y_i| + 2\sum |z_i| \le t. \tag{276}$$

We want to bound $N\mathfrak{a}$, which is the product of the y_i and z_i. We have a bound on the sum of the y_i and z_i, so this suggests using the AM-GM inequality! By AM-GM, we have

$$\left(\left|\prod y_i\right| \cdot \left|\prod z_i\right|^2\right)^{1/n} \le \frac{1}{n}\left(\sum |y_i| + 2\sum |z_i|\right). \tag{277}$$

The above equation implies

$$(N\mathfrak{a})^{1/n} \le \frac{1}{n}t \implies N\mathfrak{a} \le \frac{1}{n^n}t^n. \tag{278}$$

Since we chose a specific value of t, we get

$$|N\alpha| \le \frac{2^{r_1+2r_2}}{\mu(B_1)n^n}|D_{K/\mathbb{Q}}|^{1/2}N\mathfrak{a}. \tag{279}$$

If you do a lot of calculus, you can work out what $\mu(B_1)$ is, and our bound becomes

$$|N\alpha| \le \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n}|D_{K/\mathbb{Q}}|^{1/2}N\mathfrak{a}. \tag{280}$$

(To get a more tractable bound, one can bound $\frac{n!}{n^n}$ using Stirling's). □

Thus, summing up all of our work, we have the following theorem.

Theorem 18.4

Every ideal class in $H_K = I_K/P_K$ contains an ideal $\mathfrak{a} \subset R_K$ satisfying

$$N\mathfrak{a} \le \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}|D_{K/\mathbb{Q}}|^{1/2}. \tag{281}$$

One corollary, which we'll do next time, is that $|D_{K/\mathbb{Q}}| \ge 2$ for all extensions $K/\mathbb{Q}$ with $[K:\mathbb{Q}] \ge 2$.

19 Oct. 19, 2016

19.1 Corollaries of Ideal Bound

Last time, we proved the following.

Theorem 19.1

For all non-zero $\mathfrak{a} \subset R_K$, there exists non-zero $\alpha \in \mathfrak{a}$ with

$$|N\alpha| \le \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}|D_K|^{1/2}N\mathfrak{a}. \tag{282}$$

We have the following corollary.

Corollary 19.2

Every ideal class contains an ideal $\mathfrak{a}$ sayisfying

$$N\mathfrak{a} \le \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}|D_K|^{1/2}. \tag{283}$$

Proof. Let $\bar{\mathfrak{b}}$ be an ideal class. From previous work, we can assume $\mathfrak{b}^{-1} \subset R_K$. By the theorem, there exists non-zero $\gamma \in \mathfrak{b}^{-1}$ with

$$N\gamma \leq C|D_K|^{1/2}N(\mathfrak{b}^{-1}) \Rightarrow N(\gamma\mathfrak{b}) \leq C \cdot |D_K|^{1/2}. \qquad \square$$

Here is another corollary.

Corollary 19.3

Say $n = [K : \mathbb{Q}] \geq 2$. Then

$$|D_K| \geq \frac{\pi}{3} \cdot \left(\frac{3\pi}{4}\right)^{n-1}. \tag{284}$$

Further, this implies that if $[K : \mathbb{Q}] \geq 2$, then there exists at least one prime $p \in \mathbb{Z}$ that ramifies in K.

Proof. The second statement clearly follows from the first, since the first implies $|D_K| > 1$ and we know p ramifies iff $p \mid |D_K|$.

For the first statement, we use the previous corollary. Since $N\mathfrak{a} \geq 1$, we get

$$\begin{aligned} |D_K| &\geq \left(\frac{\pi}{4}\right)^{2r_2} \cdot \left(\frac{n^n}{n!}\right)^2 \\ &\geq \left(\frac{\pi}{4}\right)^{n} \cdot \left(\frac{n^n}{n!}\right)^2, \end{aligned} \tag{285}$$

where we use, $r_1 + 2r_2 = n$, we have $2r_2 \leq n$.

As an aside, note that, for large n, we could use Stirling's approximation,

$$n! \sim \left(\frac{n}{e}\right)^n \sqrt{2\pi n}, \tag{286}$$

and get

$$D_K \geq \left(\frac{\pi}{4}\right)^n e^{2n}\frac{1}{2\pi n} = \frac{1}{2\pi n}\left(\frac{\pi e^2}{4}\right)^n \tag{287}$$

asymptotically.

Back to the proof. Let $A_n = \left(\frac{\pi}{4}\right)^n \cdot \left(\frac{n^n}{n!}\right)^2$. We want to show

$$A_n \geq \frac{\pi}{3} \cdot \left(\frac{3\pi}{4}\right)^{n-1}. \tag{288}$$

This is mostly algebra. Inductively, we compute

$$\begin{aligned} \frac{A_{n+1}}{(\pi/3)(3\pi/4)^n} &= \frac{\frac{\pi}{4}(1+\frac{1}{n})^{2n}A_n}{\frac{\pi}{3}\left(\frac{3\pi}{4}\right)^n} \\ &\geq \frac{\frac{\pi}{4}(1+\frac{1}{n})^{2n} \cdot \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}}{\frac{\pi}{3}\left(\frac{3\pi}{4}\right)^n} \\ &= \frac{1}{3}\left(1+\frac{1}{n}\right)^{2n} \\ &\geq \frac{1}{3}\left(1+\frac{1}{2}\right)^{4} \\ &> 1. \end{aligned} \qquad \square$$

Corollary 19.4 (Hermite)
Fix T. Then, $F_T := \{K/\mathbb{Q} : |D_K| \leq T\}$ is finite.

Proof. If $K \in F_T$, then,

$$T \geq D_K \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}. \tag{289}$$

This implies there are only finitely many choices for n, which in turn implies there are only finitely many choices for r_1 and r_2. So it suffices to show that

$$F_{T,r_1,r_2} := \{K/\mathbb{Q} : |D_K| \leq T, r_1(K) = r_1, r_2(K) = r_2\} \tag{290}$$

is finite.

Our strategy is to find a finite set $\{\beta_1, ..., \beta_n\}$, where $\mathbb{Q}(\beta_i)$ is one set in F_{T,r_1,r_2}. We will do this using the geometry of numbers. For simplicity, we assume $r_1 \geq 1$ (if not, will have to modify argument).

Let $K \in F_{T,r_1,r_2}$. Consider the set

$$\begin{aligned} S = \{(y,z) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} : |y_1| \leq \frac{1}{2} \cdot 2^n \left(\frac{\pi}{2}\right)^{-r_2} |D_K|^{1/2}, \\ |y_2|, ..., |y_{r_1}| \leq \frac{1}{2} \\ |z_1|, ..., |z_{r_2}| \leq \frac{1}{2}\}. \end{aligned} \tag{291}$$

S is compact (closed, bounded), convex (triangle inequality), and symmetric. Its volume is

$$\begin{aligned} \text{vol}(S) &= \left(2 \cdot \frac{1}{2} 2^n \left(\frac{\pi}{2}\right)^{-r_2} |D_K|^{1/2}\right) \cdot \left(2 \cdot \frac{1}{2}\right)^{r_1 - 1} \cdot \left(\frac{\pi}{4}\right)^{r_2} \\ &= 2^n 2^{-r_2} |D_{K/\mathbb{Q}}|^{1/2} \\ &= 2^n \text{ vol}(R_K). \end{aligned} \tag{292}$$

Let $\sigma = (\sigma_1, ..., \sigma_{r_1+r_2}) : K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. By MInkowski's, there exists $0 \neq \beta \in R_K$ with

$$\sigma(\beta) \in \sigma(R_K) \cap S. \tag{293}$$

Claim 19.5. $K = \mathbb{Q}(\beta)$.

Claim 19.6. $\{\beta_K : K \in F_{T,r_1,r_2}\}$ is finite.

To prove the first claim, since $\sigma(\beta) \in S$, we have

$$|\sigma_2(\beta)|, \ldots, |\sigma_{r_1+r_2}(\beta)| \leq \frac{1}{2}. \tag{294}$$

We also have

$$\left|\prod_{i=1}^{r_1+r_2} \sigma_i(\beta)\right| = N\beta \geq 1. \tag{295}$$

This implies $\sigma_1(\beta) \neq \sigma_i(\beta)$ for $i > 1$, since otherwise $N\beta$ would be less than 1. I claim in fact that $\sigma_i(\beta) \neq \sigma_j(\beta)$ for $i \neq j$. This is something we should check on our own.

So assume the $\sigma_1(\beta), \ldots, \sigma_{r_1+r_2}(\beta)$ are distinct. This implies $[\mathbb{Q}(\beta) : \mathbb{Q}] \geq n$, since it has at least n distinct embeddings. But since $\mathbb{Q}(\beta)$ is a subfield of K, and $[K : \mathbb{Q}] = n$, it follows that $K = \mathbb{Q}(\beta)$.

For the second claim, we need the following theorem.

Theorem 19.7

Say $[K : \mathbb{Q}] = n$, and let $\sigma_1, \ldots, \sigma_n : K \hookrightarrow \mathbb{C}$ be distinct embeddings. Then,

$$\{\alpha \in R_K : |\sigma_i(\alpha)| \leq B \text{ for all } 1 \leq i \leq n\} \tag{296}$$

is finite.

Proof. Using σ_1, we have $K \subset \mathbb{C}$. Look at the polynomial

$$F_\beta(x) = \prod_{i=1}^{n}(x - \sigma_i(\beta)), \tag{297}$$

where $F_\beta(\beta) = 0$. Expanding out F_β gives

$$F_\beta(x) = \sum_{j=0}^{n}(-1)^{n-j} S_j x^{n-j} \tag{298}$$

where S_j is the jth symmetric polynomial in $\sigma_1(\beta), \ldots, \sigma_n(\beta)$. Thus, S_j is $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ invariant, so $S_j \in \mathbb{Q}$. Furthermore, the S_j are integral over $\mathbb{Z}$, since each $\sigma_i(\beta) \in R_K$. Thus, $S_j \in \mathbb{Z}$.

Not enough time to finish the proof now, but the next step is to prove that $|S_j| \leq (2B)^n$. Since the S_j are integers, there will only be finitely many possibilities. We'll finish this theorem, and the second corollary, next time.

20 Oct. 21, 2016

20.1 Continuing corollaries from last time

We were proving the following theorem last time.

Theorem 20.1

Let K be an extension of $\mathbb{Q}$, with $[K : \mathbb{Q}] = n$, and let $\sigma_1, \ldots, \sigma_n : K \hookrightarrow \mathbb{C}$ be distinct embeddings. Then,

$$S_B = \{\alpha \in R_K : |\sigma_i(\alpha)| \leq B \text{ for } 1 \leq i \leq n\}. \tag{299}$$

is a finite set. (Assume $B \geq 1$).

Proof. Use σ_1 to identify $K \subset \mathbb{C}$. Last time, we looked at the polynomial

$$F_\alpha(x) = \prod_{i=1}^{n}(x - \sigma_i(\alpha)). \tag{300}$$

We proved last time that $F_\alpha(x) \in \mathbb{Z}[x]$. We also have

$$F_\alpha(x) = \sum_{j=1}^{n}(-1)^{n-j} S_j \cdot x^{n-j} \tag{301}$$

where S_j is the jth symmetric polynomial. We bound S_j below.

$$\begin{aligned} |S_j| &= |S_j(\sigma_1(\alpha), \ldots, \sigma_n(\alpha))| \\ &\leq \sum_{1<i_1<\ldots<i_j<n} |\sigma_{i_1}(\alpha)\cdots\sigma_{i_j}(\alpha)| \\ &\leq \sum_{1<i_1<\ldots<i_j<n} B^j \\ &= \binom{n}{j} B^j \\ &\leq 2^n B^n = (2B)^n. \end{aligned} \tag{302}$$

Thus,

$$S_B \subset \{\text{roots of polynomials in } \mathbb{Z}[x] \text{ with } |a_i| \leq (2B)^n\}. \tag{303}$$

There are only finitely many integers less than $(2B)^n$, so there are only finitely many such polynomials. Each polynomial has at most n roots, so it follows that the RHS is finite. □

Note that this proves the theorem from last time: that there are finitely many fields extensions (of $\mathbb{Q}$) of bounded discriminant.

Corollary 20.2 (Kronecker)
$|\sigma_i(\alpha)| = 1$ for all $1 \leq i \leq n$ iff α is a root of unity.

Proof. One direction is straightforward: $\alpha^n = 1$, then $|\sigma_i(\alpha)|^n = 1^n = 1$. For the other direction, suppose $|\sigma_i(\alpha)| = 1$ for all i. Then, for all $k \geq 1$,

$$|\sigma_i(\alpha^k)| = |\sigma_i(\alpha)|^k = 1. \tag{304}$$

Thus,

$$\{\alpha^k : k \geq 1\} \subset \{\beta : |\sigma_i(\beta)| \leq 1 \text{ for all } 1 \leq i \leq n\}. \tag{305}$$

By the previous corollary, the RHS is finite. Thus, the LHS is finite, so for some k_1, k_2 we have

$$\alpha^{k_1} = \alpha^{k_2}. \tag{306}$$

Thus α is a root of unity. □

20.2 Dirichlet's Unit Theorem

Theorem 20.3
Let $K/\mathbb{Q}$ be an extension, with $r_1 + 2r_2 = n = [K : \mathbb{Q}]$. Then, R_K^* is a finitely-generated abelian grop of rank $r_1 + r_2 - 1$. Additionally, if we write

$$R_K^* \equiv (\text{finite group}) \times \mathbb{Z}^{r_1+r_2-1}, \tag{307}$$

then the finite group is cyclic.

To prove this, we first prove the following lemma.

Lemma 20.4

Let $\alpha \in K$. Then,

$$\alpha \in R_K^* \iff N\alpha = \pm 1, \text{ and } \alpha \in R_K. \tag{308}$$

Proof. Suppose $\alpha \in R_K^*$. Then, there exists $\beta \in R_K^*$ with $\alpha\beta = 1$. Taking norms of both sides, $N\alpha \cdot N\beta = 1$. Since $\alpha, \beta \in R_K$, both $N\alpha$ and $N\beta$ are integers, so we must have $N\alpha = \pm 1$.

Next, suppose $\alpha \in R_K$ and $N\alpha = \pm 1$. Let

$$x^n + a_1 x^{n-1} \cdots + a_n \in \mathbb{Z}[x] \tag{309}$$

be the minimal polynomial of α. We have $a_n = \pm N\alpha = \pm 1$, so

$$\begin{aligned} \alpha^n + a_1\alpha^{n-1} + \cdots + a_{n-1}\alpha \pm 1 = 0 \\ \Rightarrow \alpha(\alpha^{n-1} + \cdots + a_{n-1}) = \pm 1. \end{aligned} \tag{310}$$

□

Now, armed with this lemma, we prove Dirichlet.

Proof of Dirichlet. To show that R_K^* is finitely-generated, our idea is to embed R_K^* into $\mathbb{R}^N$ for some N. But this is not possible if R_K has an element of finite order. So let's try and embed R_K^*/torsion subgp. into $\mathbb{R}^N$.

Let $\sigma_1, ..., \sigma_{r_1}$ be the real embeddings, and $\sigma_{r_1+1}, ..., \sigma_{r_1+r_2}$ be the distinct (non-conjugate) complex embeddings.

Before, we had the map

$$K \xrightarrow{\sigma} \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}. \tag{311}$$

This respected addition in K, but not multiplication. We could change K to K^*, but we need the image, in $\mathbb{R}^x \times \mathbb{C}^y$, to respect addition. So instead, let's use logs, which change multiplication to addition.

Formally, define

$$L : K^* \to \mathbb{R}^{r_1+r_2} \tag{312}$$

$$\alpha \mapsto (\log(\sigma_1(\alpha)), ..., \log(\sigma_{r_1+r_2}(\alpha))). \tag{313}$$

$L : R_K^* \to \mathbb{R}^{r_1+r_2}$ is a homomorphism.

Claim 20.5. Im(L) is discrete. Hence, $L(R_K^*)$ is finitely generated, of rank $\leq r_1 + r_2$.

Proof. Define

$$D_B = \{v \in \mathbb{R}^{r_1+r_2} : |v_i| \leq B\}, \tag{314}$$

a box of size B. Consider the set

$$L(R_K^*) \cap D_B. \tag{315}$$

We want to show this set is finite, as this implies that $L(R_K^*)$ intersects compact subsets in at most finitely many points.

Let $v \in L(R_K^*) \cap D_B$. Write $v = L(\alpha)$ for some $\alpha \in R_K^*$. Then,

$$\log \sigma_i(\alpha) \leq B \tag{316}$$

for all $i = 1, ..., n$. So,

$$L(R_K^*) \cap D_B \subset L(\{\alpha \in R_K^* : |\sigma_i(\alpha)| \leq e^B \text{ for all } i\}). \tag{317}$$

From our previous result, the RHS is finite. Thus, the LHS is finite, so $L(R_K^*)$ is discrete.

Claim 20.6. $\ker(L : R_K^* \to \mathbb{R}^{r_1+r_2}) = \{\text{roots of unity in } K^*\}$.

Proof. Suppose $\zeta^m = 1$. Then $|\sigma_i(\zeta)| = 1$ for all i, so $L(\zeta) = 0$.

For the other direction, suppose $\alpha \in \ker(L) \cap R_K^*$. Then,

$$\log|\sigma_i(\alpha)| = 0 \implies |\sigma_i(\alpha)| = 1 \tag{318}$$

for all $i = 1, \ldots, n$. By Kronecker's, α is a root of unity.

Thus, by the claims, we have the exact sequence.

$$1 \to \text{ roots of unity in } K^* \to R_K^* \xrightarrow{L} \text{discrete subgp. of } \mathbb{R}^{r_1+r_2} \to 0. \tag{319}$$

Now, what is $\operatorname{rank} R_K^* = \operatorname{rank} L(R_K^*)$? If we try an example, say with a quadratic extension, we see $r_1 + r_2$ is too big.

Say $\alpha \in R_K^*$, so $|N\alpha| = 1$. This implies

$$1 = \prod_{i=1}^{r_1} |\sigma_i(\alpha)| \prod_{i=r_1+1}^{r_1+r_2} |\sigma_i(\alpha)|^2. \tag{320}$$

Taking log of both sides, we get

$$0 = \sum_{i=1}^{r_1} \log|\sigma_i(\alpha)| + 2 \sum_{i=r_1+1}^{r_1+r_2} \log|\sigma_i(\alpha)| \tag{321}$$

Now, $\log|\sigma_i(\alpha)|$ are the coordinates of $L(\alpha)$. So the coordinates of $L(\alpha)$ satisfy the above linear equation. Writing this out,

$$L(R_K^*) \subset \{y \in \mathbb{R}^{r_1+r_2} : y_1 + \cdots + y_{r_1} + 2(y_{r_1+1} + \cdots + y_{r_1+r_2}) = 0\} \equiv \mathbb{R}^{r_1+r_2-1}. \tag{322}$$

Thus, $L(R_K^*)$ is discrete, and $\operatorname{rank} L(R_K^*) \le r := r_1 + r_2 - 1$. Thus, our final step is to show equality. Somehow, we need to create lots of multiplicatively independent units in R_K^*. The idea, which we'll get to next time, is to create lots of principal ideals $\alpha_i R_K$ of "bounded size." By pigeonhole, we'll show that two of the ideals we created are the same, so that

$$\alpha_i R = \alpha_j R, \tag{323}$$

so that $\alpha_i/\alpha_j \in R_K^*$. We'll also need to talk about the dual space of $L(R_K^*)$, which is the group of functionals $f : L(R_K^*) \to \mathbb{R}$.

21 Oct. 24, 2016

Handwrote

22 Oct. 26, 2016

22.1 Cyclotomic units

Example 22.1

Suppose $K = \mathbb{Q}(\zeta_p)$, $p \geq 3$. Then, $r_1 = 0$, since none of the roots of unity are real, and $r_2 = \frac{p-1}{2}$, so

$$\operatorname{rank} \mathbb{Z}[\zeta_p] = \frac{p-3}{2}. \tag{324}$$

Note that for $p = 3$, the rank is 0, which makes sense, since $\mathbb{Q}(\zeta_3)$ is a quadratic extension.

Below are some facts about cyclotomic units. We won't prove them, and they're hard to show.

Proposition 22.2

$\frac{\zeta_i - 1}{\zeta^j - 1} \in \mathbb{Z}[\zeta_p]^*$ for $0 < i, j < p$. Call these quantities **cyclotomic units**.

Let C be the subgroup of $\mathbb{Z}[\zeta_p]^*$ generated by cyclotomic units.

Theorem 22.3

The following two facts are true.

1. C is a subgroup of finite index in $\mathbb{Z}[\zeta_p]^*$.
2. $(\mathbb{Z}[\zeta_p]^* : C)$ is approximately the class number of $\mathbb{Q}(\zeta_p)$.

22.2 Regulator

Suppose $\sigma : R_K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Then, $\operatorname{vol}(\sigma(R_K)) \sim |D_K|^{1/2}$. Now, this induces a map

$$L : R_K^* \hookrightarrow H \subset \mathbb{R}^{r_1 + r_2} \tag{325}$$

for some hyperplane H.

Definition 22.4

The **regulator of** K is $\operatorname{Reg}(K) = \operatorname{vol}(L(R_K^*)$ in $H)$.

Let $u_1, \ldots, u_r \in R_K^*$ be independent units, where $r = r_1 + r_2 - 1$. Let $\sigma_1, \ldots, \sigma_{r+1}$ be distinct (non-conjugate) embeddings. Then,

$$\operatorname{Reg}(K) = \left| \det \begin{pmatrix} \log|\sigma_1(u_1)| & \cdots & 2\log|\sigma_1(u_r)| \\ \vdots & & \vdots \\ \log|\sigma_r(u_1)| & \cdots & 2\log|\sigma_r(u_r)| \end{pmatrix} \right|. \tag{326}$$

22.3 Localization and Dirichlet's S-unit Theorem

Let S be a finite set of primes of R_K. Let $R_{K,S}$ be the localization of R_K at S. That is,

$$R_{K,S} = \{\alpha \in K : \operatorname{ord}_{\mathfrak{p}}(\alpha) \geq 0 \text{ for all } \mathfrak{p} \in S\}. \tag{327}$$

If $\alpha R_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, then $\operatorname{ord}_{\mathfrak{p}}(\alpha)$ is the exponent of $\mathfrak{p}$ in αR_K.

Theorem 22.5 (Dirichlet's S-unit Theorem)
$R^*_{K,S} = \mu_K \times \mathbb{Z}^{r_1+r_2+|S|-1}$, where μ_K is the roots of unity of K.

Example 22.6
Say $K = \mathbb{Q}, S = \{p_1, ..., p_t\}$. Then, $\mathbb{Z}_S = \mathbb{Z}[\frac{1}{p_1}, ..., \frac{1}{p_t}]$, and

$$\mathbb{Z}^*_S = \{\pm 1\} \times (\text{group generated by } p_1, ..., p_t). \tag{328}$$

22.4 Galois Theory and Algebraic Number Theory

Example 22.7
Say $\operatorname{char} K \neq 2$, and $[L : K] = 2$. Then by the quadratic formula, $L = K(\sqrt{d})$. $G(L/K) = \{1, \sigma\}$, where $\sigma(\sqrt{d}) = -\sqrt{d}$.

Example 22.8
Say $\operatorname{char} K = 0$ or p, with $p \nmid n$. Consider the extension $K(\zeta_n)/K$. We have the map

$$K(\zeta_n)/K \longrightarrow (\mathbb{Z}/n\mathbb{Z})^* \tag{329}$$

$$\sigma \mapsto i(\sigma) \pmod{n}, \text{ where } i(\sigma) \text{ is such that } \sigma(\zeta_n) = \zeta_n^{i(\sigma)}. \tag{330}$$

Example 22.9
Finite fields. (Why is this important? If we have a number field K and a prime ideal $\mathfrak{p}$, then $R_K/\mathfrak{p}$ is a finite field; it's a field since $\mathfrak{p}$ is prime, and we showed before that it's finite for any ideal).

Recall that, for each prime power q, there is a unique field $\mathbb{F}_q$ with $\#\mathbb{F}_q = q$. We have

$$\mathbb{F}_{q^m} \subset \mathbb{F}_{q^n} \iff m \mid n. \tag{331}$$

We also have $G(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$, so $G(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is generated by the map $\sigma_q(\alpha) = \alpha^q$. Then, $\sigma_q^k = \sigma_{q^k}$. The map σ_q is called the (q-power) Frobenius map.

Our **goal** for this section is as follows. Let $K/\mathbb{Q}$ be Galois (if your number field isn't Galois, you can find some Galois extension). Take $\mathfrak{p} \subset R_K$. Then there exists $\sigma \in G(K/\mathbb{Q})$ that "looks like" Frobenius for $\mathfrak{p}$. That is,

$$\sigma(\alpha) \equiv \alpha^{N\mathfrak{p}} \pmod{\mathfrak{p}} \tag{332}$$

for all $\alpha \in R_K$.

22.5 Starting to prove Galois theory facts

Let $L/K/\mathbb{Q}$ be extensions, with L/K Galois. Then $R_K \subset R_L$. Let $G = G(L/K)$.

Proposition 22.10

Let $\sigma \in G$. Then,

(a) $\sigma(R_L) = R_L$,

(b) Let $\mathcal{P} \mid \mathfrak{p}$, where $\mathfrak{p} \subset R_K, \mathcal{P} \subset R_L$. Then, $\sigma(\mathcal{P}) \mid \mathfrak{p}$.

Proof. For the first part, let $\alpha \in R_L$. Then, α is a root of monic polynomial $f(x) = \sum a_i x^i$, so $\sigma(\alpha)$ is a root of $\sum \sigma(a_i)x^i = f(x)$, since σ fixes $\mathbb{Q}$. Thus, $\sigma(\alpha)$ is integral, so $\sigma(\alpha) \in R_L$.

For the second part, we have

$$\begin{aligned} \mathcal{P} \mid \mathfrak{p} &\Rightarrow \mathfrak{p}R_L = \mathcal{P}\mathfrak{a}, \text{ for some } \mathfrak{a} \\ &\Rightarrow \sigma(\mathfrak{p}R_L) = \sigma(\mathcal{P})\sigma(\mathfrak{a}) \\ &\Rightarrow \mathfrak{p}R_L = \sigma(\mathcal{P})\sigma(\mathfrak{a}), \text{ since } \sigma \text{ fixes } \mathfrak{p} \text{ and } R_L, \\ &\Rightarrow \sigma(\mathcal{P}) \mid \mathfrak{p}. \end{aligned}$$

□

Notice that we have the isomorphism

$$\begin{aligned} R_L/\mathcal{P} &\to R_L/\sigma(\mathcal{P}) \\ \bar{\alpha} &\mapsto \sigma(\bar{\alpha}). \end{aligned}$$

Now, write

$$\mathfrak{p}R_K = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_r}, \tag{333}$$

with $\sum_{i=1}^r e_i f_i = n$, where $f_i = [R_L/\mathcal{P}_i : R_K/\mathfrak{p}]$. Then, $\sigma \in G$ permutes $\mathcal{P}_1, ..., \mathcal{P}_r$. Let $\mathcal{P} \mid \mathfrak{p}$. We have

$$f(\sigma(\mathcal{P})/\mathfrak{p}) = f(\mathcal{P}/\mathfrak{p}) \tag{334}$$

$$e(\sigma(\mathcal{P})/\mathfrak{p}) = e(\mathcal{P}/\mathfrak{p}) \tag{335}$$

The first equation follows from $R_L/\mathcal{P} \equiv R_L/\sigma(\mathcal{P})$. For the second one, note that if $\mathcal{P} \mid \mathfrak{p}$ and $\sigma(\mathcal{P}) \mid \mathfrak{p}$, then $\mathfrak{p}' = \mathfrak{p} \cdot \mathcal{P}^{-1} \cdot \sigma(\mathcal{P})^{-1}$ is a proper ideal. As long as we can keep dividing by $\mathcal{P}$, we can also keep dividing by $\sigma(\mathcal{P})^{-1}$, so the second statement follows.

Theorem 22.11

$G(L/K)$ acts transitively on the primes $\mathcal{P} \mid \mathfrak{p}$. This means that, for all i, j, there exists $\sigma \in G(L/K)$ with $\sigma(\mathcal{P}_i) = \mathcal{P}_j$.

We don't have time to prove this theorem, but here's a corollary.

Corollary 22.12

If L/K Galois, then

$$\mathfrak{p}R_L = (\mathcal{P}_1 \cdots \mathcal{P}_r)^e, \tag{336}$$

with $f(\mathcal{P}_i/\mathfrak{p}) = f$ the same. In particular,

$$efr = n = [L : K]. \tag{337}$$

23 Oct. 28, 2016

Got lazy and handwrote.

24 Oct. 31, 2016

24.1 Finishing proof of decomposition group isomorphism

Our current diagram

$$\begin{tikzcd}
L \arrow[r, hook] \arrow[d, dash] & R_L \arrow[d, dash] & \mathcal{P} \arrow[d, dash] & \mathbb{F}_{\mathcal{P}} \arrow[d, dash] \\
K \arrow[r, hook] & R_K & \mathfrak{p} & \mathbb{F}_{\mathfrak{p}}
\end{tikzcd}$$

We defined

$$D_{\mathcal{P}} = \{\sigma \in G : \sigma(\mathcal{P}) = \mathcal{P}\} \tag{338}$$

$$I_{\mathcal{P}} = \{\sigma \in G : \sigma(\alpha) = \alpha \pmod{\mathcal{P}} \text{ for all } \alpha \in R_L\} \tag{339}$$

We get a map $D_{\mathcal{P}} \to G(\mathbb{F}_{\mathcal{P}}/\mathbb{F}_{\mathfrak{p}})$. The kernel of this map is $I_{\mathcal{P}}$. We will show that this map is surjective.

Proof. Let K_D be the fixed field of $D_{\mathcal{P}}$ (or $L^{D_{\mathcal{P}}}$). That is,

$$K_D = \{\alpha \in L : \sigma(\alpha) = \alpha \text{ for all } \sigma \in D_{\mathcal{P}}\}. \tag{340}$$

Also, let R_D be the ring of integers of K_D, $\mathcal{P}_D = R_D \cap \mathcal{P}$, and $\mathbb{F}_D = R_D/\mathcal{P}_D$.

Claim 24.1. $\mathbb{F}_{\mathfrak{p}} \to \mathbb{F}_D$ is an isomorphism. ($\mathbb{F}_{\mathfrak{p}} \subset \mathbb{F}_D$).

Proof. Since $\mathcal{P}_D \subset \mathcal{P}$, factoring $\mathcal{P}_D$ in R_L,

$$\mathcal{P}_D R_L = (\sigma_1(\mathcal{P}) \cdot \sigma_r(\mathcal{P}))^{e(\mathcal{P}/\mathcal{P}_D)} \tag{341}$$

where $\sigma_1(\mathcal{P}), \ldots, \sigma_r(\mathcal{P})$ are the distinct conjugates of $\mathcal{P}$ for $\sigma \in G(L/K_D) = D_{\mathcal{P}}$. But by definition, the image of $\mathcal{P}$ in $D_{\mathcal{P}}$ is $\mathcal{P}$, so

$$\mathcal{P}_D R_L = \mathcal{P}^{e(\mathcal{P}/\mathcal{P}_D)}. \tag{342}$$

By the ref theorem,

$$[L : K_D] = e(\mathcal{P}/\mathcal{P}_D) \cdot f(\mathcal{P}/\mathcal{P}_D) = e(\mathcal{P}/\mathcal{P}_D) \cdot [\mathbb{F}_{\mathcal{P}} : \mathbb{F}_D]. \tag{343}$$

On the other hand, $[L : K_D] = \# D_{\mathcal{P}}$ by Galois theory. From last time, we have

$$\# D_{\mathcal{P}} = e(\mathcal{P}/\mathfrak{p}) \cdot f(\mathcal{P}/\mathfrak{p}) = e(\mathcal{P}/\mathfrak{p}) \cdot [\mathbb{F}_{\mathcal{P}} : \mathbb{F}_{\mathfrak{p}}]. \tag{344}$$

Thus,

$$e(\mathcal{P}/\mathcal{P}_D) \cdot f(\mathcal{P}/\mathcal{P}_D) = e(\mathcal{P}/\mathfrak{p}) \cdot f(\mathcal{P}/\mathfrak{p}) \tag{345}$$

Now, since $\mathbb{F}_{\mathfrak{p}} \subset \mathbb{F}_D \subset \mathbb{F}_{\mathcal{P}}$, we have

$$f(\mathcal{P}/\mathfrak{p}) \geq f(\mathcal{P}/\mathcal{P}_D). \tag{346}$$

Finally, we can factor $\mathfrak{p}$ in R_D as

$$\mathfrak{p}R_D = \mathcal{P}_D^{e(\mathcal{P}_D/\mathfrak{p})} \cdot \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_s^{e_s}. \tag{347}$$

Note that, since K_D is not necessarily Galois over K, we cannot assume all the primes have the same exponent. Factoring $\mathfrak{p}$ in R_L gives us

$$\mathfrak{p}R_L = \mathcal{P}^{e(\mathcal{P}/\mathfrak{p})} \cdot (\text{other primes}). \tag{348}$$

Now, we could have first factored $\mathfrak{p}$ in R_D, and then moved that factorization up to R_L. Thus,

$$\mathfrak{p}R_L = \mathcal{P}_D^{e(\mathcal{P}_D/\mathfrak{p})} \cdot (\text{other primes}) = \mathcal{P}^{e(\mathcal{P}_d/\mathfrak{p}) \cdot e(\mathcal{P}/\mathcal{P}_D)} \cdot (\text{other primes}). \tag{349}$$

Comparing exponents, we get

$$e(\mathcal{P}/\mathfrak{p}) = e(\mathcal{P}_d/\mathfrak{p}) \cdot e(\mathcal{P}/\mathcal{P}_D). \tag{350}$$

(This is a tower law for e!, f follows one as well, by finite fields results). In particular, this implies $e(\mathcal{P}/\mathfrak{p}) \geq e(\mathcal{P}/\mathcal{P}_D)$. Now, each term on the RHS of 345 is greater than the LHS term. But since their product is equal, this implies $e(\mathcal{P}/\mathcal{P}_D) = e(\mathcal{P}/\mathfrak{p})$ and $f(\mathcal{P}/\mathcal{P}_D) = f(\mathcal{P}/\mathfrak{p})$.

Thus, $[\mathbb{F}_D : \mathbb{F}_\mathfrak{p}] = 1$, so $\mathbb{F}_\mathfrak{p} \hookrightarrow \mathbb{F}_D$ is an isomorphism. □

Now, back to the theorem. Recall the primitive element theorem: if L is a separable extension of K, we can write $L = K(\alpha)$ for some $\alpha \in L$. So we can choose $\alpha \in R_L$ with $\mathbb{F}_\mathcal{P} = \mathbb{F}_\mathfrak{p}(\bar{\alpha}_p)$, where $\bar{\alpha} = \alpha \pmod{\mathcal{P}}$ in $\mathbb{F}_\mathcal{P}$. Now let

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in R_L[x] \tag{351}$$

be the minimal polynomial of α over K_D. We can also write

$$f(x) = \prod_{\sigma \in G(L/K_D)/\sigma \text{that fix } \alpha} (x - \sigma(\alpha)) = \prod_{\sigma \text{ in some subset of } D_\mathcal{P}} (x - \sigma(\alpha)) \tag{352}$$

since $G(L/K_D) = D_\mathcal{P}$. Reducing this mod $\mathcal{P}$, we get

$$\begin{aligned} \bar{f}(x) &= \sum_{i=1}^{n} \bar{a}_i x^i \in \mathbb{F}_{\mathcal{P}_D}[x] \\ &= \prod_{\sigma \text{ in some subset of } D_\mathcal{P}} (x - \bar{\sigma(\alpha)}) \end{aligned} \tag{353}$$

We also know that $\bar{f}(\bar{\alpha}) = 0$. Thus,

$$(\text{min. poly of } \bar{\alpha} \text{ over } \mathbb{F}_{\mathcal{P}_D}) \mid \bar{f}(x). \tag{354}$$

By field theory, the roots of the LHS are the $G(\mathbb{F}_\mathcal{P}/\mathbb{F}_{\mathcal{P}_D})$ conjugates of α. Thus, every $G(\mathbb{F}_\mathcal{P}/\mathbb{F}_{\mathcal{P}_D})$ conjugate has the form $\bar{\sigma(\alpha)}$ for some $\sigma \in D_\mathcal{P}$, so every element of $G(\mathbb{F}_\mathcal{P}/\mathbb{F}_D)$ has the form $\bar{\sigma}$ for some $\sigma \in D_\mathcal{P}$. Thus,

$$D_\mathcal{P} \to G(\mathbb{F}_\mathcal{P}/\mathbb{F}_D) \tag{355}$$

is onto. By our claim, $G(\mathbb{F}_\mathcal{P}/\mathbb{F}_D) = G(\mathbb{F}_\mathcal{P}/\mathbb{F}_\mathfrak{p})$, so we are done. □

Corollary 24.2

Consider the diagram

$$\begin{tikzcd} L \arrow[r, hook] \arrow[d, dash] & \mathcal{P}_1, \ldots, \mathcal{P}_r \arrow[d, dash] \\ K \arrow[r, hook] & \mathfrak{p}. \end{tikzcd}$$

Then, $\mathfrak{p}$ ramifies in L iff there is some $\mathcal{P} \mid \mathfrak{p}$ with $I_{\mathcal{P}/\mathfrak{p}} \neq 1$, which is true iff every $\mathcal{P} \mid \mathfrak{p}$ has $I_{\mathcal{P}/\mathfrak{p}} \neq 1$.

Proof. We showed that $\#I(\mathcal{P}/\mathfrak{p}) = e(\mathcal{P}/\mathfrak{p})$, which implies the first statement. For the second part, we note that

$$I(\tau\mathcal{P}/\mathfrak{p}) = \tau^{-1}I(\mathcal{P}/\mathfrak{p})\tau, \tag{356}$$

so if $I(\mathcal{P}/\mathfrak{p}) \neq 1$ for one $\mathcal{P}$, then $I(\mathcal{P}/\mathfrak{p}) \neq 1$ for all $\mathcal{P}$. □

24.2 Abelian Galois groups

We also make the following (important!) observation. If L/K is abelian (so $G(L/K)$ is abelian), then $D(\mathcal{P}/\mathfrak{p})$ and $I(\mathcal{P}/\mathfrak{p})$ only depend on $\mathfrak{p}$. This is because

$$D(\tau(\mathcal{P})/\mathfrak{p}) = \tau^{-1}D(\mathcal{P}/\mathfrak{p})\tau = D(\mathcal{P}/\mathfrak{p}) \tag{357}$$

using commutativity (as L/K is abelian). Similarly, $I(\tau(\mathcal{P})/\mathfrak{p}) = T(\mathcal{P}/\mathfrak{p})$.

24.3 Primes that don't ramify

A generalization of a previous result is that, if L/K is an extension, then $\mathfrak{p}$ ramifies iff $\mathfrak{p} \mid \mathcal{D}_{L/K}$.

So consider a prime $\mathfrak{p}$ that does not ramify in L. Then $e(\mathcal{P}/\mathfrak{p}) = 1$, so $\#I(\mathcal{P}/\mathfrak{p}) = 1$. Thus, we have an isomorphism

$$D_{\mathcal{P}} \to G(\mathbb{F}_{\mathcal{P}}/\mathbb{F}_{\mathfrak{p}}). \tag{358}$$

Now, $G(\mathbb{F}_{\mathcal{P}}/\mathbb{F}_{\mathfrak{p}})$ is a cyclic group generated by the map $\alpha \mapsto \alpha^{N\mathfrak{p}} = \alpha^{\#\mathbb{F}_{\mathcal{P}}}$. So $D_{\mathcal{P}}$ is cyclic as well, and we know what its generator should look like.

Corollary 24.3

If $\mathfrak{p}$ is unramified in L/K, then for each $\mathcal{P} \mid \mathfrak{p}$, there is a unique element $(\mathcal{P}, L/K)$

$$(\mathcal{P}, L/K) \in D_{\mathcal{P}} \subset G_{L/K} \tag{359}$$

with

$$(\mathcal{P}, L/K) \pmod{\mathcal{P}} = \text{Frobenius element in } G(\mathbb{F}_{\mathcal{P}}/\mathbb{F}_{\mathfrak{p}}). \tag{360}$$

That is,

$$(\mathcal{P}, L/K) \cdot \alpha = \alpha^{N\mathfrak{p}} \pmod{\mathcal{P}} \tag{361}$$

for all $\alpha \in R_L$. This is called the **Artin symbol** of $\mathcal{P}/\mathfrak{p}$.